

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

NOAH SAEEDY, VISHAL SHAH, TINA
WILKINSON, and M.S., individually, and on
behalf of all others similarly situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a
Washington Corporation,

Defendant.

Case No. 2:23-cv-1104

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Noah Saeedy, Vishal Shah, M.S., a minor, by and through his natural parent and legal guardian Crystal Arterberry, (collectively, the “California Plaintiffs”) and Tina Wilkinson (“Washington Plaintiff”) (collectively, “Plaintiffs”), individually and on behalf of all other similarly situated, by and through their undersigned counsel, allege the following upon information and belief, except as to those allegations concerning Plaintiffs, which they allege upon personal knowledge.

I. NATURE AND OVERVIEW OF THE ACTION

1
2 1. The Microsoft Edge browser (“Edge”) is a proprietary, cross-platform internet
3 browser¹ created and marketed by Defendant Microsoft Corp. (“Microsoft” or “Defendant”). Like
4 its predecessor Internet Explorer, Edge has proven to be widely popular with internet users both in
5 the United States and abroad, taking up the third-largest market share of all internet browsers
6 across desktops and all platforms. Versions 90, 92, 93 and earlier and later versions of Edge offer
7 a default “non-private” browsing mode, as well as a “private” browsing mode through the use of
8 an “inPrivate” window.

9 2. Unbeknownst to users, Defendant programmed Versions 90, 92, 93, and earlier and
10 later versions of Edge to surreptitiously intercept, collect and send to Defendant a wide range of
11 private data relating to users’ internet browsing activities, internet searches, and online shopping
12 behavior, including while in “private” browsing mode. As this private data is intercepted and
13 collected, it is associated with unique user identifiers that Defendant assigns to users, and/or
14 cookies—small text files containing unique data by which to identify a user’s device—that it
15 installs on users’ devices. Upon intercepting and receiving the private user data, unique user
16 identifiers, and cookies from Edge, Defendant then links or binds the private user data to
17 individual users though the unique user identifiers and cookies.

18 3. Edge sends the intercepted and collected private user data and the unique user
19 identifiers and cookies to several Microsoft-controlled servers, including those servers located at
20 nav.smartscreen.microsoft.com (the “SmartScreen Server”) and at
21 <https://www.bing.com/api/shopping/v1> (the “Bing Server”).

22 4. By associating the collected private data with the unique user identifiers and cookies,
23 Defendant can and does determine individual users’ precise internet browsing activities and habits.
24
25

26 ¹ The terms “internet browser” and “web browser” are used interchangeably throughout this Complaint.

1 Defendant thus utilized and configured Versions 90, 92, and 93, and earlier and later versions of
2 the Edge browser to intercept, collect and process personally identifiable private data.

3 5. Defendant intercepts, collects, and sends users' keyword search terms, URLs, and
4 unique user identifiers and cookies to the SmartScreen and Bing servers without their actual or
5 implied consent. Defendant fails to conspicuously present its flawed and deficient Privacy
6 Statement and Terms of Use to users and thus these electronic documents have no legal effect .

7 6. As such, Defendant's practices have and continue to result in numerous violations
8 of both federal and state laws as described herein.

9 **II. PARTIES**

10 7. Plaintiff Noah Saeedy ("Plaintiff Saeedy" or "Saeedy") resides in Glendora,
11 California. Plaintiff Saeedy has used Microsoft Edge since June of 2021 and used the Microsoft
12 Edge browser from his personal computer daily or weekly for both personal and work purposes.
13 Plaintiff Saeedy used Edge to shop on Amazon and eBay's websites. Plaintiff Saeedy has a
14 reasonable expectation of privacy in his private data described herein as well as in the collection
15 and processing of his unique user identifiers in connection with that content. Plaintiff Saeedy has
16 a property right and interest in his private data described herein such that the interception and use
17 of that data is violative of those rights and therefore causes him injury and damages. Saeedy
18 would not have used the Microsoft Edge browser had he known Defendant was collecting,
19 intercepting, and using his private data described herein. Plaintiff Saeedy could not provide
20 consent to the interception and use because he did not know that his private content was being
21 collected, intercepted, and used by Defendant, and reasonably anticipated that private data
22 described herein and connected unique user identifiers and cookies would remain private. Saeedy
23 has suffered further economic injury as a result of Defendant's unlawful and unauthorized
24 interceptions and recordings of communications. Defendant used Plaintiff Saeedy's private data
25 for various purposes, including, but not limited to, improving its software, services, and devices,
26

1 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
2 learning systems.

3 8. Plaintiff Vishal Shah (“Plaintiff Shah” or “Shah”) resides in Buena Park,
4 California. Plaintiff Shah has used Microsoft Edge since June of 2021 and used the Microsoft
5 Edge browser from a computer provided by an employer or workplace. Plaintiff Shah used Edge
6 to shop on Amazon and BestBuy’s websites. Plaintiff Shah has a reasonable expectation of
7 privacy in his private data described herein as well as in the collection and processing of his
8 unique user identifiers in connection with that content. Plaintiff Shah has a property right and
9 interest in his private data described herein such that the interception and use of that data is
10 violative of those rights and therefore causes him injury and damages. Shah would not have used
11 the Microsoft Edge browser had he known Defendant was collecting, intercepting, and using his
12 private content. Plaintiff Shah could not provide consent to the interception and use because he
13 did not know that his private content was being collected, intercepted, and used by Defendant, and
14 reasonably anticipated that his private data described herein and connected unique user identifiers
15 and cookies would remain private. Shah has suffered further economic injury as a result of
16 Defendant’s unlawful and unauthorized interceptions and recordings of communications.

17 9. Plaintiff Tina Wilkinson (“Plaintiff Wilkinson” or “Wilkinson”) resides in
18 Richland, Washington. Plaintiff Wilkinson has used Microsoft Edge since June of 2021 and used
19 the Microsoft Edge browser on a computer provided by an academic institution. Plaintiff
20 Wilkinson used Edge to shop on third party websites. Plaintiff Wilkinson has a reasonable
21 expectation of privacy in her private data described herein as well as in the collection and
22 processing of her unique user identifiers in connection with that content. Plaintiff Wilkinson has a
23 property right and interest in her private data described herein such that the interception and use of
24 that data is violative of those rights and therefore causes her injury and damages. Wilkinson
25 would not have used the Microsoft Edge browser had she known Defendant was collecting,
26 intercepting, and using her private content. Plaintiff Wilkinson could not provide consent to the

1 interception and use because she did not know that her private content was being collected,
2 intercepted, and used by Defendant, and reasonably anticipated that her private data described
3 herein and connected unique user identifiers and cookies would remain private. Wilkinson has
4 suffered further economic injury as a result of Defendant’s unlawful and unauthorized
5 interceptions and recordings of communications.

6 10. Plaintiff M.S., a minor, (“Plaintiff M.S.” or “M.S.”) resides in Lancaster,
7 California. Plaintiff M.S. has used Microsoft Edge since June of 2021 and used the Microsoft
8 Edge browser from a personal computer daily or weekly for both personal purposes. Plaintiff
9 M.S. used Edge to shop on Amazon’s website and search on Google and Yahoo’s search engine.
10 Plaintiff M.S. has a reasonable expectation of privacy in his private data described herein as well
11 as in the collection and processing of his unique user identifiers in connection with that content.
12 Plaintiff M.S. has a property right and interest in his private data described herein such that the
13 interception and use of that data is violative of those rights and therefore causes him injury and
14 damages. M.S. would not have used the Microsoft Edge browser had he known Defendant was
15 intercepting, collecting, and sharing his private content. Plaintiff M.S. could not provide consent
16 to the interception and use because he is a minor and further because he did not know that his
17 private content was being collected, intercepted, and used by Defendant, and reasonably
18 anticipated that his private data described herein and connected unique user identifiers and cookies
19 would remain private. M.S. has suffered further economic injury as a result of Defendant’s
20 unlawful and unauthorized interceptions and recordings of communications.

21 11. Defendant Microsoft is a publicly traded company incorporated under the laws of
22 Washington with its principal executive offices located at One Microsoft Way, Redmond,
23 Washington 98052. Microsoft offers computer hardware and software products for business and
24 personal use, including the Microsoft Edge internet browser (“Edge”). Microsoft describes Edge
25
26

1 as its “fast and secure browser that helps protect [users’] data, with built-in shopping tools
2 designed to save [users] time and money.”²

3 III. JURISDICTION AND VENUE

4 12. The Court has personal jurisdiction over Defendant because Defendant is
5 headquartered in this District.

6 13. This Court has subject matter jurisdiction over the federal claims in this action,
7 specifically the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*, and the
8 Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

9 14. This Court also has subject matter jurisdiction over this entire action pursuant to the
10 Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because this is a class action in which
11 the amount in controversy exceeds \$5,000,000, and at least one member of the Class is a citizen of
12 a state other than Washington.

13 15. The Court also has supplemental jurisdiction over the remaining state law claims
14 pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or
15 controversy as those that give rise to the federal claims.

16 16. Venue is proper in this District because Defendant is headquartered in this District.
17 In addition, in the current Microsoft Software License Terms and prior versions of the Terms,
18 Defendant purports to bind Plaintiffs to bring disputes in this District. *See* Exhibit A, at § 2.16.

19 IV. SUBSTANTIVE ALLEGATIONS

20 A. The Microsoft Edge Internet Browser

21 17. Microsoft Edge is a proprietary, cross-platform internet browser created and
22 marketed by Defendant. Microsoft first released the Edge browser to the general public in July 2015
23 as the successor to Defendant’s highly successful Internet Explorer web browser, which was at one
24 time the most-widely used internet browser in the world. Since being released to the public, Edge
25

26 ² Microsoft Corporation, Annual Report (Form 10-K), at 5 (July 28, 2022).

1 has undergone various iterations and updates, beginning with the original Version 20 in July 2015
2 to Version 115 at the time of the filing of this Complaint.

3 18. Defendant Microsoft describes Edge as its “fast and secure browser that helps protect
4 [users’] data, with built-in shopping tools designed to save [users] time and money.”³ Through
5 Edge, users can, among other things, browse the internet and its numerous websites, access their
6 email and social media accounts, conduct keyword searches, engage in online shopping and other
7 e-commerce, download files, and communicate with their friends, family, and business colleagues.

8 19. Since its release, Edge has been available to users via download through Microsoft’s
9 website or the online Microsoft Store. Microsoft releases new versions of Edge to the public for
10 download through what it refers to as “channels,” first releasing new versions through its
11 development channels, such as the “Beta Channel,” to a sample set of users before deploying them
12 broadly to the public through the “Stable Channel.”⁴

13 20. Additionally, Defendant’s Windows 10 operating system—which, like Edge, was
14 released in July 2015—comes with Edge pre-installed, thereby ensuring that Edge appears on any
15 new computer purchased with Windows 10 or any computer that has had its operating system
16 upgraded to Windows 10 from a previous version.

17 21. Like its predecessor Internet Explorer, Edge has proven to be widely popular with
18 internet users both in the United States and abroad. According to web analytics service Statcounter,
19 in the United States, where there are an estimated 299 million internet users, Edge owned the third-
20 largest market share of all internet browsers across desktops and all platforms (*i.e.*, desktops, tablets,
21
22
23

24 ³ Microsoft Corporation, Annual Report (Form 10-K), at 5 (July 28, 2022).

25 ⁴ See *Overview of the Microsoft Edge Channels*, Microsoft, [https://learn.microsoft.com/en-
26 us/deployedge/microsoft-edge-channels#channel-overview](https://learn.microsoft.com/en-us/deployedge/microsoft-edge-channels#channel-overview) (last visited July 21, 2023).

1 and mobile devices) as of February 2023, with approximately 13.23%⁵ and 6.85%⁶ market share,
 2 respectively. Internationally, where there are an estimated 5.16 billion internet users,⁷ Statcounter
 3 calculates that as of February 2023, Edge represented the second-largest market share of all internet
 4 browsers across desktops and the third-largest market share of all internet browsers across all
 5 platforms, with 10.84%⁸ and 4.27%⁹ market share, respectively. Put simply, Edge is used by tens
 6 of millions of people in the United States and hundreds of millions of people around the world.

7 **B. Versions 90, 92, 93, and Earlier and Later Versions of Edge Offer “Private”**
 8 **Browsing Windows**

9 22. Versions 90, 92, 93, and earlier and later versions of Edge offer a default “non-
 10 private” browsing mode, as well as a “private” browsing mode through the use of an “inPrivate”
 11 window. When users open Version 90, 92, 93 and earlier and later versions of the Edge browser, a
 12 “non-private” browsing window appears. Users can select to open and browse through an inPrivate
 13 window by selecting it from the Edge browser’s options. Defendant describes its inPrivate window
 14 to users as a more private way to browse the internet that, among other things, “deletes [users’]
 15 browsing information when [they] close all inPrivate windows” and “prevents Microsoft Bing
 16

17 ⁵ See *Desktop Browser Market Share United States of America Jan 2020–Mar 2023*, statcounter,
 18 <https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america#monthly-202001-202303> (last visited July 17, 2023).

19 ⁶ See *Browser Market Share United States of America Jan 2020–Mar 2023*, statcounter,
 20 <https://gs.statcounter.com/browser-market-share/all/united-states-of-america#monthly-202001-202303> (last visited July 21, 2023).

21 ⁷ See Ani Petrosyan, *Number of internet and social media users worldwide as of January 2023 (in billions)*, statista (Apr. 3, 2023), <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

23 ⁸ See *Desktop Browser Market Share Worldwide Jan 2020–Mar 2023*, statcounter,
 24 <https://gs.statcounter.com/browser-market-share/desktop/worldwide#monthly-202001-202303> (last visited July 21, 2023).

25 ⁹ See *Browser Market Share Worldwide Jan 2020–Mar 2023*, statcounter,
 26 <https://gs.statcounter.com/browser-market-share#monthly-202001-202303> (last visited July 21, 2023).

1 searches from being associated with [users].” Defendant neither clearly nor expressly explains that
2 browsing the internet through an inPrivate window does not prevent Edge from intercepting,
3 collecting, and sending data associated with users’ internet activity, including users’ search terms
4 on websites, visited webpages, and online shopping activities to Defendant.

5 **C. Versions 90, 92, 93 and Earlier and Later Versions of Edge Surreptitiously Intercept**
6 **and Collect Private User Data and Send it to Defendant**

7 23. Unbeknownst to users, Defendant programmed Versions 90, 92, 93 and earlier and
8 later versions of Edge to surreptitiously intercept, collect and send to Defendant a wide range of
9 private data relating to users’ internet browsing activities, internet searches, and online shopping
10 behavior. As this data is collected, it is associated with unique user identifiers that Defendant
11 assigns to users, and/or cookies—small text files containing unique data by which to identify a user’s
12 device—that it installs on users’ devices. These unique user identifiers and cookies include the
13 user’s: (i) Microsoft Machine Unique Identifier (“MUID”); (ii) WLS Identifier (“WLS”); (iii)
14 Windows Live ID (“WLID”); (iv) impressionId; and (v) X-Client-Data.

15 24. The MUID cookie is a unique user identifier used for advertising, site analytics, and
16 other operational purposes, which links the user data it collects to a specific user and consists of an
17 alphanumeric string.

18 25. The WLS is a unique user identifier assigned to a specific user that consists of an
19 alphanumeric string. The WLS also includes a user’s real name.

20 26. The WLID is a unique user identifier assigned to a specific user that consists of an
21 alphanumeric string.

22 27. The impressionId is a unique user identifier assigned to a specific user that consists
23 of an alphanumeric string.

24 28. X-User-Data is a user identifier assigned to a specific user that consists of an
25 alphanumeric string.

26

1 29. Edge also collects and sends to Microsoft identifying information about a user’s web
2 browser, which it collectively terms “User-Agent Data.”

3 30. Edge sends the collected user data and the unique user identifiers and cookies to
4 several Microsoft-controlled servers, including those servers located at
5 nav.smartscreen.microsoft.com (the “SmartScreen Server”) and at
6 https://www.bing.com/api/shopping/v1 (the “Bing Server”).

7 31. Upon receiving the private user data, unique user identifiers, and cookies from Edge,
8 Defendant then links or binds the user data to individual users through the unique user identifiers and
9 cookies.

10 **1. Microsoft Uses the Private Data It Surreptitiously Intercepts and Collects**
11 **from Users**

12 32. More than just intercepting and collecting the private data described herein from
13 users of the Edge Browser, Defendant uses that data for various purposes, including, but not
14 limited to, improving its software, services, and devices, and providing targeted advertising.

15 33. Microsoft’s surreptitious interception, collection and use of private user data has
16 become so rampant that even fellow tech giant Twitter has accused Microsoft of misusing
17 Twitter’s data, with Twitter CEO Elon Musk also accusing Microsoft and its partner OpenAI of
18 illegally using Twitter data to develop sophisticated artificial intelligence systems such as
19 ChatGPT.¹⁰ On information and belief, Microsoft is also using the intercepted private user data
20 described herein to develop its sophisticated artificial intelligence and machine-learning systems.

21 34. Edge users are not aware, and Defendant does not adequately provide them with
22 notice, that Defendant uses users’ private data described herein for various purposes, including,
23

24
25 ¹⁰ David Hamilton, *Twitter accuses Microsoft of misusing its data, foreshadowing a possible*
26 *fight over AI*, AP News, <https://apnews.com/article/twitter-microsoft-ai-training-data-dispute-musk-nadella-292fd9de9cc2623003fd1ce44897c912>.

1 but not limited to, improving its software, services, and devices, providing targeted advertising,
2 and developing its sophisticated artificial intelligence and machine-learning systems.

3 **D. Microsoft Edge Version 90**

4 35. Microsoft Edge Version 90 (“Version 90”) was released via the Beta Channel on or
5 around March 16, 2021 and was released through the Stable Channel on or around April 15,
6 2021.¹¹ Unbeknownst to users, Version 90 surreptitiously collects, intercepts, and sends to the
7 Bing Server a wide range of private data relating to users’ internet browsing and online shopping
8 activities, and links that data with unique user identifiers, without users’ knowledge or consent.
9 By linking users’ unique user identifiers and User Agent Data with the collected data regarding
10 users’ internet browsing and online shopping activities, Defendant is able to identify individual
11 users and associate them with their internet activities. The intercepted data includes, as further
12 described herein, search queries and visited webpages.

13 **1. Version 90 “Binds” User Identifiers**

14 36. When a user opens Version 90 of the Edge Browser and is either already logged in
15 to his Microsoft Account or logs in to his Microsoft Account, Edge collects and processes the
16 user’s WLS and MUID together in the same data packet, “binding” them together for the
17 remainder of the user’s web-browsing session.¹² By having Version 90 process these unique user
18 identifiers and/or cookies at the beginning of the user’s web-browsing session, Defendant is able
19 to link them with the user’s internet browsing and online shopping activities and identify
20 individual users. Defendant’s ability to identify individual users is further enhanced by Version
21 90’s processing of User Agent Data as the user browses the internet. Furthermore, by having
22 Version 90 bind the user’s MUID and WLS together at the beginning of the user’s internet-

23 _____
24 ¹¹ See *Microsoft Edge release schedule*, Microsoft, <https://learn.microsoft.com/en-us/deployedge/microsoft-edge-release-schedule> (last visited June 17, 2023).

25 ¹² If a user opens an inPrivate window to browse the internet, Version 90 does not process the
26 user’s WLS or MUID at the start of the user’s session. However, on information and belief,
Version 90 process the user’s MUID later in the session as the user browses the internet.

1 browsing session, Defendant is able to continuously associate the user with his internet activity
2 even if the MUID changes throughout the session.

3 **2. Search Queries in Integrated Search Bars**

4 37. Many websites contain an integrated search bar that allows any visitor to search for
5 information on the website using search terms, similar to using an internet search engine like Bing,
6 Google, or Yahoo. When a user runs a search query on a website using the website's integrated
7 search bar, the website will often return a list of search results with links to the specific webpages
8 on the website that contain the information the user is searching for. A user can navigate to those
9 webpages by clicking on the links.

10 38. Unbeknownst to Version 90 users, when a Version 90 user utilizes the integrated
11 search bar on many websites, Edge collects, intercepts, and sends to the Bing Server the search
12 terms entered by the user.

13 39. Version 90 collects, intercepts, and sends this data to the Bing Server even when
14 the user is utilizing an inPrivate window.

15 40. Version 90 also collects and processes unique user identifiers and/or cookies
16 associated with the user as it collects, intercepts, and sends to the Bing Server the user's search
17 queries. These include the user's MUID and impressionId. Version 90 also collects and processes
18 the user's User Agent Data as it collects, intercepts, and sends to Defendant the user's search
19 queries, whether or not the user is logged in to his Microsoft Account. Defendant is able to link
20 the collected search queries to individual users through their unique user identifiers and/or
21 cookies, revealing to Defendant users' identities and internet search activity. If a user was logged
22 in to his Microsoft Account and not using an inPrivate window when he ran the search, Defendant
23 can additionally utilize the user's WLS to link the user to his search queries and identify the user,
24 even if the user's MUID changes throughout the session because Version 90 "binds" it together
25 with the user's MUID at the start of the user's session. Defendant's ability to identify users is
26 further enhanced by Version 90's processing of User Agent Data.

1 41. Defendant uses the above-described private data for various purposes discussed
2 above.

3 42. Version 90 users, including Plaintiffs and Class members, are unaware that Version
4 90 is collecting, intercepting, and sending to Defendant the above-described private data, and that
5 Defendant uses that data, and have not provided their consent, whether implied or express, for
6 Defendant to collect, intercept, receive, or use this data.

7 **3. Visited Webpages**

8 43. As users browse the internet using Edge, they navigate between different
9 webpages. Each webpage has a unique uniform resource locator, also known as a “URL,” which
10 serves as the webpage’s address on the internet.

11 44. Unbeknownst to Version 90 users, for many websites, whenever a Version 90 user
12 visits those websites or URLs within those websites, Edge collects, intercepts, and sends to the
13 Bing Server the full URL of each webpage a user visits. Version 90 collects, intercepts, and sends
14 this data to the Bing Server even when the user is utilizing an inPrivate window.

15 45. Version 90 also collects and processes unique user identifiers and/or cookies
16 associated with the user as it collects, intercepts, and sends to the Bing Server the user’s visited
17 URLs. These include the user’s MUID and impressionId. Version 90 also collects and processes
18 the user’s User Agent Data as it collects, intercepts, and sends to Defendant the user’s visited
19 URLs, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the
20 visited URLs to individual users through their unique user identifiers and/or cookies, revealing
21 users’ identities and internet search activity to Defendant. If a user was logged in to his Microsoft
22 Account and not using an inPrivate window when he visited the URL, Defendant can additionally
23 utilize the user’s WLS to link the user to his visited URLs and identify the user, even if the user’s
24 MUID changes throughout the session because Version 90 “binds” it together with the user’s
25 MUID at the start of the user’s session. Defendant’s ability to identify users is further enhanced
26 by Version 90’s processing of User Agent Data.

1 46. Defendant uses the above-described private data for various purposes discussed
2 above.

3 47. Version 90 users, including Plaintiffs and the Class, are unaware that Version 90 is
4 collecting, intercepting, and sending to Defendant the above-described private data, and that
5 Defendant uses that data, and have not provided their consent, whether implied or express, for
6 Defendant to collect, intercept, receive, or use this data.

7 **E. Microsoft Edge Version 92**

8 48. Microsoft Edge Version 92 (“Version 92”) was released via the Beta Channel on or
9 around June 8, 2021, and was released through the Stable Channel on or around July 22, 2021.¹³
10 Unbeknownst to users, Edge Version 92 surreptitiously collects, intercepts, and sends to the Bing
11 Server and/or SmartScreen Server a wide range of data relating to users’ internet browsing and
12 online shopping activities, and links that data with unique user identifiers, without users’
13 knowledge or consent. By linking users’ unique user identifiers and User Agent Data with the
14 collected data regarding users’ internet browsing and online shopping activities, Defendant can
15 identify individual users and associate them with their internet activities. The intercepted data
16 includes, as further described herein, search queries and visited webpages.

17 **1. Version 92 “Binds” User Identifiers**

18 49. When a user opens Version 92 of the Edge Browser and is either already logged in
19 to his Microsoft Account or logs in to his Microsoft Account, Edge collects and processes the
20 user’s WLS, MUID, WLID, and X-Client Data together in the same data packet, “binding” them
21 together for the remainder of the user’s web-browsing session. By having Version 92 process
22 these unique user identifiers and/or cookies at the beginning of the user’s web-browsing session,
23 Defendant is able to link them with the user’s internet browsing and online shopping activities and
24 identify individual users. Defendant’s ability to identify individual users is further enhanced by
25

26 ¹³ See *Microsoft Edge release schedule*, *supra*, note 11.

1 Version 92's processing of User Agent Data as the user browses the internet. Furthermore, by
2 having Version 92 bind the user's MUID, WLS, WLID, and X-Client-Data together at the
3 beginning of the user's internet-browsing session, Defendant is able to continuously associate the
4 user with his internet activity even if some of those identifiers change throughout the session.

5 **2. Search Queries in Integrated Search Bars**

6 50. Many websites contain an integrated search bar that allows any visitor to search for
7 information on the website using search terms, similar to using an internet search engine like Bing,
8 Google, or Yahoo. When a user runs a search query on a website using the website's integrated
9 search bar, the website will often return a list of search results with links to the specific webpages
10 on the website that contain the information the user is searching for. A user can navigate to those
11 webpages by clicking on the links.

12 51. Unbeknownst to Version 92 users, when a Version 92 user utilizes the integrated
13 search bar on many websites, Edge collects, intercepts, and sends to the Bing Server the search
14 terms entered by the user. Edge collects, intercepts, and sends this data to the Bing Server even
15 when the user is utilizing an inPrivate window.

16 52. Version 92 also collects and processes unique user identifiers and/or cookies
17 associated with the user together with the user's search queries. These include the user's MUID
18 and impressionId. Version 92 also collects and processes the user's User Agent Data as it collects,
19 intercepts, and sends to Defendant the user's search queries, whether or not the user is logged in to
20 his Microsoft Account. Defendant is able to link the collected search queries to individual users
21 through their unique user identifiers and cookies, revealing users' identity and internet search
22 activity to Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate
23 window when he ran the search, Defendant can additionally utilize the user's WLS, WLID, and X-
24 Client-Data to link the user to his search queries and identify the user, even if some of those
25 identifiers change throughout the session because Version 92 "binds" them together with the
26

1 user's MUID at the start of the user's session. Defendant's ability to identify users is enhanced by
2 Version 92's processing of User Agent Data.

3 53. Defendant uses the above-described private data for various purposes discussed
4 above.

5 54. Edge Version 92 users, including Plaintiffs and the Class, are unaware that Version
6 92 is collecting, intercepting, and sending to Defendant the above-described private data, and that
7 Defendant uses that data, and have not provided their consent, whether implied or express, for
8 Defendant to collect, intercept, receive, or use this data.

9 **3. Search Queries in Search Engines**

10 55. Edge Version 92 contains an address bar through which users can navigate the
11 internet. Users can use the address bar to navigate to a specific website or webpage by entering
12 the webpage's URL into the address bar.

13 56. Alternatively, users can use the address bar to enter search terms similar to the way
14 they would use a search engine like Google or Yahoo. Edge allows users to select from one of
15 several search engines to process their searches and return results when the address bar is used in
16 this way. Users can select their preferred search engine through Edge's "Settings" menu. By
17 default, Edge sets Bing as the search engine to process users' searches. However, users can select
18 between the Bing, Google, Yahoo, and DuckDuckGo search engines to process searches they enter
19 into the address bar.

20 57. When used to conduct a search, the address bar functions in two ways:

21 58. First, as a user types each character that makes up the key terms of his or her
22 search, Edge displays in real-time a list of potentially relevant search suggestions based on a
23 prediction of the user's search terms. A user may select one of the suggested searches by clicking
24 on it. If a user does so, the user's selected search engine will run the suggested search, and Edge
25 will navigate the user to a page displaying results for that search on the selected search engine's
26

1 website. From there, the user may click on any of the displayed results and navigate to the
2 specific webpage on which they appear.

3 59. Second, a user may choose to forgo selecting one of the suggested searches
4 displayed under the address bar as he enters search terms, and instead run his own search query
5 using search terms he enters. Like when a user chooses a suggested search, the user's selected
6 search engine will run the user's search query, and Edge will navigate the user to a page
7 displaying results for that search on the selected search engine's website. From there, a user may
8 click on any of the displayed results and navigate to the specific webpage on which they appear.

9 60. Unbeknownst to Version 92 users not utilizing an inPrivate window, when a user
10 sets his default search engine to Yahoo and runs a search through the Edge address bar, Edge
11 collects, intercepts, and sends to Defendant the user's search queries. Specifically, Edge collects
12 this data and sends it to the SmartScreen Server, thereby revealing to Defendant the user's internet
13 search activity. The same occurs if a user navigates to Yahoo's website and enters a search
14 through the search bar located there.

15 61. Defendant uses the above-described private data for various purposes discussed
16 above.

17 62. Edge users, including Plaintiffs and the Class, are unaware Defendant is collecting
18 the above-described data, regardless of whether they have chosen Bing to process their searches
19 queries in the Edge address bar, and that Defendant uses that data, and have not provided their
20 consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

21 **4. Visited Webpages**

22 63. As users browse the internet using Edge, they navigate between different webpages.
23 Each webpage has a URL which serves as the webpage's address on the internet.

24 64. Unbeknownst to Version 92 users, for many websites, whenever a Version 92 user
25 visits those websites or URLs within those websites, Edge collects, intercepts, and sends to the
26

1 Bing Server the full URL of each webpage a user visits. Version 92 collects, intercepts, and sends
2 this data to the Bing Server even when the user is utilizing an inPrivate window.

3 65. Version 92 also collects and processes unique user identifiers and/or cookies
4 associated with the user as it collects, intercepts, and sends to the Bing Server the user's visited
5 URLs. These include the user's MUID and impressionId. Version 92 also collects and processes
6 the user's User Agent Data as it collects, intercepts, and sends to Defendant the user's visited
7 URLs, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the
8 visited URLs to individual users through their unique user identifiers and/or cookies, revealing to
9 Defendant users' identities and internet search activity. If a user was logged in to his Microsoft
10 Account and not using an inPrivate window when he ran the search, Defendant can additionally
11 utilize the user's WLS, WLID, and X-Client-Data to link the user to his visited URLs and identify
12 the user, even if some of those identifiers change throughout the session because Version 92
13 "binds" them with the user's MUID at the start of the user's session. Defendant's ability to
14 identify users is further enhanced by Version 92's processing of User Agent Data.

15 66. Defendant uses the above-described private data for various purposes discussed
16 above.

17 67. Version 92 users, including Plaintiffs and the Class, are unaware that Version 92 is
18 collecting, intercepting, and sending the above-described private data to Defendant, and that
19 Defendant uses that data, and have not provided their consent, whether implied or express, for
20 Defendant to collect, intercept, receive, or use this data.

21 **F. Microsoft Edge Version 93**

22 68. Microsoft Edge Version 93 ("Version 93") was released via the Beta Channel on or
23 around August 3, 2021 and was released through the Stable Channel on or around September 2,
24 2021.¹⁴ Unbeknownst to users, Edge Version 93 surreptitiously collects, intercepts, and sends to
25

26 ¹⁴ See *Microsoft Edge release schedule*, *supra*, note 11.

1 the Bing Server a wide range of data relating to users' internet browsing and online shopping
2 activities, and links that data with unique user identifiers, without users' knowledge or consent.
3 By linking users' unique user identifiers and User Agent Data with the collected data regarding
4 users' internet browsing and online shopping activities, Defendant is able to identify individual
5 users and associate them with their internet activities. The intercepted data includes, as further
6 described herein, search queries and visited webpages.

7 **1. Version 93 "Binds" User Identifiers**

8 69. When a user opens Version 93 of the Edge Browser and is either already logged in
9 to his Microsoft Account or logs in to his Microsoft Account, Edge collects and processes the
10 user's WLS, MUID, and WLID together in the same data packet, "binding" them together for the
11 remainder of the user's web-browsing session. By having Version 93 process these unique user
12 identifiers and/or cookies at the beginning of the user's web-browsing session, Defendant is able
13 to link them with the user's internet browsing and online shopping activities and identify
14 individual users. Defendant's ability to identify individual users is further enhanced by Version
15 93's processing of User Agent Data as the user browses the internet. Furthermore, by having
16 Version 93 bind the user's MUID, WLS, and WLID together at the beginning of the user's
17 internet-browsing session, Defendant is able to continuously associate the user with his internet
18 activity even if some of those identifiers change throughout the session.

19 **2. Search Queries in Integrated Search Bars**

20 70. Many websites contain an integrated search bar that allows any visitor to search for
21 information on the website using search terms, similar to using an internet search engine like Bing,
22 Google, or Yahoo. When a user runs a search query on a website using the website's integrated
23 search bar, the website will often return a list of search results with links to the specific webpages
24 on the website that contain the information the user is searching for. A user can navigate to those
25 webpages by clicking on the links.
26

1 71. Unbeknownst to Version 93 users, when a Version 93 user utilizes the integrated
2 search bar on many websites that appear, Edge collects, intercepts, and sends to the Bing Server
3 the search terms entered by the user. Edge collects, intercepts, and sends this data to the Bing
4 Server even when the user is utilizing an inPrivate window.

5 72. Version 93 also collects and processes unique user identifiers and/or cookies
6 associated with the user together with the user's search queries. These include the user's MUID
7 and impressionId. Version 93 also collects and processes the user's User Agent Data as it collects,
8 intercepts, and sends to Defendant the user's search queries, whether or not the user is logged in to
9 his Microsoft Account. Defendant is able to link the collected search queries to individual users
10 through their unique user identifiers and cookies, revealing to Defendant users' identity and
11 internet search activity. If a user was logged in to his Microsoft Account and not using an
12 inPrivate window when he ran the search, Defendant can additionally utilize the user's WLS and
13 WLID to link the user to his search queries and identify the user, even if the WLID changes
14 throughout the session because Version 93 "binds" them together with the user's MUID at the
15 start of the user's session. Defendant's ability to identify users is enhanced by Version 93's
16 processing of User Agent Data.

17 73. Defendant uses the above-described private data for various purposes discussed
18 above.

19 74. Edge Version 93 users, including Plaintiffs and Class members, are unaware that
20 Version 93 is collecting, intercepting, and sending to Defendant the above-described private data,
21 and that Defendant uses that data, and have not provided their consent, whether implied or
22 express, for Defendant to collect, intercept, receive, or use this data.

23 **3. Visited Webpages**

24 75. As users browse the internet using Edge, they navigate between different
25 webpages. Each webpage has a unique URL which serves as the webpage's address on the
26 internet.

1 76. Unbeknownst to Version 93 users, for many websites, whenever a Version 93 user
2 visits those websites or URLs within those websites, Edge collects, intercepts, and sends to the
3 Bing Server the full URL of each webpage a user visits. Version 93 collects, intercepts, and sends
4 this data to the Bing Server even when the user is utilizing an inPrivate window.

5 77. Version 93 also collects and processes unique user identifiers and/or cookies
6 associated with the user as it collects, intercepts, and sends to the Bing Server the user's visited
7 URLs. These include the user's MUID and impressionId. Version 93 also collects and processes
8 the user's User Agent Data as it collects, intercepts, and sends the user's visited URLs to
9 Defendant, whether or not the user is logged in to his Microsoft Account. Defendant can link the
10 visited URLs to individual users through their unique user identifiers and/or cookies, revealing to
11 Defendant users' identities and internet search activity. If a user was logged in to his Microsoft
12 Account and not using an inPrivate window when he ran the search, Defendant can additionally
13 utilize the user's WLS and WLID to link the user to his visited URLs and identify the user, even if
14 the WLID changes throughout the session because Version 93 "binds" them with the user's MUID
15 at the start of the user's session. Defendant's ability to identify users is further enhanced by
16 Version 93's processing of User Agent Data.

17 78. Defendant uses the above-described private data for various purposes discussed
18 above.

19 79. Version 93 users, including Plaintiffs and the Class, are unaware that Version 93 is
20 collecting, intercepting, and sending to Defendant the above-described private data, and that
21 Defendant uses that data, and have not provided their consent, whether implied or express, for
22 Defendant to collect, intercept, receive, or use this data.

23 **G. Earlier and Later Versions of Edge**

24 80. On information and belief, as with Edge Versions 90, 92, and 93, and unbeknownst
25 to users, earlier and later versions of Edge surreptitiously intercept, collect, and send to the Bing
26 Server and/or SmartScreen Server a wide range of data relating to users' internet browsing and

1 online shopping activities, and link that data with unique user identifiers without users' knowledge
2 or consent. By linking users' unique user identifiers and User Agent Data with the collected data
3 regarding users' internet browsing and online shopping activities, Defendant can identify
4 individual users and associate them with their internet activities. The intercepted data includes at
5 least some of the same categories of data as those collected by Versions 90, 92, and 93.

6 81. Defendant uses the above-described private data for various purposes discussed
7 above.

8 82. Users of earlier and later versions of Edge, including Plaintiffs and the Class, are
9 unaware that these versions are collecting, intercepting, and sending to Defendant the above-
10 described private data, and that Defendant uses that data, and have not provided their consent,
11 whether implied or express, for Defendant to collect, intercept, receive, or use this data.

12 **H. Versions 90, 92, 93, and Earlier and Later Versions of Edge Surreptitiously Intercept**
13 **and Collect Users' Online Shopping Data**

14 83. Versions 90, 92, 93, and earlier and later versions of Edge each collect, intercept,
15 and send to Defendant via the Bing and/or SmartScreen Servers a plethora of data related to users'
16 online shopping habits on some of the world's largest retail websites, including those of Amazon,
17 eBay, Walmart, and Best Buy. As described in further detail below, Defendant's surreptitious
18 conduct includes the interception and collection of the URLs users visit, the search terms they
19 input, the contents of the product pages they view (*e.g.*, product reviews, product images), and the
20 contents of their shopping carts. Defendant indiscriminately intercepts and collects, and sends this
21 data to Microsoft, with no regard for the nature of the product a user browses or purchases, even
22 those items for intimate use.

23 84. Edge collects, intercepts, and sends this data to the Bing and/or SmartScreens
24 Servers, and links it with users' unique user identifiers and cookies, which allows Defendant to
25 identify users and associate them with the specific items they browsed or purchased as well as
26 with their online shopping habits more broadly. Edge users, including Plaintiffs and the Class, are

1 unaware that Defendant is collecting this data, and have not provided their consent, whether
2 implied or express, for Defendant to collect, intercept, or receive this data.

3 **1. Amazon**

4 85. Amazon.com, Inc. (“Amazon”) is one of the world’s largest online marketplaces
5 and retailers, with over 300 million active customer accounts¹⁵ and net sales of \$514 billion in
6 2022¹⁶. Through Amazon’s website, located at www.amazon.com (the “Amazon Website”), users
7 are able to view, place in their online shopping carts, and purchase products or items from private
8 sellers, other retailers, or Amazon directly.

9 86. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users’
10 data, including data related to their online shopping habits, when they visit the Amazon Website.

11 **a. Version 90**

12 87. Unbeknownst to Version 90 users, when a Version 90 user browses the Amazon
13 Website using Version 90 of Edge, Version 90 does each of the following:

- 14 • **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms
15 entered by the user into the integrated search bar on the Amazon Website;
- 16 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
17 user navigates to, including the URL for the page of each product or item the user
18 clicks on and views. If a user navigated to the product by first running a search
19 using the Amazon Website’s integrated search bar, the user’s search terms are also
20 included among the data collected, intercepted, and sent to the Bing Server when
21 the user navigates to the product page;

22
23

¹⁵ See *Amazon Stats, Growth, Sales, and More*, Amazon, [https://sell.amazon.com/blog/amazon-](https://sell.amazon.com/blog/amazon-stats)
24 [stats](https://sell.amazon.com/blog/amazon-stats) (last visited July 21, 2023).

25 ¹⁶ See *Amazon.com Announces Fourth Quarter Results*, Amazon,
26 [https://ir.aboutamazon.com/news-release/news-release-details/2023/Amazon.com-Announces-](https://ir.aboutamazon.com/news-release/news-release-details/2023/Amazon.com-Announces-Fourth-Quarter-Results/default.aspx)
[Fourth-Quarter-Results/default.aspx](https://ir.aboutamazon.com/news-release/news-release-details/2023/Amazon.com-Announces-Fourth-Quarter-Results/default.aspx) (last visited July 21, 2023).

- 1 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server,
2 the content of the reviews left by other users for each product or item the user
3 clicks on and views; and
- 4 • **Product Ratings:** Scrapes and collects, intercepts, and sends to the Bing Server,
5 the ratings left by other users for each product or item the user clicks on and views.

6 This data collection occurs even when the user is utilizing an inPrivate window.

7 88. Together with the above-described data, Version 90 also collects and processes
8 unique user identifiers and/or cookies associated with the user. These include the user's MUID
9 and impressionId. Version 90 also collects and processes the user's User Agent Data as it collects,
10 intercepts, and sends to Defendant the above-described data, whether or not the user is logged in to
11 his Microsoft Account. Defendant is able to link the above-described data to individual users
12 through their unique user identifiers and/or cookies, revealing to Defendant users' identities and
13 online shopping activity. If a user was logged in to his Microsoft Account and not using an
14 inPrivate window when he browsed the Amazon Website, Defendant can additionally utilize the
15 user's WLS to link the user to the above-described data and identify the user, even if the user's
16 MUID changes throughout the session because Version 90 "binds" it together with the user's
17 MUID at the start of the user's session. Defendant's ability to identify users is further enhanced
18 by Version 90's processing of User Agent Data.

19 89. Defendant uses the above-described private data for various purposes discussed
20 above.

21 90. Version 90 users, including Plaintiffs and the Class, are unaware that Version 90 is
22 collecting, intercepting, and sending to Defendant the above-described private data, and that
23 Defendant uses that data, and have not provided their consent, whether implied or express, for
24 Defendant to collect, intercept, receive, or use this data.

1 **b. Version 92**

2 91. Unbeknownst to Version 92 users, when a Version 92 user browses the Amazon
3 Website using Version 92 of Edge, Version 92 does each of the following:

- 4 • **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms
5 entered by the user into the integrated search bar on the Amazon Website;
- 6 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
7 user navigates to, including the URL for the page of each product or item the user
8 clicks on and views. If a user navigated to the product by first running a search
9 using the Amazon Website's integrated search bar, the user's search terms are also
10 included among the data collected, intercepted, and sent to the Bing Server when
11 the user navigates to the product page;
- 12 • **Shopping Cart Contents:** Intercepts and collects, and sends to the Bing Server, the
13 title, price, quantity, and URL for each product or item in the user's shopping cart;
- 14 • **Product Reviews:** Scrapes and collects, and sends to the Bing Server, the content
15 of the reviews left by other users for each product or item the user clicks on and
16 views; and
- 17 • **Product Ratings:** Scrapes and collects, and sends to the Bing Server, the ratings
18 left by other users for each product or item the user clicks on and views.

19 This data collection occurs even when the user is utilizing an inPrivate window.

20 92. Together with the above-described data, Version 92 also collects and processes
21 unique user identifiers and/or cookies associated with the user. These include the user's MUID
22 and impressionId. Version 92 also collects and processes the user's User Agent Data as it collects,
23 intercepts, and sends to Defendant the above-described data, whether or not the user is logged in to
24 his Microsoft Account. Defendant is able to link the above-described data to individual users
25 through their unique user identifiers and cookies, revealing to Defendant users' identity and online
26 shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate

1 window when he browsed the Amazon Website, Defendant can additionally utilize the user's
2 WLS, WLID, and X-Client-Data to link the user to the above-described data and identify the user,
3 even if some of those identifiers change throughout the session because Version 92 "binds" them
4 together with the user's MUID at the start of the user's session. Defendant's ability to identify
5 users is enhanced by Version 92's processing of User Agent Data.

6 93. Defendant uses the above-described private data for various purposes discussed
7 above.

8 94. Edge Version 92 users, including Plaintiffs and the Class, are unaware that Version
9 92 is collecting, intercepting, and sending to Defendant the above-described private data, and that
10 Defendant uses that data, and have not provided their consent, whether implied or express, for
11 Defendant to collect, intercept, receive, or use this data.

12 **c. Version 93**

13 95. Unbeknownst to users, when a user browses the Amazon Website using Version 93
14 of Edge with the Updated Configuration applied, Edge does each of the following:

- 15 • **URLs:** Collects, intercepts, and sends to the Bing Server, the URL of each page the
16 user navigates to, including the URL for the page of each product or item the user
17 clicks on and views;
- 18 • **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server, the
19 title, price, quantity, image (and URL for that image), and URL for each product or
20 item in the user's shopping cart;
- 21 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server,
22 the content of the reviews left by other users for each product or item the user
23 clicks on and views;
- 24 • **Product Ratings:** Scrapes and collects, intercepts, and sends to the Bing Server,
25 the ratings left by other users for each product or item the user clicks on and views;
26 and

- **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the image (and URL for that image) of each product or item the user clicks and views.

This data collection occurs even when the user is utilizing an inPrivate window.

96. Together with the above-described data, Version 93 also collects and processes unique user identifiers and/or cookies associated with the user. These include the user’s MUID and impressionId. Version 93 also collects and processes the user’s User Agent Data as it collects, intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the above-described data to individual users through their unique user identifiers and cookies, revealing to Defendant users’ identity and online shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he browsed the Amazon Website, Defendant can additionally utilize the user’s WLS and WLID to link the user to the above-described data and identify the user, even if the WLID changes throughout the session because Version 93 “binds” them together with the user’s MUID at the start of the user’s session. Defendant’s ability to identify users is enhanced by Version 93’s processing of User Agent Data.

97. Defendant uses the above-described private data for various purposes discussed above.

98. Edge Version 93 users, including Plaintiffs and the Class, are unaware that Version 93 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

2. eBay

99. eBay Inc. (“eBay”) is one of the world’s largest online marketplaces, with approximately 138 million active users in 2022 and revenue of nearly \$10 billion in that year.¹⁷

¹⁷ *eBay Revenue and Usage Statistics (2023)*, Business of Apps, <https://www.businessofapps.com/data/ebay-statistics/> (last visited July 21, 2023).

1 Through eBay’s website, located at www.ebay.com (the “eBay Website”), users are able to view,
2 place in their online shopping carts, and purchase or bid on products or items from private sellers
3 or retailers.

4 100. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users’
5 data, including data related to their online shopping habits, when they visit the eBay Website.

6 **a. Version 92**

7 101. Unbeknownst to Version 92 users, when a Version 92 user browses the eBay
8 Website using Version 92 of Edge, Version 92 does each of the following:

- 9 • **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms
10 entered by the user into the integrated search bar on the eBay Website.
11 Furthermore, if a user is not logged in to his Microsoft Account, Version 92 also
12 collects, intercepts, and sends the user’s search terms to the SmartScreen server;
- 13 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
14 user navigates to, including the URL for the page of each product or item the user
15 clicks on and views; and
- 16 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
17 image (and URL for that image) of each product or item the user clicks and views
18 when a user is not utilizing an inPrivate to browse the eBay website.

19 102. Together with the above-described data, Version 92 also collects and processes
20 unique user identifiers and/or cookies associated with the user. These include the user’s MUID
21 and impressionId. Version 92 also collects and processes the user’s User Agent Data as it collects,
22 intercepts, and sends to Defendant the above-described data, whether or not the user is logged in to
23 his Microsoft Account. Defendant is able to link the above-described data to individual users
24 through their unique user identifiers and cookies, revealing users’ identity and online shopping
25 activity to Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate
26 window when he browsed the eBay Website, Defendant can additionally utilize the user’s WLS,

1 WLID, and X-Client-Data to link the user to the above-described data and identify the user, even
2 if some of those identifiers change throughout the session because Version 92 “binds” them
3 together with the user’s MUID at the start of the user’s session. Defendant’s ability to identify
4 users is enhanced by Version 92’s processing of User Agent Data.

5 103. Defendant uses the above-described private data for various purposes discussed
6 above.

7 104. Edge Version 92 users, including Plaintiffs and the Class, are unaware that Version
8 92 is collecting, intercepting, and sending the above-described private data to Defendant, and that
9 Defendant uses that data, and have not provided their consent, whether implied or express, for
10 Defendant to collect, intercept, receive, or use this data.

11 **b. Version 93**

12 105. Unbeknownst to users, when a user browses the eBay Website using Version 93 of
13 Edge with the Updated Configuration applied, Edge does each of the following:

- 14 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
15 user navigates to, including the URL for the page of each product or item the user
16 clicks on and views;
- 17 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server
18 the content of the reviews left by other users for each product or item the user
19 clicks on and views;
- 20 • **Product Ratings:** Scrapes and collects, intercepts, and sends to the Bing Server the
21 ratings left by other users for each product or item the user clicks on and views; and
22 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
23 image (and URL for that image) of each product or item the user clicks and views
24 when a user is not utilizing an inPrivate to browse the eBay website.

25 This data collection occurs even when the user is utilizing an inPrivate window.

26 106. Together with the above-described data, Version 93 also collects and processes

1 unique user identifiers and/or cookies associated with the user. These include the user’s MUID
2 and impressionId. Version 93 also collects and processes the user’s User Agent Data as it collects,
3 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
4 his Microsoft Account. Defendant is able to link the above-described data to individual users
5 through their unique user identifiers and cookies, revealing to Defendant users’ identity and online
6 shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate
7 window when he browsed the eBay Website, Defendant can additionally utilize the user’s WLS
8 and WLID to link the user to the above-described data and identify the user, even if the WLID
9 changes throughout the session because Version 93 “binds” them together with the user’s MUID
10 at the start of the user’s session. Defendant’s ability to identify users is enhanced by Version 93’s
11 processing of User Agent Data.

12 107. Defendant uses the above-described private data for various purposes discussed
13 above.

14 108. Edge Version 93 users, including Plaintiffs and the Class, are unaware that Version
15 93 is collecting, intercepting, and sending the above-described private data to Defendant, and that
16 Defendant uses that data, and have not provided their consent, whether implied or express, for
17 Defendant to collect, intercept, receive, or use this data.

18 3. Best Buy

19 109. Best Buy Co., Inc. (“Best Buy”) is an American multinational consumer electronics
20 retailer, with 1,144 retail stores worldwide in 2022.¹⁸ For its 2022 and 2023 fiscal years, Best Buy
21 reported revenue of approximately \$51.8 billion and \$46.3 billion, respectively.¹⁹ Through Best
22 Buy’s website, located at www.bestbuy.com (the “Best Buy Website”), users are able to view,

23 ¹⁸ See *Best Buy Co., Inc., Continuing Operations—Number of Stores and Retail Square Footage*,
24 Best Buy, [https://s2.q4cdn.com/785564492/files/doc_earnings/2024/q1/earnings-result/Square-](https://s2.q4cdn.com/785564492/files/doc_earnings/2024/q1/earnings-result/Square-Footage-and-Store-Counts.pdf)
25 [Footage-and-Store-Counts.pdf](https://s2.q4cdn.com/785564492/files/doc_earnings/2024/q1/earnings-result/Square-Footage-and-Store-Counts.pdf) (last visited July 21, 2023).

26 ¹⁹ See *Best Buy reports Q4 FY23 results*, Best Buy, [https://corporate.bestbuy.com/best-buy-](https://corporate.bestbuy.com/best-buy-reports-q4-fy23-results/)
[reports-q4-fy23-results/](https://corporate.bestbuy.com/best-buy-reports-q4-fy23-results/) (last visited July 21, 2023).

1 place in their online shopping carts, and purchase products or items from Best Buy or “top-rated
2 sellers.”²⁰

3 110. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users’
4 data, including data related to their online shopping habits, when they visit the Best Buy Website.

5 **a. Version 90**

6 111. Unbeknownst to Version 90 users, when a Version 90 user browses the Best Buy
7 Website using Version 90 of Edge, Version 90 does each of the following:

- 8 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
9 user navigates to, including the URL for the page of each product or item the user
10 clicks on and views; and
- 11 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
12 the title, price, and description of each product a user clicks on as that information
13 appears on that product’s webpage.

14 This data collection occurs even when the user is utilizing an inPrivate window.

15 112. Together with the above-described data, Version 90 also collects and processes
16 unique user identifiers and/or cookies associated with the user. These include the user’s MUID
17 and impressionId. Version 90 also collects and processes the user’s User Agent Data as it collects,
18 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
19 his Microsoft Account. Defendant is able to link the above-described data to individual users
20 through their unique user identifiers and/or cookies, revealing to Defendant users’ identities and
21 online shopping activity. If a user was logged in to his Microsoft Account and not using an
22 inPrivate window when he browsed the Best Buy Website, Defendant can additionally utilize the
23 user’s WLS to link the user to the above-described data and identify the user, even if the user’s
24 MUID changes throughout the session because Version 90 “binds” it together with the user’s

25 ²⁰ See *Partner Portal*, Best Buy, <https://partners.bestbuy.com/canada/marketplace> (last visited
26 July 21, 2023).

1 MUID at the start of the user’s session. Defendant’s ability to identify users is further enhanced
2 by Version 90’s processing of User Agent Data.

3 113. Defendant uses the above-described private data for various purposes discussed
4 above.

5 114. Version 90 users, including Plaintiffs and the Class, are unaware that Version 90 is
6 collecting, intercepting, and sending the above-described private data to Defendant, and that
7 Defendant uses that data, and have not provided their consent, whether implied or express, for
8 Defendant to collect, intercept, receive, or use this data.

9 **b. Version 92**

10 115. Unbeknownst to Version 92 users, when a Version 92 user browses the Best Buy
11 Website using Version 92 of Edge, Version 92 does each of the following:

- 12 • **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms
13 entered by the user into the integrated search bar on the Best Buy Website
14 regardless of whether a user is utilizing an inPrivate window. However, search
15 terms are not collected, intercepted, and sent to Microsoft if a user is not logged
16 into his Microsoft account;
- 17 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
18 user navigates to, including the URL for the page of each product or item the user
19 clicks on and views;
- 20 • **Shopping Cart Contents:** Scrapes, collects, intercepts, and sends to the Bing
21 Server the URL and price of each product or item in the user’s shopping cart when
22 a user is utilizing an inPrivate window to browse the Best Buy website;
- 23 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
24 image (and URL for that image) of each product or item the user clicks and views
25 when a user is not utilizing an inPrivate to browse the Best Buy website; and
26

- 1 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
2 the title, and price of each product a user clicks on as that information appears on
3 that product's webpage when a user is not utilizing an inPrivate window to browse
4 the Best Buy website.

5 116. Together with the above-described data, Version 92 also collects and processes
6 unique user identifiers and/or cookies associated with the user. These include the user's MUID
7 and impressionId. Version 92 also collects and processes the user's User Agent Data as it collects,
8 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
9 his Microsoft Account. Defendant is able to link the above-described data to individual users
10 through their unique user identifiers and cookies, revealing to Defendant users' identity and online
11 shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate
12 window when he browsed the Walmart Website, Defendant can additionally utilize the user's
13 WLS, WLID, and X-Client-Data to link the user to the above-described data and identify the user,
14 even if some of those identifiers change throughout the session because Version 92 "binds" them
15 together with the user's MUID at the start of the user's session. Defendant's ability to identify
16 users is enhanced by Version 92's processing of User Agent Data.

17 117. Defendant uses the above-described private data for various purposes discussed
18 above.

19 118. Edge Version 92 users, including Plaintiffs and the Class, are unaware that Version
20 92 is collecting, intercepting, and sending the above-described private data to Defendant, and that
21 Defendant uses that data, and have not provided their consent, whether implied or express, for
22 Defendant to collect, intercept, receive, or use this data.

23 **c. Version 93**

24 119. Unbeknownst to Version 93 users, when a Version 93 user browses the Best Buy
25 Website using Version 93 of Edge, Version 93 does each of the following:
26

- 1 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
2 user navigates to, including the URL for the page of each product or item the user
3 clicks on and views;
- 4 • **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server the
5 title, price, quantity, image URL (and therefore the ability to view the image), and
6 URL for each product or item in the user’s shopping cart;
- 7 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
8 image (and URL for that image) of each product or item the user clicks and views;
9 and
- 10 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
11 the price and description of each product a user clicks on as that information
12 appears on that product’s webpage.

13 This data collection occurs even when the user is utilizing an inPrivate window.

14 120. Together with the above-described data, Version 93 also collects and processes
15 unique user identifiers and/or cookies associated with the user. These include the user’s MUID
16 and impressionId. Version 93 also collects and processes the user’s User Agent Data as it collects,
17 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
18 his Microsoft Account. Defendant is able to link the above-described data to individual users
19 through their unique user identifiers and cookies, revealing to Defendant users’ identity and online
20 shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate
21 window when he browsed the Best Buy Website, Defendant can additionally utilize the user’s
22 WLS and WLID to link the user to the above-described data and identify the user, even if the
23 WLID changes throughout the session because Version 93 “binds” them together with the user’s
24 MUID at the start of the user’s session. Defendant’s ability to identify users is enhanced by
25 Version 93’s processing of User Agent Data.

1 121. Defendant uses the above-described private data for various purposes discussed
2 above.

3 122. Edge Version 93 users, including Plaintiffs and the Class, are unaware that Version
4 93 is collecting, intercepting, and sending the above-described private data to Defendant, and that
5 Defendant uses that data, and have not provided their consent, whether implied or express, for
6 Defendant to collect, intercept, receive, or use this data.

7 **4. Walmart**

8 123. Walmart Inc. (“Walmart”) is an American multinational retail corporation
9 operating more than 10,500 stores throughout the world.²¹ For its 2023 fiscal year, Walmart
10 reported revenue of \$611.3 billion.²² Through Walmart’s website, located at www.walmart.com
11 (the “Walmart Website”), users are able to view, place in their online shopping carts, and purchase
12 products or items from Walmart or other sellers.²³

13 124. Unbeknownst to users, Edge intercepts and collects, and users’ data, including data
14 related to their online shopping habits to Defendant, when they visit the Walmart Website.

15 **a. Version 90**

16 125. Unbeknownst to Version 90 users, when a Version 90 user browses the Walmart
17 Website using Version 90 of Edge, Version 90 does each of the following:

- 18 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
19 user navigates to, including the URL for the page of each product or item the user
20 clicks on and views;

21
22 ²¹ See *Location Facts*, Walmart, <https://corporate.walmart.com/about/location-facts> (last visited
23 July 21, 2023).

24 ²² See *Walmart Releases Q4 and FY23 Earnings*, Walmart,
25 <https://corporate.walmart.com/newsroom/2023/02/21/walmart-releases-q4-and-fy23-earnings> (last
26 visited July 21, 2023).

²³ See *Walmart Marketplace*, Walmart, <https://marketplace.walmart.com/> (last visited July 21,
2023).

- 1 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
2 image (and URL for that image) of each product or item the user clicks and views;
3 and
- 4 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
5 the title and price of each product a user clicks on as that information appears on
6 that product's webpage.

7 126. Together with the above-described data, Version 90 also collects and processes
8 unique user identifiers and/or cookies associated with the user. These include the user's MUID
9 and impressionId. Version 90 also collects and processes the user's User Agent Data as it collects,
10 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
11 his Microsoft Account. Defendant is able to link the above-described data to individual users
12 through their unique user identifiers and/or cookies, revealing to Defendant users' identities and
13 online shopping activity. If a user was logged in to his Microsoft Account and not using an
14 inPrivate window when he browsed the Walmart Website, Defendant can additionally utilize the
15 user's WLS to link the user to the above-described data and identify the user, even if the user's
16 MUID changes throughout the session because Version 90 "binds" it together with the user's
17 MUID at the start of the user's session. Defendant's ability to identify users is further enhanced
18 by Version 90's processing of User Agent Data.

19 127. Defendant uses the above-described private data for various purposes discussed
20 above.

21 128. Version 90 users, including Plaintiffs and the Class, are unaware that Version 90 is
22 collecting, intercepting, and sending the above-described private data to Defendant, and that
23 Defendant is using that data, and have not provided their consent, whether implied or express, for
24 Defendant to collect, intercept, receive. or use this data.

1 **b. Version 92**

2 129. Unbeknownst to Version 92 users, when a Version 92 user browses the Walmart
3 Website using Version 92 of Edge, Version 92 does each of the following:

- 4 • **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms
5 entered by the user into the integrated search bar on the Walmart Website if a user
6 is utilizing an inPrivate window;
 - 7 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
8 user navigates to, including the URL for the page of each product or item the user
9 clicks on and views;
 - 10 • **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server the
11 title, price, and quantity for each product or item in the user’s shopping cart when a
12 user is not utilizing an inPrivate to browse the Walmart website. When a user is
13 utilizing an inPrivate window, Version 92 scrapes, collects, intercepts, and sends to
14 the Bing Server the price of the products in the user’s shopping cart;
 - 15 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server
16 the content of the reviews left by other users for each product or item the user
17 clicks on and views when a user is not utilizing an inPrivate to browse the Walmart
18 website;
 - 19 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
20 image (and URL for that image) of each product or item the user clicks and views
21 when a user is not utilizing an inPrivate to browse the Walmart website; and
 - 22 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
23 the title, price, and description of each product a user clicks on as that information
24 appears on that product’s webpage when a user is not utilizing an inPrivate window
25 to browse the Walmart website.
- 26

1 130. Together with the above-described data, Version 92 also collects and processes
2 unique user identifiers and/or cookies associated with the user. These include the user’s MUID
3 and impressionId. Version 92 also collects and processes the user’s User Agent Data as it collects,
4 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
5 his Microsoft Account. Defendant is able to link the above-described data to individual users
6 through their unique user identifiers and cookies, revealing users’ identity and online shopping
7 activity to Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate
8 window when he browsed the Walmart Website, Defendant can additionally utilize the user’s
9 WLS, WLID, and X-Client-Data to link the user to the above-described data and identify the user,
10 even if some of those identifiers change throughout the session because Version 92 “binds” them
11 together with the user’s MUID at the start of the user’s session. Defendant’s ability to identify
12 users is enhanced by Version 92’s processing of User Agent Data.

13 131. Defendant uses the above-described private data for various purposes discussed
14 above.

15 132. Edge Version 92 users, including Plaintiffs and the Class, are unaware that Version
16 92 is collecting, intercepting, and sending the above-described private data to Defendant, and that
17 Defendant uses that data, and have not provided their consent, whether implied or express, for
18 Defendant to collect, intercept, receive, or use this data.

19 **c. Version 93**

20 133. Unbeknownst to Version 93 users, when a Version 93 user browses the Walmart
21 Website using Version 93 of Edge, Version 93 does each of the following:

- 22 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
23 user navigates to, including the URL for the page of each product or item the user
24 clicks on and views;

- 1 • **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server the
2 title, price, quantity, the image URL (and therefore the ability to view the image),
3 and URL for each product or item in the user’s shopping cart;
- 4 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
5 image URL (and therefore the ability to view the image) of each product or item
6 the user clicks and views. If the user is not utilizing an inPrivate window, Version
7 93 also scrapes, collects, intercepts, and sends to the Bing Server the image of each
8 product or item the user clicks and views; and
- 9 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
10 the price and description of each product a user clicks on as that information
11 appears on that product’s webpage.

12 With the exception noted above relating to product or item images, this data collection occurs even
13 when the user is utilizing an in Private window.

14 134. Together with the above-described data, Version 93 also collects and processes
15 unique user identifiers and/or cookies associated with the user. These include the user’s MUID
16 and impressionId. Version 93 also collects and processes the user’s User Agent Data as it collects,
17 intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to
18 his Microsoft Account. Defendant is able to link the above-described data to individual users
19 through their unique user identifiers and cookies, revealing users’ identity and online shopping
20 activity to Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate
21 window when he browsed the Walmart Website, Defendant can additionally utilize the user’s
22 WLS and WLID to link the user to the above-described data and identify the user, even if the
23 WLID changes throughout the session because Version 93 “binds” them together with the user’s
24 MUID at the start of the user’s session. Defendant’s ability to identify users is enhanced by
25 Version 93’s processing of User Agent Data.

1 135. Defendant uses the above-described private data for various purposes discussed
2 above.

3 136. Edge Version 93 users, including Plaintiffs and the Class, are unaware that Version
4 93 is collecting, intercepting, and sending the above-described private data to Defendant, and that
5 Defendant uses that data, and have not provided their consent, whether implied or express, for
6 Defendant to collect, intercept, receive, or use this data.

7 **5. Earlier and Later Versions of Edge**

8 137. On information and belief, as with Versions 90, 92, and 93, and unbeknownst to
9 users, when users of earlier and later versions of Edge browse the Amazon, eBay, Best Buy, and
10 Walmart Websites, those versions of the Edge Browser collect, intercept, and send to the Bing
11 Server and/or SmartScreen Server a wide range of data relating to users' online shopping habits on
12 those websites and link that data with unique user identifiers and cookies (including MUID and X-
13 Client-Data) without users' knowledge or consent. By linking users' unique user identifiers and
14 User Agent Data with the collected data regarding users' online shopping activities, Defendant is
15 able to identify individual users and associate them with the specific items they browsed or
16 purchased as well as with their online shopping habits more broadly. The intercepted data
17 includes at least some of the same categories of data as those collected by Versions 90, 92, and 93.

18 138. Defendant uses the above-described private data for various purposes discussed
19 above.

20 139. Users of earlier and later versions of Edge, including Plaintiffs and the Class, are
21 unaware that those versions are collecting, intercepting, and sending the above-described private
22 data to Defendant, and that Defendant uses that data, and have not provided their consent, whether
23 implied or express, for Defendant to collect, intercept, receive, or use this data.

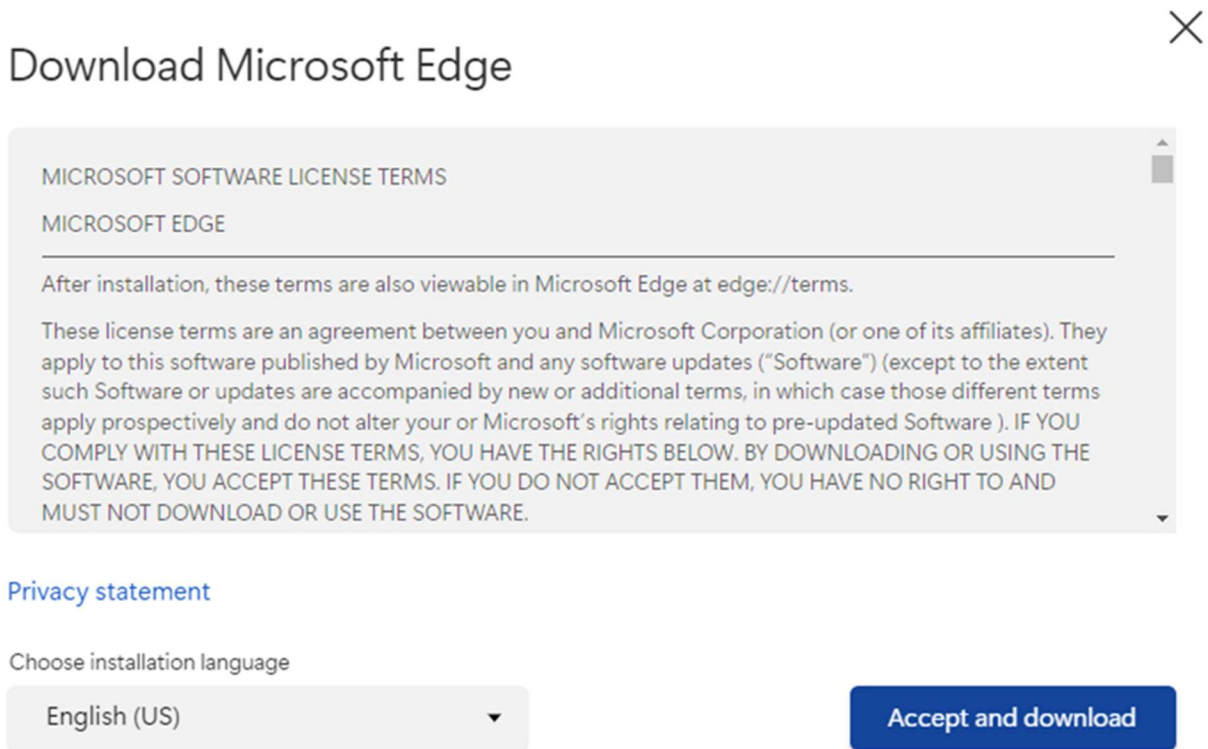
1 **I. Microsoft Does Not Disclose Edge’s Data Collection Practices to Users, and Users Are**
2 **Not Given Adequate Legal Notice of Microsoft’s Privacy Policy**

3 140. Many Microsoft Edge users have the Edge browser embedded into their computer
4 because it came that way: pre-installed within the Windows Operating System. Quintessential
5 examples include: a college or law student who buys a laptop at her school bookstore with *Office*
6 *Home & Student* preinstalled; a white-collar worker given a company-owned laptop by her
7 employer with, for example, *Microsoft Office* preinstalled; government employees who operate
8 Microsoft products paid for by United States’ taxpayers. These illustrative examples are a tiny
9 subset of the massive swath of Microsoft’s user base who are not presented with *any* separate
10 notice relating to Microsoft Edge’s highly intrusive data collection practices.

11 141. Nor would any user of Edge who borrows a device, *e.g.*, a sibling or a roommate of
12 the device owner, be presented with any disclosure or link to any Microsoft policy or agreement.
13 Such users are given no notice of Microsoft’s Privacy Policy.

14 142. While many Edge users have Edge forced upon them—embedded as the default
15 browser within a larger package of software that they actually need (like Microsoft Word), a far
16 smaller number of users actually seek Edge out and download the software on its own. As of
17 2023, for those standalone Edge users, the Privacy Statement that purportedly goes along with it is
18 not conspicuously, immediately or directly presented. Instead, the user must search for it, and
19 then press a separate link to access it. *See Image 1, below.*

Image 1:



143. Also, during the Edge download process, users are presented with a window that shows only the beginning of Microsoft's Software License Terms. See Image 1.

144. Users need not scroll through the full Software License Terms to download Edge, however. In fact, users need not scroll through the Software License Terms or press the link to the Privacy Statement: they can just download Edge by clicking the blue button depicted below without scrolling through or clicking on anything. See Image 2.

Image 2:

Download Microsoft Edge

limitation or exclusion may not apply to you because your state, province, or country may not allow the exclusion or limitation of incidental, consequential, or other damages.

Source code for portions of Microsoft Edge is available free of charge from <https://thirdpartysource.microsoft.com> under the third party open source license terms provided at <https://aka.ms/thirdpartynotices> and in Microsoft Edge at `edge://credits` after installation. Or to obtain this source code you may send a check or money order for US \$5.00, including the Edge version number, to:

Source Code Compliance Team
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Privacy statement

Choose installation language

English (US)

Accept and download

145. Upon information and belief, previous versions of Microsoft’s Privacy Statement were presented in an even less conspicuous manner and did not provide adequate legal notice to users about Edge’s data collection practices. Upon information and belief, previous versions of the Software License Terms also were presented in an even less conspicuous manner.

146. Edge users who did not personally or individually download Edge, as well as Edge users who are minors are similarly not provided adequate legal notice regarding Defendant’s data collection practices in relation to the users’ use of the Edge browser.

J. Plaintiffs and the Class’s Personal Information Has Value

147. The value of personal data is well understood and generally accepted as a form of currency.

148. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

1 149. The robust market for user data has been analogized to the “oil” of the tech
2 industry.²⁴ A 2015 article from TechCrunch accurately noted that “Data has become a strategic
3 asset that allows companies to acquire or maintain a competitive edge.”²⁵ That article noted that
4 the value of a single Internet user—or really, a single user’s data—varied from about \$15 to more
5 than \$40.

6 150. The Organization for Economic Cooperation and Development (“OECD”) itself
7 has published numerous volumes discussing how to value data such as that which is the subject
8 matter of this Complaint, including as early as 2013, with its publication “Exploring the Economic
9 of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”²⁶ The OECD
10 recognizes that data is a key competitive input not only in the digital economy but in all markets:
11 “Big data now represents a core economic asset that can create significant competitive advantage
12 for firms and drive innovation and growth.”²⁷

13 151. In *The Age of Surveillance Capitalism*, Harvard Business School Professor
14 Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have
15 transformed their business models from fee-for-services-provided to monetizing their users’
16 data—including user data that is not necessary for product or service use, which she refers to as
17 “behavioral surplus.”²⁸ In essence, Professor Zuboff explains that revenue from user Internet data

18
19 ²⁴ *The world’s most valuable resource is no longer oil, but data*, *The Economist* (May 6, 2017),
20 <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

21 ²⁵ Pauline Glickman and Nicolas Glady, *What’s the Value of Your Data?* TechCrunch (Oct. 13,
22 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

23 ²⁶ *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring
24 Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013),
25 <http://dx.doi.org/10.1787/5k486qtxldmq-en>.

26 ²⁷ *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct.
13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en.

²⁸ SHOSHANNA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 166 (2019).

1 pervades every economic transaction in the modern economy. It is a fundamental assumption of
2 these revenues that there is a *market* for this data; data generated by Internet users using Versions
3 90, 92, 93, and earlier and later versions of the Edge Browser has economic value.

4 152. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes:

5 Personal information is an important currency in the new millennium.
6 The monetary value of personal data is large and still growing, and
7 corporate America is moving quickly to profit from the trend. Companies
8 view this information as a corporate asset and have invested heavily in
9 software that facilitates the collection of consumer information.²⁹

10 153. This economic value has been leveraged largely by corporations who pioneered the
11 methods of its extraction, analysis, and use. However, the data also has economic value to Internet
12 users. Market exchanges have sprung up where individual users like Plaintiffs can sell or
13 monetize their own data. For example, Nielsen Data and Mobile Computer will pay users for their
14 data.³⁰ Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with
15 the app.³¹

16 154. There are countless examples of this kind of market, which is growing more robust
17 as information asymmetries are diminished when users discover how their data is being covertly
18 intercepted, collected, and used.

19 155. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article “The
20 Economics of Privacy,” published in the *Journal of Economic Literature*:

21 Such vast amounts of collected data have obvious and substantial
22 economic value. Individuals’ traits and attributes (such as a person’s age,
23 address, gender, income, preferences, and reservation prices, but also her
24 clickthroughs, comments posted online, photos uploaded to social media,
25

26 ²⁹ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

³⁰ Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10, 2020), <https://wallethacks.com/apps-for-selling-your-data/>.

³¹ Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch videos*, The Verge (May 29, 2020), <https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival>.

1 and so forth) are increasingly regarded as business assets that can be used
2 to target services or offers, provide relevant advertising, or be traded with
3 other parties.³²

4 156. There is also a private market for users' personal information. While there is a
5 wide range in values, the prices are nonetheless significant. For example:

- 6 • "Each piece of personal info has a price tag. A Social Security number
7 may sell for as little as \$1. Credit card, debit card and banking info can go
8 for as much as \$110. Usernames and passwords for non-financial
9 institution logins are \$1, but it can range from \$20 to \$200 for login info
10 for online payment platforms."³³
- 11 • "Researchers pored through the prices of personal data and information—
12 called 'fullz' by those searching for 'full credentials'—that are available
13 for sale on nearly 50 different Dark Web marketplaces, finding that Japan,
14 the UAE, and EU countries have the most expensive identities available at
15 an average price of \$25."³⁴
- 16 • "According to Comparitech, who researched the prices of stolen credit
17 cards, hacked PayPal accounts, and private Social Security numbers on
18 more than 40 different dark web marketplaces, the average price of each
19 U.S. citizen's "fullz," or complete information including name, date of
20 birth, address, phone number, account numbers and other information is
21 \$8."³⁵

22 ³² Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. OF
23 ECON. LITERATURE 2, 444 (June 2016),
24 <https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf>.

25 ³³ *Understanding the Illegal Market for Personal Information*, OnPoint Community Credit
26 Union, <https://www.onpointcu.com/blog/understanding-the-illegal-market-for-personal-information/#:~:text=Each%20piece%20of%20personal%20info,info%20for%20online%20payment%20platforms.>

³⁴ Jonathan Greig, *How much is your info worth on the Dark Web? For Americans, it's just \$8*,
TechRepublic, <https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/>.

³⁵ *There's Value in Everything: Stop Underestimating the Value of Your Data on the Black Market*, Virtually Managed IT Solutions LLC, <https://vmits.com/theres-value-in-everything-stop-underestimating-the-value-of-your-data-on-the-black-market/>.

1 157. These rates are assumed to be discounted because they do not operate in
2 competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users'
3 content, surely users can sell their own.

4 158. In short, there is a quantifiable economic value to Internet users' data that is greater
5 than zero. The exact number will be a matter for experts to determine.

6 **K. Plaintiffs and Class and Subclass Members Suffered an Economic Injury**

7 159. Property is the right of any person to possess, use, enjoy, or dispose of a thing,
8 including intangible things such as data or communications.

9 160. California courts have recognized the lost "property value" of personal information.
10 Recent changes in California law have also confirmed that individuals have a property interest in
11 their information. In 2018, California enacted the California Consumer Privacy Act ("CCPA").
12 Among other things, the CCPA permits businesses to purchase consumer information from
13 consumers themselves (Cal. Civ. Code § 1798.125(b)(1)) and permits businesses to assess and
14 appraise – *i.e.*, to place a monetary value on – consumer data (Cal. Civ. Code § 1798.125(a)(2)).

15 161. Accordingly, Plaintiffs' and Class and Subclass members' private data described
16 herein is property under California law.

17 162. Defendant's interception, collection, and use of Plaintiffs' and Class and Subclass
18 members' private data described herein without authorization is a taking of Plaintiffs' and Class
19 and Subclass members' property. Plaintiffs and Class and Subclass members have a right to
20 disgorgement and/or restitution damages for the value of the improperly collected private data
21 described herein by Defendant through Versions 90, 92, 93, and earlier and later versions of the
22 Edge browser.

23 163. Plaintiffs and Class and Subclass members have suffered benefit of the bargain
24 damages, in that Defendant took more data than authorized. Those benefit of the bargain damages
25 also include, but are not limited to (i) loss of the promised benefits of their experience using
26 Versions 90, 92, 93, and earlier and later versions of the Edge browser to browse the internet; (ii)

1 loss of the promised benefits of their experience on the websites they visited using Versions 90,
2 92, 93, and earlier and later versions of the Edge browser from which those versions of the Edge
3 Browser collected their private data; (ii) out-of-pocket costs; and (iii) loss of control over property
4 which has marketable value.

5 164. To preserve their privacy, Plaintiffs and Class and Subclass members who now
6 understand at least some of Defendant's violations are presented with the choice of (i) reducing or
7 ending their use of Versions 90, 92, 93, and earlier and later versions of the Edge browser; or (ii)
8 knowingly accepting less privacy than they were promised. Each of these options deprives
9 Plaintiffs and Class and Subclass members of the benefits of their original bargain. There is no
10 option that recovers the property improperly intercepted and collected by Defendant.

11 165. Further, Plaintiffs and Class and Subclass members were denied the benefit of
12 knowing that Defendant was intercepting and collecting their private data described herein. Thus,
13 they were unable to mitigate the harms they incurred because of Defendant's actions. That is,
14 Defendant's lack of transparency prevented and still prevents Plaintiffs' and Class and Subclass
15 members' ability to mitigate the harms.

16 166. Defendant avoided costs they should have incurred because of its actions—had it
17 transparently disclosed its actions, it would have suffered losses stemming from the loss of user
18 engagement with Versions 90, 92, 93, and earlier and later versions of the Edge browser. Warning
19 users would have chilled engagement on Versions 90, 92, 93, and earlier and later versions of the
20 Edge browser as well as discouraged potential new users, and thus chilled use of Versions 90, 92,
21 93, and earlier and later versions of the Edge browser.

22 167. Defendant thus was not only able to evade or defer these costs, but it was able to
23 continue to accrue value and further benefit from the delay due to the time value of money.
24 Defendant has thus transferred all of the costs imposed by the unauthorized interception and
25 collection of users' private data described herein onto Plaintiffs and Class and Subclass members.
26 Defendant increased the cost to Plaintiffs and Class and Subclass members of mitigating the

1 interception and collection of their private data described herein by failing to notify them that
2 Defendant was intercepting and collecting Plaintiffs' and Class and Subclass members' private
3 data described herein.

4 168. In addition, Plaintiffs and Class and Subclass members have suffered from the
5 diminished value of their own private data described herein, which is property that has both
6 personal and economic value to Plaintiffs and Class and Subclass members.

7 169. Plaintiffs' and Class and Subclass members' private data described herein have
8 different forms of value. First, there is transactional, or barter, value. Indeed, Defendant has
9 traded (i) the ability to use Versions 90, 92, 93, and earlier and later versions of the Edge Browser
10 in exchange for (ii) the collection and use of Plaintiffs' and Class and Subclass members' private
11 data described herein—all while concealing the extent to which this information would be
12 intercepted, collected, and used.

13 170. Second, Plaintiffs' and Class and Subclass members' property, which has economic
14 value, was taken from them without their consent. There is a market for the private data described
15 herein, and it has at minimum a value greater than zero. Plaintiff and Class and Subclass members
16 cannot bring their private data described herein to market because Defendant's improper
17 interception, collection, and use of that private data for various reasons, including, but not limited
18 to, improving its software, services, and devices, providing targeted advertising, and developing
19 its sophisticated artificial intelligence and machine-learning systems means that Plaintiff's and
20 Class and Subclass members' private data described herein is no longer needed or marketable for
21 that purpose.

22 171. Third, in addition to the monetary value of selling their data, Plaintiff and Class and
23 Subclass members also assign value to keeping their private data described herein private. It is
24 possible to quantify this privacy value, which is destroyed when Defendant intercepts and collects
25 Plaintiffs' and Class and Subclass members' private data described herein without notice or
26 authorization.

1 172. Plaintiffs and Class and Subclass members were harmed when Defendant took their
2 property and exerted exclusive control over it, intercepting and collecting it without Plaintiffs' and
3 Class and Subclass members' knowledge to benefit Defendant and, additionally, for still
4 undisclosed purposes.

5 173. Further, Defendant's control over these ever-expanding digital dossiers makes
6 tracking and profiling Plaintiffs and Class and Subclass members, and targeting them with
7 advertising, much more efficient and effective. Defendant unjustly earn substantial profits from
8 such targeted advertising and/or from the sale of user data and/or information or services derived
9 from such data.

10 174. In sum, Defendant has intercepted and collected Plaintiffs' and Class and Subclass
11 members' private data described herein without providing anything of value to Plaintiffs and Class
12 and Subclass members in exchange for that private data. Moreover, Defendant's unauthorized
13 access to Plaintiffs' and Class and Subclass members' private data described herein has
14 diminished the value of that private data. These actions and omissions by Defendant have resulted
15 in harm to Plaintiffs and Class and Subclass members.

16 **L. Microsoft Intercepted, Collected, and Used Plaintiffs' Private Data**

17 175. Defendant's unauthorized interception, collection, and use of Plaintiffs' private
18 data described herein resulted in the diminished value of that private content.

19 176. Plaintiff Saeedy has consistently used Edge since at least June of 2021 for both
20 personal and work purposes. Specifically, Saeedy used the various versions of Edge to shop on
21 Amazon and eBay's websites. Accordingly, Defendant's unlawful data collection practices
22 through Versions 90, 92, 93, and earlier and later versions of Edge have resulted in the
23 unauthorized interception, collection, and sharing of Plaintiff Saeedy's private data described
24 herein. By associating the collected data with Saeedy's unique user identifiers and cookies,
25 Defendant was and is able to determine his precise internet browsing activities and habits.
26 Defendant thus utilized and configured the SmartScreen and Bing servers to transmit Plaintiff

1 Saeedy's personally identifiable information without his express or implied consent. Defendant
2 used Plaintiff Saeedy's private data for various purposes, including, but not limited to, improving
3 its software, services, and devices, providing targeted advertising, and developing its sophisticated
4 artificial intelligence and machine-learning systems.

5 177. Plaintiff Shah has consistently used Edge since at least June of 2021 on a computer
6 provided by an employer or workplace. Specifically, Shah used the various versions of Edge to
7 shop on Amazon and BestBuy's websites. Accordingly, Defendant's unlawful data collection
8 practices through Versions 90, 92, 93, and earlier and later versions of Edge have resulted in the
9 unauthorized interception, collection, and sharing of Plaintiff Shah's keyword search terms and
10 URLs visited. By associating the collected data with Shah's unique user identifiers and cookies,
11 Defendant was and is able to determine his precise internet browsing activities and habits.
12 Defendant thus utilized and configured the SmartScreen and Bing servers to transmit Plaintiff
13 Shah's personally identifiable information without his express or implied consent. Defendant used
14 Plaintiff Shah's private data for various purposes, including, but not limited to, improving its
15 software, services, and devices, providing targeted advertising, and developing its sophisticated
16 artificial intelligence and machine-learning systems.

17 178. Minor Plaintiff M.S. has consistently used Edge since at least June of 2021 for
18 personal purposes. Specifically, M.S. used the various versions of Edge to shop on Amazon and
19 access Google and Yahoo search engines. Accordingly, Defendant's unlawful data collection
20 practices through Versions 90, 92, 93, and earlier and later versions of Edge have resulted in the
21 unauthorized interception, collection, and sharing of Plaintiff M.S.'s keyword search terms and
22 URLs visited. By associating the collected data with M.S.'s unique user identifiers and cookies,
23 Defendant was and is able to determine M.S.'s precise internet browsing activities and habits.
24 Defendant thus utilized and configured the SmartScreen and Bing servers to transmit Plaintiff
25 M.S.'s personally identifiable information without M.S.'s express or implied consent. Defendant
26 used Plaintiff M.S.'s private data for various purposes, including, but not limited to, improving its

1 software, services, and devices, providing targeted advertising, and developing its sophisticated
2 artificial intelligence and machine-learning systems.

3 179. Plaintiff Wilkinson has consistently used Edge since at least June of 2021 on a
4 computer provided by an academic institution. Specifically, Wilkinson used the various versions
5 of Edge to shop on third-party websites and access Google and Yahoo search engines.
6 Accordingly, Defendant's unlawful data collection practices through Versions 90, 92, 93, and
7 earlier and later versions of Edge have resulted in the unauthorized interception, collection, and
8 sharing of Plaintiff Wilkinson's keyword search terms and URLs visited. By associating the
9 collected data with Wilkinson's unique user identifiers and cookies, Defendant was and is able to
10 determine her precise internet browsing activities and habits. Defendant thus utilized and
11 configured the SmartScreen and Bing servers to transmit Plaintiff Wilkinson's personally
12 identifiable information without her express or implied consent. Defendant used Plaintiff
13 Wilkinson's private data for various purposes, including, but not limited to, improving its
14 software, services, and devices, providing targeted advertising, and developing its sophisticated
15 artificial intelligence and machine-learning systems.

16 V. TOLLING, CONCEALMENT, AND ESTOPPEL

17 180. Any applicable statutes of limitations have been tolled under (1) the fraudulent
18 concealment doctrine, based on Defendant's knowing and active concealment and denial of the
19 conduct alleged herein and (2) the delayed discovery doctrine, as Plaintiffs and Class and Subclass
20 members did not and could not reasonably have discovered Defendant's conduct alleged herein
21 until shortly before the Complaint was filed.

22 181. Defendant did not adequately disclose that it would intercept, collect, and use their
23 private data described herein when users' used the Edge browser generally or that Defendant
24 would still intercept, collect, and use their private data described herein even when the user
25 followed Defendant's instructions on how to browse privately using an "inPrivate" window.
26

1 182. Moreover, Defendant’s labeling of the relevant products’ “Private Mode” as a
2 “InPrivate” window is, in and of itself, misleading absent clear disclosures about the ways in
3 which Defendant intercepts, collects, and uses users’ private data. Indeed, “private” is commonly
4 defined and understood as “not known or intended to be known publicly: secret.”³⁶ However, as
5 alleged above, Microsoft Edge takes user information even when they are browsing the internet
6 with Edge’s “InPrivate” window.

7 183. Plaintiffs and Class and Subclass members did not discover and could not
8 reasonably have discovered, that Defendant was intercepting and using their data in the ways set
9 forth in this Complaint until shortly before the lawsuit was filed .

10 184. Plaintiffs and Class and Subclass members exercised reasonable diligence to
11 protect their data from interception. Indeed, that is precisely the reason why they used
12 Defendant’s “InPrivate” browsing window. Yet Plaintiffs did not and could not reasonably have
13 discovered their claims until consulting with counsel shortly before the filing of this Complaint
14 through the exercise of reasonable diligence.

15 185. Accordingly, Plaintiffs and the Class and Subclass members could not have
16 reasonably discovered the truth about Defendant’s practices until shortly before Plaintiffs
17 commenced this class litigation. .

18 186. Defendant is therefore estopped from relying on any statute of limitations.

19 VI. CLASS ALLEGATIONS

20 187. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rule of Civil
21 Procedure on behalf of the following Class and Subclasses:

22 Nationwide Class (the “Class”): All persons residing in the United States
23 who used Microsoft’s Edge browser to browse, enter keyword searches,
24 or visit URLs and whose communications, including personal

25 ³⁶ *Private*, Merriam-Webster, [https://www.merriam-](https://www.merriam-webster.com/dictionary/private#:~:text=%3A%20not%20known%20or%20intended%20to,withdr)
26 [webster.com/dictionary/private#:~:text=%3A%20not%20known%20or%20intended%20to,withdr](https://www.merriam-webster.com/dictionary/private#:~:text=%3A%20not%20known%20or%20intended%20to,withdr)
[awn%20from%20company%20or%20observation](https://www.merriam-webster.com/dictionary/private#:~:text=%3A%20not%20known%20or%20intended%20to,withdr) (last visited July 21, 2023).

1 information, online browsing activity, key word searches, or visited
2 URLs, Defendant intercepted, received, or collected from July 29, 2015
through the present (the “Class Period”).

3 Nationwide Business Subclass: All persons residing in the United States
4 who used Microsoft’s Edge browser to browse, enter keyword searches,
5 or visit URLs via a device provided by an employer or workplace that
6 came with the Edge browser pre-downloaded and whose
7 communications, including personal information, online browsing
8 activity, key word searches, or visited URLs, Defendant intercepted,
9 received, or collected during the Class Period.

10 Nationwide Academic Subclass: All persons residing in the United States
11 who used Microsoft’s Edge browser to browse, enter keyword searches,
12 or visit URLs via a device provided by an academic institution that came
13 with the Edge browser pre-downloaded and whose communications,
14 including personal information, online browsing activity, key word
15 searches, or visited URLs, Defendant intercepted, received, or collected
16 during the Class Period.

17 Nationwide Shared Devices Subclass: All persons residing in the United
18 States who used Microsoft’s Edge browser to browse, enter keyword
19 searches, or visit URLs on a shared or public device that they personally
20 did not download the Edge browser onto and whose communications,
21 including personal information, online browsing activity, key word
22 searches, or visited URLs, Defendant intercepted, received, or collected
23 during the Class Period.

24 Nationwide Minor Subclass: All persons residing in the United States
25 who, while under 18 years of age, used Microsoft’s Edge browser to
26 browse, enter keyword searches, or visit URLs and whose
communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
received, or collected during the Class Period.

California Class (the “California Class”): All persons residing in the
State of California who used Microsoft’s Edge browser to browse, enter
keyword searches, or visit URLs and whose communications, including
personal information, online browsing activity, key word searches, or
visited URLs, Defendant intercepted, received, or collected from during
the Class Period.

California Business Subclass: All persons residing in the State of
California who used Microsoft’s Edge browser to browse, enter keyword
searches, or visit URLs via a device provided by an employer or

1 workplace that came with the Edge browser pre-downloaded and whose
2 communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
3 received, or collected during the Class Period.

4 California Academic Subclass: All persons residing in the State of
California who used Microsoft’s Edge browser to browse, enter keyword
5 searches, or visit URLs via a provided by an academic institution that
came with the Edge browser pre-downloaded and whose
6 communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
7 received, or collected during the Class Period.

8 California Shared Devices Subclass: All persons residing in the State of
9 California who used Microsoft’s Edge browser to browse, enter keyword
searches, or visit URLs on a shared or public device that they personally
10 did not download the Edge browser onto and whose communications,
including personal information, online browsing activity, key word
11 searches, or visited URLs, Defendant intercepted, received, or collected
during the Class Period.

12 California Minor Subclass: All persons residing in the State of California
13 who, while under 18 years of age, used Microsoft’s Edge browser to
browse, enter keyword searches, or visit URLs and whose
14 communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
15 received, or collected during the Class Period.

16 Washington Class (the “Washington Class”): All persons residing in the
17 State of Washington who used Microsoft’s Edge browser to browse,
enter keyword searches, or visit URLs and whose communications,
18 including personal information, online browsing activity, key word
searches, or visited URLs, Defendant intercepted, received, or collected
19 during the Class Period.

20 Washington Business Subclass: All persons residing in the State of
21 Washington who used Microsoft’s Edge browser to browse, enter
keyword searches, or visit URLs via a device provided by an employer or
22 workplace that came with the Edge browser pre-downloaded and whose
communications, including personal information, online browsing
23 activity, key word searches, or visited URLs, Defendant intercepted,
24 received, or collected during the Class Period.

25 Washington Academic Subclass: All persons residing in the State of
26 Washington who used Microsoft’s Edge browser to browse, enter

1 keyword searches, or visit URLs via a device provided by an academic
2 institution that came with the Edge browser pre-downloaded and whose
3 communications, including personal information, online browsing
4 activity, key word searches, or visited URLs, Defendant intercepted,
5 received, or collected during the Class Period.

6 Washington Shared Devices Subclass: All persons residing in the State
7 of Washington who used Microsoft's Edge browser to browse, enter
8 keyword searches, or visit URLs on a shared or public device that they
9 personally did not download the Edge browser onto and whose
10 communications, including personal information, online browsing
11 activity, key word searches, or visited URLs, Defendant intercepted,
12 received, or collected during the Class Period.

13 Washington Minor Subclass: All persons residing in the State of
14 Washington who, while under 18 years of age, used Microsoft's Edge
15 browser to browse, enter keyword searches, or visit URLs and whose
16 communications, including personal information, online browsing
17 activity, key word searches, or visited URLs, Defendant intercepted,
18 received, or collected during the Class Period.

19 188. Excluded from the Classes and Subclasses are: (1) the Court (including any judge
20 or magistrate presiding over this action and any members of their families); (2) Defendant, its
21 subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of
22 them have a controlling interest and its officers, directors, employees, affiliates, legal
23 representatives; (3) persons who properly execute and file a timely request for exclusion from the
24 Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or
25 otherwise released; (5) Plaintiffs' counsel, Class counsel and Defendant's counsel; and (6) the
26 legal representatives, successors, and assigns of any such excluded persons.

189. **Numerosity**: The Class and Subclass members are so numerous that joinder of all
members is impracticable. The precise number of Class and Subclass members is unknown to
Plaintiffs at this time but is believed to consist of millions of individuals who can be identified
through Defendant's records.

190. **Typicality**: Plaintiffs' claims are typical of the claims of the Class and Subclass
members, who are similarly affected by Defendant's wrongful conduct in violation of the laws

1 complained of herein. The claims of Plaintiffs and the members of the Class and Subclasses arise
2 from the same conduct by Defendant and are based on the same legal theories. Defendant acted or
3 refused to act on grounds generally applicable to the Class and Subclasses, and Defendant’s
4 policies and practices challenged herein apply equally and uniformly to each Class and Subclass
5 member, including Plaintiffs. Plaintiffs do not have any interest that is in conflict with the
6 interests of the Class or Subclass members.

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

11 a. Whether Defendant represented that Class and Subclass members could
12 control what communications of user information, browsing history and web activity data were
13 intercepted, received, or collected by Defendant;

14 b. Whether Defendant gave the Class and Subclass members a reasonable
15 expectation of privacy that their communications of user information, browsing history and web
16 activity data were not being intercepted, received, or collected by Defendant when the Class or
17 Subclass member was using a browser while in “Private Mode”;

18 c. Whether Defendant in fact intercepted, received, or collected
19 communications of user information, browsing history and web activity from Class and Subclass
20 members when the Class and Subclass members were using a browser while in “Private Mode”;

21 d. Whether Defendant’s practice of intercepting, receiving, or collecting
22 communications of user information, browsing history and web activity violated state and federal
23 privacy laws;

24 e. Whether Defendant’s practice of intercepting, receiving, or collecting
25 communications of user information, browsing history and web activity violated state and federal
26 anti-wiretapping laws;

1 f. Whether Defendant’s practice of intercepting, receiving, or collecting
2 communications of user information, browsing history and web activity violated any other state
3 and federal tort laws;

4 g. Whether Plaintiffs, Class, and Subclass members are entitled to declaratory
5 and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

6 h. Whether Plaintiffs, Class, and Subclass members have sustained damages as
7 a result of Defendant’s conduct and if so, what is the appropriate measure of damages or
8 restitution.

9 192. **Adequate Representation:** Plaintiffs have and will continue to fairly and
10 adequately represent and protect the interests of the Classes and Subclasses. Plaintiffs have
11 retained counsel competent and experienced in complex litigation and class actions, including
12 litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the
13 interests of the Classes and Subclasses, and Defendant has no defenses unique to any plaintiff.
14 Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the
15 members of the Classes and Subclasses, and they have the resources to do so. Neither Plaintiffs
16 nor their counsel have any interest adverse to the interests of the other members of the Classes and
17 Subclasses.

18 193. **Superiority:** A class action is superior to other available methods for the fair and
19 efficient adjudication of this controversy and joinder of all members of the Classes and Subclasses
20 is impracticable. This proposed class action presents fewer management difficulties than
21 individual litigation, and provides the benefits of single adjudication, economies of scale, and
22 comprehensive supervision by a single, able court. Class treatment will create economies of time,
23 effort, and expense and promote uniform decision-making. A class action is a particularly
24 efficient and appropriate procedure in this case because absent a class action Defendant would
25 gain an unconscionable economic advantage. Individual plaintiffs have limited resources and
26 could be outspent many times over by Defendant. Moreover, the recovery in each individual suit

1 would not cover the cost of litigation. Additionally, Defendant's course of conduct described
2 herein is common to each Class and Subclass member; maintaining individual actions would
3 create a risk of inconsistent results.

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

7 **VII. CHOICE OF LAW**

8 195. California substantive law applies to every member of the California Class and
9 California Subclasses. California substantive law may be constitutionally applied to the claims of
10 the California Plaintiffs, California Class, and California Subclasses under the Due Process
11 Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S.
12 Constitution. California has significant contact, or significant aggregation of contacts, to the
13 claims asserted by the California Plaintiffs and California Class and California Subclasses
14 members, thereby creating state interests to ensure that the choice of California state law is not
15 arbitrary or unfair.

16 196. Defendant conducts substantial business in California, such that California has an
17 interest in regulating Defendant's conduct under its laws. Defendant's decision to conduct
18 substantial business in California and avail itself of California's laws, renders the application of
19 California law to the claims herein constitutionally permissible.

20 197. The application of California law to the California Class and California Subclasses
21 is also appropriate under California and Washington's choice of law rules because California has
22 significant contacts to the claims of the California Plaintiffs and the proposed California Class and
23 California Subclasses, and California has a greater interest in applying its laws here than any other
24 interested state.

25 198. Washington substantive law applies to every member of the Washington Class and
26 Washington Subclasses. Washington substantive law may be constitutionally applied to the

1 claims of the Washington Plaintiff, Washington Class, and Washington Subclasses under the Due
2 Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S.
3 Constitution. Washington has significant contact, or significant aggregation of contacts, to the
4 claims asserted by the Washington Plaintiff and Washington Class and Washington Subclasses
5 members, thereby creating state interests to ensure that the choice of Washington state law is not
6 arbitrary or unfair.

7 199. Defendant conducts substantial business in Washington, such that Washington has
8 an interest in regulating Defendant's conduct under its laws. Defendant's decision to conduct
9 substantial business in Washington and avail itself of Washington's laws, renders the application
10 of Washington law to the claims herein constitutionally permissible.

11 200. The application of Washington law to the Washington Class and Washington
12 Subclasses is also appropriate under Washington's choice of law rules because Washington has
13 significant contacts to the claims of the Washington Plaintiff and the proposed Washington Class
14 and Washington Subclasses, and Washington has a greater interest in applying its laws here than
15 any other interested state.

16 **FIRST CAUSE OF ACTION**

17 **(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*)**

18 **(All Plaintiffs, Classes, and Subclasses Against MICROSOFT CORP.)**

19 201. Plaintiffs, the Classes, and Subclasses repeat and incorporate by reference all
20 preceding paragraphs as if fully set forth herein.

21 202. Plaintiffs, the Classes, and Subclasses' private data described herein that Defendant
22 intercepted, collected, and used includes contents of electronic communications that Plaintiffs, the
23 Classes, and Subclasses intended to convey to recipients.

24 203. Plaintiffs, the Classes, and Subclasses had a reasonable expectation of privacy in
25 their private data described herein as well as in the collection and processing of their unique user
26 identifiers and cookies in connection with that content.

1 204. However, Defendant intentionally intercepted, collected, and used the private data
2 described herein contained in communications and messages transmitted via the Microsoft Edge
3 browser, and collected and processed users' unique user identifiers and cookies in connection with
4 that data, without Plaintiffs', the Classes', or Subclasses' consent or knowledge.

5 205. Defendant owned and operated the Microsoft Edge browser. Defendant collected
6 and intercepted Plaintiffs', the Classes', and Subclasses' private data described herein through
7 Versions 90, 92, 93, and earlier and later versions of Edge. Defendant transmitted this data to the
8 SmartScreen and/or Bing servers. Defendant used that data for various purposes, including, but
9 not limited to, improving its software, services, and devices, providing targeted advertising, and
10 developing its sophisticated artificial intelligence and machine-learning systems.

11 206. By associating the collected data with the unique user identifiers and cookies,
12 Defendant can and does determine individual users' precise internet browsing activities and habits.
13 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions
14 of the Edge browser to collect and process users' unique user identifiers and cookies for this
15 purpose.

16 207. Defendant was actively involved in designing and programming the data flows for
17 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
18 interception and collection alleged herein, and promoted the use of the Edge browser to California,
19 Washington, and U.S. residents, knowing about the privacy violations alleged herein.

20 208. The unauthorized interceptions described herein are not covered by any business
21 exception because the interceptions were not required to facilitate users' use of Versions 90, 92,
22 93, and earlier and later versions of the Edge browser.

23 209. Plaintiffs, the Classes, and Subclasses could not provide consent to Defendant's
24 interception because they did not know that their private content was being intercepted and
25 reasonably anticipated that their private data described herein would remain private.

1 210. These acts violate § 2511(1)(a) of the Electronic Communications Privacy Act
2 (“ECPA”) because Defendant intentionally endeavors to intercept, and does in fact intercept,
3 electronic content transmitted by Plaintiffs’, the Classes’, and Subclasses’ use of Versions 90, 92,
4 93, and earlier and later versions of the Edge browser.

5 211. Defendant intercepts Plaintiffs’, the Classes’, and Subclasses’ private data
6 described herein using the Microsoft Edge browser by collecting and sending that data to the
7 SmartScreen Server and/or Bing Servers along with users’ unique user identifiers and cookies, by
8 which Defendant is able to determine individual users’ precise browsing activities and habits.

9 212. Defendant’s acts further violate § 2511(1)(d) because the information intercepted,
10 collected, and sent from Plaintiffs’ and the Classes and Subclasses members’ communications
11 were intentionally used for gain by Defendant as alleged above.

12 213. Plaintiffs, the Classes, and the Subclasses are also damaged when Defendant
13 intentionally intercepts, collects, and uses their information, despite knowing that such
14 interception, collection, and use was unauthorized, for corporate gain and profit such that
15 Defendant was unjustly enriched.

16 214. Plaintiffs, the Classes, and Subclasses seek: (i) injunctive relief to correct
17 Defendant’s actions, including, but not limited to, requiring Defendant to stop intercepting,
18 collecting, or using any portion of, among other things, Plaintiffs’, the Classes’, and Subclasses’
19 private data described herein; (ii) the sum of actual damages suffered by them and any profits
20 Defendant made as a result of its violations of the ECPA, or statutory damages of whichever is the
21 greater of \$100 a day for each day of violation or \$10,000; and (iii) reasonable attorneys’ fees and
22 costs under 18 U.S.C. § 2520.

SECOND CAUSE OF ACTION

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

(All Plaintiffs, Classes, and Subclasses Against MICROSOFT CORP.)

1
2
3
4 215. Plaintiffs, the Classes, and Subclasses repeat and incorporate by reference all
5 preceding paragraphs as if fully set forth herein.

6 216. Plaintiffs', the Classes', and Subclasses' devices used to operate Versions 90, 92,
7 and 93, and earlier and later versions of Edge are, and at all relevant times were, used for interstate
8 communication and commerce and are therefore "protected computers" under 18 U.S.C. §
9 1030(e)(2)(B). Plaintiffs', the Classes', and Subclasses' internet browsing activity, which Defendant
10 impermissibly tracked, involved submissions to websites for companies all over the United States,
11 both for purchases of goods and information.

12 217. Defendant intentionally accessed Plaintiffs', the Classes', and Subclasses' protected
13 computers and obtained information thereby, and in doing so exceeded authority granted by
14 Plaintiffs, the Classes, and Subclasses to access the protected computers in violation of 18 U.S.C. §
15 1030(a)(2), (a)(2)(C). Plaintiffs, the Classes, and Subclasses have a civil cause of action for
16 violation of the Computer Fraud and Abuse Act ("CFAA") under 18 U.S.C. § 1030(g) and have
17 suffered damage or loss as follows.

18 218. Defendant's violations of the CFAA were intentional and reckless, or, pleaded in the
19 alternative, negligent.

20 219. Defendant owned and operated the Microsoft Edge browser. Defendant intercepted
21 and collected Plaintiffs', the Classes', and Subclasses' private data described herein along with their
22 unique user identifiers and cookies through Versions 90, 92, 93, and earlier and later versions of
23 Edge. Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that
24 data for various purposes, including, but not limited to, improving its software, services, and
25 devices, providing targeted advertising, and developing its sophisticated artificial intelligence and
26 machine-learning systems.

1 of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement
2 (2nd) of Torts § 652B.

3 225. A claim for intrusion upon seclusion requires (1) intrusion into a private place,
4 conversation, or matter; (2) in a manner highly offensive to a reasonable person.

5 226. The California Plaintiffs, California Class, and California Subclasses had a
6 reasonable expectation of privacy in their private data described herein as well as in the collection
7 and processing of their unique user identifiers in connection with that data.

8 227. The California Plaintiffs, California Class, and California Subclasses reasonably
9 expected that their private data described herein would not be collected, intercepted, and used by
10 Defendant. It is not necessary for the operation of Versions 90, 92, 93, and earlier and later
11 versions of the Edge browser for users’ private data described herein to be collected and
12 intercepted by Defendant. Furthermore, the California Plaintiffs, California Class, and California
13 Subclasses were not adequately notified that their private data described herein and unique user
14 identifiers and cookies would be intercepted, collected, processed, and used by Defendant.

15 228. Defendant intentionally intruded—and continues to intrude—upon the California
16 Plaintiffs’, California Class’s, and California Subclasses’ solitude, seclusion, and private affairs by
17 intentionally and secretively intercepting, collecting, and using the California Plaintiffs’, California
18 Class’s, and California Subclasses’ private data described herein and unique user identifiers and
19 cookies. Certain intrusions mentioned in this cause of action are illustrative and are not intended
20 to exclude from the scope of this cause of action all of the unlawful behavior as alleged against
21 Defendant herein.

22 229. Defendant owned and operated the Microsoft Edge browser. Defendant designed
23 and programmed Versions 90, 92, 93, and earlier and later versions of Edge to intercept, collect,
24 and send to Defendant the California Plaintiffs’, the California Class’s, and the California
25 Subclasses’ private data described herein and unique user identifiers and cookies through Versions
26 90, 92, 93, and earlier and later versions of Edge. Defendant transmitted this data to the

1 SmartScreen and/or Bing servers. Defendant used that data for various purposes, including, but
2 not limited to, improving its software, services, and devices, providing targeted advertising, and
3 developing its sophisticated artificial intelligence and machine-learning systems.

4 230. By associating the collected data with the unique user identifiers and cookies,
5 Defendant can and does determine individual users' precise internet browsing activities and habits.
6 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions
7 of the Edge browser to collect and process users' unique user identifiers and cookies for this
8 purpose.

9 231. Defendant was actively involved in designing, programming, and implementing the
10 data flows for Versions 90, 92, 93, and earlier and later versions of the Edge browser, including
11 the unlawful interception and collection alleged herein, and promoted the use of the Edge browser
12 to California residents, knowing about the privacy violations alleged herein.

13 232. Defendant's intrusions are highly offensive to a reasonable person, as evidenced by
14 substantial research, literature, and governmental enforcement and investigative efforts to protect
15 consumer privacy against surreptitious technological intrusions. The intentionality of Defendant's
16 conduct, and the steps Defendant has taken to disguise it also reveals the highly offensive nature of its
17 conduct.

18 233. Defendant intercepted, collected, processed, and used the California Plaintiffs',
19 California Class's, and California Subclasses' private data described herein and unique user
20 identifiers and cookies without authority or consent from those California Plaintiffs, California Class
21 members, and California Subclass members.

22 234. The California Plaintiffs, California Class, and California Subclasses were all
23 harmed by, and continue to suffer harm as a direct and proximate result of Defendant's intrusions
24 as detailed throughout this Complaint and are entitled to just compensation and injunctive relief, as
25 well as such other relief as the Court may deem just and proper.
26

1 235. Defendant’s conduct was a substantial factor in causing the harm suffered by the
2 California Plaintiffs, California Class, and California Subclasses.

3 236. The California Plaintiffs, California Class, and California Subclasses seek nominal
4 and punitive damages as a result of Defendant’s actions. Punitive damages are warranted because
5 Defendant’s malicious, oppressive, and willful actions were calculated to injure the California
6 Plaintiffs, California Class, and California Subclasses, and were made in conscious disregard of
7 their rights. Punitive damages are also warranted to deter Defendant from engaging in future
8 misconduct.

9 237. The California Plaintiffs, California Class, and California Subclasses seek
10 injunctive relief to remedy Defendant’s actions, including, but not limited to, requiring Defendant
11 to stop taking users’ private and personally-identifiable data described herein; to make clear
12 disclosures of the information that is reasonably necessary to operate the Microsoft Edge browser;
13 and to recall and destroy all information already taken in contravention of the California Plaintiffs’,
14 California Class’s, and California Subclasses’ privacy rights.

15 238. The California Plaintiffs, California Class, and California Subclasses seek
16 restitution and disgorgement for Defendant’s intrusion upon seclusion. A person acting in
17 conscious disregard of the rights of another must disgorge all profits because disgorgement both
18 benefits the injured parties and deters the perpetrator from committing the same unlawful actions
19 again. Disgorgement is available for conduct that constitutes “conscious interference with a
20 claimant’s legally protected interests,” including tortious conduct or conduct that violates another
21 duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FOURTH CAUSE OF ACTION

(Violation of the Right to Privacy – California Constitution)

(California Plaintiffs, California Class, and California Subclasses

Against MICROSOFT CORP.)

239. The California Plaintiffs, California Class, and California Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

240. In 1972, California added a right of privacy to the list of enumerated inalienable rights in Article I, Section 1 of its Constitution, which expressly provides that “[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” Cal. Const., art. I, § 1.

241. The right to privacy was added to the California Constitution after voters approved a legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses’ control over the unauthorized collection and use of consumers’ personal information, stating:

The right to privacy is the right to be left alone . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulating of personal information. This is essential to social relationships and personal freedom.³⁷

242. The principal purpose of this Constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendant.

³⁷ BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (NOV. 7, 1972).

1 243. The right to privacy in California’s Constitution creates a private right of action
2 against entities like Defendant.

3 244. To plead invasion of privacy under the California Constitution, the California
4 Plaintiffs, California Class, and California Subclasses must allege “that (1) they possess a legally
5 protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the
6 intrusion is ‘so serious . . . as to constitute an egregious breach of the social norms’ such that the
7 breach is ‘highly offensive.’” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601
8 (9th Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)).

9 245. The California Plaintiffs, California Class, and California Subclasses hold a legally
10 protected privacy interest in their private and personally-identifiable data described herein that
11 Defendant intercepts, collects, and uses.

12 246. The California Plaintiffs, California Class, and California Subclasses have a legally
13 protected privacy interest in (a) precluding the interception, collection, copying, dissemination
14 and/or misuse of their private data described herein; and (b) making personal decisions and/or
15 conducting personal activities without observation, intrusion or interference, including, but not
16 limited to, the right to use Versions 90, 92, and 93, and earlier and later versions of the Edge
17 browser, and to visit and interact with various internet sites without having that information
18 intercepted and transmitted to Defendant without the knowledge or consent of the California
19 Plaintiffs, California Class, and California Subclasses.

20 247. The California Plaintiffs, California Class, and California Subclasses have a
21 reasonable expectation of privacy in the private data described herein that Defendant intercepts,
22 collects, and uses without adequate notice or consent – especially since it is not necessary for the
23 operation of the Edge browser for users’ private data described herein to be intercepted, collected,
24 processed, and used by Defendant.

25 248. Defendant’s actions constitute a serious invasion of privacy in that it: (a) invades a
26 zone of privacy protected by the Fourth Amendment, namely, the right to privacy in data

1 contained on personal computing devices, including web search and browsing histories; (b)
2 violates federal criminal laws including the Electronic Communications Privacy Act and
3 Computer Fraud and Abuse Act; and (c) invades the privacy interests and rights of millions of
4 U.S. residents (including the California Plaintiffs, California Class, and California Subclasses)
5 without their consent.

6 249. Defendant fails to effectively inform users that Microsoft Edge intercepts, collects,
7 and uses the private data. Defendant does not ensure that relevant disclosures are immediately
8 apparent and fails to disclose the extent of the information intercepted, received, or collected, or
9 the result of information that is intercepted, received, or collected. This results in injury to the
10 California Plaintiffs, California Class, and California Subclasses.

11 250. Defendant owned and operated the Microsoft Edge browser. Defendant collected
12 and intercepted the California Plaintiffs', California Class's, and California Subclasses' private
13 data described herein along with their unique user identifiers and cookies through Versions 90, 92,
14 93, and earlier and later versions of Edge. Defendant transmitted this private data to the
15 SmartScreen and/or Bing servers. Defendant used that private data for various purposes,
16 including, but not limited to, improving its software, services, and devices, providing targeted
17 advertising, and developing its sophisticated artificial intelligence and machine-learning systems.

18 251. By associating the collected data with the unique user identifiers and cookies,
19 Defendant is able to and does determine individual users' precise internet browsing activities and
20 habits. Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later
21 versions of the Edge browser to collect and process users' unique user identifiers and cookies for
22 this purpose.

23 252. Defendant was actively involved in designing and programming the data flows for
24 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
25 interception and collection alleged herein, and promoted the use of the Microsoft Edge browser to
26 California residents, knowing about the privacy violations alleged herein.

1 253. Defendant acted with deceit and disregard for the California Plaintiffs', California
2 Class's, and California Subclasses' privacy by intercepting, collecting, and using private data
3 described herein without authorization.

4 254. The reasonableness of the California Plaintiffs', California Class's, and California
5 Subclasses' expectations of privacy is supported by the clandestine nature of Defendant's
6 interception and collection of the California Plaintiffs', California Class's, and California
7 Subclasses' private data described herein. Defendant acted with deceit and disregard for the
8 California Plaintiffs', California Class's, and California Subclasses' privacy.

9 255. Defendant's conduct violated the California Plaintiffs', California Class's, and
10 California Subclasses' privacy interests, was highly offensive to a reasonable person, and
11 constituted and continues to constitute an egregious breach of social norms. Not only did
12 Defendant intercept, collect, and use this private information, Defendant either did not disclose at
13 all, or failed to make an effective disclosure, that it would intercept, collect, and use the California
14 Plaintiffs', California Class's, and California Subclasses' private data described herein. Defendant
15 intentionally invaded the California Plaintiffs', California Class's, and California Subclasses'
16 privacy interests by intentionally designing its Edge browser to surreptitiously obtain, improperly
17 gain knowledge of, review, and retain the California Plaintiffs', California Class's, and California
18 Subclasses' private and personally-identifiable information.

19 256. These intrusions are highly offensive to a reasonable person, as evidenced by
20 substantial research, literature, and governmental enforcement and investigative efforts to protect
21 consumer privacy against surreptitious technological intrusions.

22 257. The intentionality of Defendant's conduct, and the steps it has taken to disguise it,
23 also show the highly offensive nature of its conduct.

24 258. Further, Defendant's conduct targeted the California Plaintiffs', California Class's,
25 and California Subclasses' computer devices, which the United States Supreme Court has
26

1 characterized as almost a feature of human anatomy, and which contain the California Plaintiffs’,
2 California Class’s, and California Subclasses’ private and personally-identifiable information.

3 259. The California Plaintiffs, California Class, and California Subclasses were harmed
4 by the intrusion as detailed throughout this Complaint.

5 260. Defendant’s conduct was a substantial factor in causing the harm suffered by the
6 California Plaintiffs, California Class, and California Subclasses.

7 261. The California Plaintiffs, California Class, and California Subclasses seek nominal
8 and punitive damages as a result of Defendant’s actions. Punitive damages are warranted because
9 Defendant’s malicious, oppressive, and willful actions were calculated to injure the California
10 Plaintiffs, California Class, and California Subclasses and were made in conscious disregard of
11 their rights. Punitive damages are also warranted to deter Defendant from engaging in future
12 misconduct.

13 262. The California Plaintiffs, California Class, and California Subclasses seek
14 injunctive relief to remedy Defendant’s actions, including, but not limited to, requiring Defendant
15 to stop taking private information from users’ electronic devices; to make clear disclosures of the
16 information that is reasonably necessary to operate the Microsoft Edge browser; and to recall and
17 destroy all private information already taken in contravention of the California Plaintiffs’,
18 California Class’s, and California Subclasses’ privacy rights.

19 263. The California Plaintiffs, California Class, and California Subclasses seek
20 restitution and disgorgement for Defendant’s violation of their privacy rights. A person acting in
21 conscious disregard for the rights of another must disgorge all profit because disgorgement both
22 benefits the injured parties and deters the perpetrator from committing the same unlawful actions
23 again. Disgorgement is available for conduct that constitutes “conscious interference with a
24 claimant’s legally protected interests,” including tortious conduct or conduct that violates another
25 duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FIFTH CAUSE OF ACTION

(Violation of California Invasion of Privacy Act, California Penal Code §§ 630, *et seq.*)

(California Plaintiffs, California Class, and California Subclasses

Against MICROSOFT CORP.)

264. The California Plaintiffs, California Class, and California Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

265. The California Invasion of Privacy Act (“CIPA”), codified at Cal. Pen. Code §§ 630-638, begins by providing its statement of purpose:

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

Cal. Pen. Code § 630.

266. Cal. Pen. Code § 631(a) imposes liability upon:

Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and *without the consent of all parties to the communication*, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section [Emphasis added.]

267. Cal. Pen. Code § 632(a) imposes liability upon:

A person who, intentionally and *without the consent of all parties* to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential

1 communication, whether the communication is carried on among the
2 parties in the presence of one another or by means of a telegraph,
telephone, or other device, except a radio [Emphasis added.]

3 268. Under either section of the CIPA quoted above, a defendant must show it had the
4 consent of all parties to a communication.

5 269. Defendant knowingly and intentionally used and continues to use Versions 90, 92,
6 93, and earlier and later versions of the Edge browsers and receiving servers (where users' private
7 data described herein was and is saved and recorded), all of which are recording devices under
8 CIPA, to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic
9 communications containing the private data described herein from the California Plaintiffs,
10 California Class, and California Subclasses, while these electronic communications were and are
11 in transit, originating in or sent to California, and without the authorization or consent of the
12 California Plaintiffs, California Class, or California Subclasses.

13 270. The California Plaintiffs, California Class, and California Subclasses were and are
14 in California during one or more of the instances where Defendant intercepted their
15 communications. Upon information and belief, the California Plaintiffs, California Class,
16 California Subclasses, during one or more of their interactions on the internet during the
17 applicable statute of limitations period, communicated with one or more entities based in
18 California, and/or with one or more entities whose servers were located in California.
19 Communications from the California web-based entities to members of the California Class and
20 California Subclasses were sent from California. Communications to the California web-based
21 entities from members of the California Classes and California Subclasses were sent to California.

22 271. The communications intercepted by Defendant include "contents" of electronic
23 communications exchanged between the California Plaintiffs, California Class, and California
24 Subclasses, on the one hand, and the websites that they visited, on the other, in the form of the
25 private data described herein. Defendant's non-consensual interception of these communications
26 was designed to learn at least some of these contents.

1 272. The following items constitute “machine[s], instrument[s], or contrivance[s]” under
2 Cal. Penal Code § 631(a), and even if they did not, Defendant’s purposeful scheme that facilitated
3 its interceptions falls under the broad statutory catch-all category of “any other manner”:

4 a. The California Plaintiffs’, California Class’s, and California Subclasses’
5 browser (*i.e.*, the Edge Browser);

6 b. The California Plaintiffs’, California Class’s, and California Subclasses’
7 personal computing devices;

8 c. The computer codes and programs used by Defendant to effectuate the
9 interception of communications exchanged between websites and search engines, on the one hand,
10 and the California Plaintiffs, California Class, and California Subclasses on the other;

11 d. Defendant’s servers, at least some of which, on information and belief, are
12 located in California;

13 e. The servers of the third-party websites, at least some of which, on
14 information and belief, are located in California, with respect to which Defendant intercepted the
15 California Plaintiffs’, California Class’s, and California Subclasses’ communications;

16 f. The plan Defendant carried out to effectuate the interception of the
17 communications that were exchanged between the third-party websites, on the one hand, and the
18 California Plaintiffs, California Class, and California Subclasses on the other.

19 273. The private data described herein collected by Defendant constituted “confidential
20 communications,” as that term is used in Cal. Pen. Code § 632(a), because the California
21 Plaintiffs, California Class, and California Subclasses have an objectively reasonable expectation
22 of privacy that their private browsing communications are not being intercepted, collected,
23 disseminated, or used by Defendant. In particular, it is not necessary for the operation of the Edge
24 browser for users’ private data described herein to be intercepted, collected, disseminated, or used
25 by Defendant.

1 286. Defendant wrongfully exercised control over the California Plaintiffs', California
2 Class's, and California Subclasses' private data described herein and have not returned such data.

3 287. The California Plaintiffs, California Class, and California Subclasses have been
4 damaged as a result of Defendant's unlawful conversion of their property.

5 **EIGHTH CAUSE OF ACTION**

6 **(Violation of the California Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq.*)**

7 **(California Plaintiffs, California Class, and California Subclasses**

8 **Against MICROSOFT CORP.)**

9 288. The California Plaintiffs, California Class, and California Subclasses repeat and
10 incorporate by reference all preceding paragraphs as if fully set forth herein.

11 289. California's Unfair Competition Law ("UCL") prohibits any "unlawful unfair or
12 fraudulent business act or practice." which can include false or misleading advertising. Cal. Bus.
13 & Prof. Code §§ 17200 *et seq.*

14 290. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

15 291. Defendant engaged in "unlawful" conduct through its violation of state and federal
16 law, including: (i) violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et*
17 *seq.*; (ii) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (iii) intrusion upon
18 seclusion; (iv) invasion of privacy under Article I, Section 1 of the California Constitution; (v)
19 violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; (vi) violation
20 of Cal. Penal Code §§ 484 and 496; and (vii) conversion.

21 292. Defendant engaged in "unfair" conduct, because it knowingly intercepted and
22 collected and used communications, and/or knowingly received intercepted communications,
23 containing the private data described herein of the California Plaintiffs and members of the
24 California Class and California Subclasses under circumstances in which those Plaintiffs and
25 Class and Subclasses members would have no reason to know that such information was being
26 intercepted and used because it was never disclosed or otherwise made known to them by

1 Defendant. This conduct offended established public policy established by the California
2 legislature and is immoral, unethical, oppressive, unscrupulous, and substantially injurious to
3 consumers.

4 293. The California Plaintiffs, California Class, and California Subclasses have suffered
5 injury-in-fact, including the loss of money and/or property as a result of Defendant's unfair and/or
6 unlawful practices, to wit, the unauthorized collection of their private data described herein, which
7 has value in an amount to be proven at trial. Moreover, the California Plaintiffs, California Class,
8 California Subclasses have suffered harm in the form of diminution of the value of their private
9 data described herein.

10 294. Defendant's actions caused damage to and loss of the California Plaintiffs',
11 California Class's, and California Subclasses' property right to control the dissemination and use
12 of their private data described herein.

13 295. Defendant has taken property from the California Plaintiffs, California Class, and
14 California Subclasses without providing just, or any, compensation.

15 296. Defendant should be required to cease their unfair and/or illegal collection of users'
16 private data described herein and to retrieve and delete all unfairly and/or illegally obtained private
17 user data. Defendant reaped unjust profits and revenues in violation of the UCL. The California
18 Plaintiffs, California Class, and California Subclasses seek injunctive relief governing Defendant's
19 ongoing taking and possession of their private data described herein, and/or failure to account to
20 the California Plaintiffs, California Class, and California Subclasses concerning Defendant's
21 interception, collection, possession, and use of that data, and restitution and disgorgement of
22 resulting unjust profits and revenues to Defendant.

23 297. The California Plaintiffs, California Class, and California Subclasses lack an
24 adequate remedy at law because the ongoing harms from Defendant's interception, collection,
25 taking, possession, and use of private data described herein must be addressed by injunctive relief
26

1 and, due to the ongoing and nature of the harm, the harm cannot be adequately addressed by
2 monetary damages alone.

3 **NINTH CAUSE OF ACTION**

4 **(Intrusion Upon Seclusion)**

5 **(Washington Plaintiff, Washington Class, and Washington Subclasses**

6 **Against MICROSOFT CORP.)**

7 298. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat and
8 incorporate by reference all preceding paragraphs as if fully set forth herein.

9 299. Washington follows a common law cause of action for invasion of privacy by
10 intrusion upon seclusion. *Reid v. Pierce County*, 961 P.2d 333 (Wash. 1998). “Invasion of privacy
11 by intrusion consists of a deliberate intrusion, physical or otherwise, into a person’s solitude,
12 seclusion, or private affairs. [To prevail on this cause of action] the intruder must have acted
13 deliberately to achieve the result, with the certain belief that the result would happen.” *Fisher v.*
14 *State Dep’t of Health*, 106 P.3d 836, 879 (Wash. Ct. App. 2005).

15 300. The Washington Plaintiff, Washington Class, and Washington Subclasses had a
16 reasonable expectation of privacy in their private data described herein as well as in the collection
17 and processing of their unique user identifiers in connection with that content.

18 301. The Washington Plaintiff, Washington Class, and Washington Subclasses
19 reasonably expected that their private data described herein would not be collected, intercepted,
20 and used by the Defendant. It is not necessary for the operation of Versions 90, 92, 93, and earlier
21 and later versions of the Edge browser for such data to be collected, intercepted, and used by
22 Defendant.

23 302. Defendant intentionally intruded—and continues to intrude—upon the Washington
24 Plaintiff’s, Washington Class’s, and Washington Subclasses’ solitude, seclusion, and private
25 affairs by intentionally and secretly collecting the Washington Plaintiff’s, Washington Class’s,
26 Washington Subclasses’ private and personally-identifiable information and using that data, as

1 described above. Certain intrusions are shared within this claim as illustrative; however, not to
2 the exclusion of all of the unlawful behavior as alleged against Defendant herein.

3 303. Defendant owned and operated the Microsoft Edge browser. Defendant collected
4 and intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses'
5 private data described herein through Versions 90, 92, 93, and earlier and later versions of Edge.
6 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
7 for various purposes, including, but not limited to, improving its software, services, and devices,
8 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
9 learning systems. By associating the collected data with the unique user identifiers and cookies,
10 Defendant is able to determine individual users' precise internet browsing activities and habits.
11 Defendant thus designed and programmed Versions 90, 92, 93, and earlier and later versions of the
12 Edge browser to collect and process users' unique user identifiers and cookies.

13 304. Defendant was actively involved in designing and programming the data flows for
14 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
15 collection interception alleged herein, and promoted the use of the Microsoft Edge browser to
16 Washington and U.S. residents, knowing about the privacy violations alleged herein.

17 305. Defendant's intrusions are highly offensive to a reasonable person, as evidenced by
18 substantial research, literature, and governmental enforcement and investigative efforts to protect
19 consumer privacy against surreptitious technological intrusions. The intentionality of Defendant's
20 conduct, and the steps it has taken to disguise it also reveals the highly offensive nature of its conduct.

21 306. Defendant collected, intercepted, processed, and used the Washington Plaintiff's,
22 Washington Class's, and Washington Subclasses' private data described herein and unique user
23 identifiers and cookies without authority or consent from that Plaintiff and members of that Class
24 and those Subclasses.

25 307. The Washington Plaintiff, Washington Class, and Washington Subclasses were all
26 harmed by, and continue to suffer harm as a direct and proximate result of Defendant's intrusions,

1 as detailed throughout this Complaint, and are entitled to just compensation and injunctive relief,
2 as well as such other relief as the Court may deem just and proper.

3 308. Defendant's conduct was a substantial factor in causing the harm suffered by the
4 Washington Plaintiff, Washington Class, and Washington Subclasses.

5 309. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
6 nominal and punitive damages because of Defendant's actions. Punitive damages are warranted
7 because Defendant's malicious, oppressive, and willful actions were calculated to injure the
8 Washington Plaintiff, Washington Class, and Washington Subclasses, and were made in conscious
9 disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in
10 future misconduct.

11 310. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
12 injunctive relief to remedy Defendant's actions, including, but not limited to, requiring Defendant
13 to stop taking private and personally-identifiable information from users' electronic devices; to
14 make clear disclosures of the information that is reasonably necessary to operate the Microsoft
15 Edge browser; and to recall and destroy all information already taken in contravention of the
16 Washington Plaintiff's, Washington Class's, and Washington Subclasses' privacy rights.

17 **TENTH CAUSE OF ACTION**

18 **(Conversion)**

19 **(Washington Plaintiff, Washington Class, and Washington Subclasses**

20 **Against MICROSOFT CORP.)**

21 311. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat
22 and incorporate by reference all preceding paragraphs as if fully set forth herein.

23 312. Conversion is the unjustified, willful interference with a chattel which deprives a
24 person entitled to the property of possession. "Chattel" includes both tangible and intangible
25 goods, such as corporate property. *Lang v. Hougan*, 136 Wn. App. 708, 718 (Wash. Ct. App.
26 2007). The essence of conversion is the dispossession of property from the rightful owner. *Repin*

1 v. *State*, 198 Wn. App. 243, 270 (Wash. Ct. App. 2017). The Washington Plaintiff, Washington
2 Class, and Washington Subclasses have a property interest in their personal information.

3 313. Defendant unlawfully collected, used, and exercised dominion and control over the
4 California Plaintiffs, Class, and Subclasses' private data described herein without authorization.

5 314. Defendant owned and operated the Microsoft Edge browser. Defendant collected
6 and intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses'
7 private data described herein through Versions 90, 92, 93, and earlier and later versions of Edge.
8 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
9 for various purposes, including, but not limited to, improving its software, services, and devices,
10 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
11 learning systems.

12 315. By associating the collected data with the unique user identifiers and cookies,
13 Defendant is able to determine individual users' precise internet browsing activities and habits.
14 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions
15 of the Edge browser to collect and process users' unique user identifiers and cookies.

16 316. Defendant wrongfully exercised control over the Washington Plaintiff's,
17 Washington Class's, and Washington Subclasses' private data described herein and have not
18 returned it.

19 317. The Washington Plaintiff, Washington Class, and Washington Subclasses have
20 been damaged as a result of Defendant's unlawful conversion of their private data described
21 herein. The reasonable and fair market value of the unlawfully obtained private data can be
22 determined in the marketplace.

ELEVENTH CAUSE OF ACTION

(Violation of the Washington Privacy Act, Wash. Rev. Code ch. 9.73)

(Washington Plaintiff, Washington Class, and Washington Subclasses

Against MICROSOFT CORP.)

1
2
3
4
5 318. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat
6 and incorporate by reference all preceding paragraphs as if fully set forth herein.

7 319. Washington’s Privacy Act (“WPA”) prohibits the interception or recording of a
8 private communication or conversation by any device, electronic or otherwise, without obtaining
9 the consent of all the parties participating in the conversation. RCW § 9.73.030(1)(a)(b). Under
10 the WPA, communication is private when parties “manifest a subjective intention that it be private
11 and where that expectation is reasonable.” *State v. Kipp*, 179 Wn.2d. 718, 729 (Wash. Ct. App.
12 2014). Proof of subjective intent need not be explicit. *Id.* at 729.

13 320. The Washington Plaintiff, Washington Class, and Washington Subclasses have an
14 expectation of privacy in their private data described herein, and they exercised a reasonable
15 expectation of privacy concerning the transmission of that content.

16 321. However, Defendant intercepted the Washington Plaintiff’s, Washington Class’s,
17 and Washington Subclasses’ private data described herein without their consent or knowledge.

18 322. Defendant owned and operated the Microsoft Edge browser. Defendant collected
19 and intercepted the Washington Plaintiff’s, Washington Class’s, and Washington Subclasses’
20 private data described herein through Versions 90, 92, 93, and earlier and later versions of Edge.
21 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
22 for various purposes, including, but not limited to, improving its software, services, and devices,
23 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
24 learning systems.

25 323. By associating the collected data with the unique user identifiers and cookies,
26 Defendant is able to determine individual users’ precise internet browsing activities and habits.

1 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions
2 of the Edge browser to collect and process users' unique user identifiers and cookies.

3 324. Defendant was actively involved in designing and programming the data flows for
4 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
5 collection interception alleged herein, and promoted the use of the Microsoft Edge browser to
6 Washington and U.S. residents, knowing about the privacy violations alleged herein.

7 325. Defendant designed the Microsoft Edge browser in a way that it knew the
8 Washington Plaintiff's, Washington Class's, and Washington Subclasses' privacy rights would be
9 violated, in that their content would be unlawfully intercepted. The defective and unlawful design
10 of the Microsoft Edge browser directly facilitates Defendant's unlawful conduct.

11 326. The unauthorized interceptions described herein are not covered by any business
12 exception because the interceptions were not required to facilitate communications between users.

13 327. The Washington Plaintiff, Washington Class, and Washington Subclasses could not
14 provide consent to the interception because they did not know that their private data described
15 herein was being intercepted and reasonably anticipated that such data would remain private.

16 328. The Washington Plaintiff, Washington Class, and Washington Subclasses have a
17 property right and interest in their private data described herein such that the interception of that
18 data is violative of those rights and therefore causes them injury and damages.

19 329. The Washington Plaintiff, Washington Class, and Washington Subclasses suffered
20 further economic injury as a result of Defendant's unlawful and unauthorized collection,
21 interception, and use of their private data described herein.

22 330. The Washington Plaintiff, Washington Class, and Washington Subclasses seek the
23 amount of their actual damages in the amount of \$100 for each day of violation not to exceed
24 \$1,000, liquidated damages, reasonable attorneys' fees and costs, and any other relief this court
25 deems just.
26

TWELFH CAUSE OF ACTION

(Violation of the Washington Consumer Protection Act, Wash. Rev. Code ch. 19.86)

(Washington Plaintiff, Washington Class, and Washington Subclasses

Against MICROSOFT CORP.)

331. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

332. The Washington Consumer Protection Act (“WCPA”) makes unlawful any unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. RCW § 19.86.020. “Trade or commerce” includes any commerce directly or indirectly affecting the people of the state of Washington. Wash. Rev. Code Ann § 19.86.010. An unfair or deceptive act is proved if the defendant’s actions possessed a tendency or capacity to mislead. *Testo v. Russ Dunmire Oldsmobile, Inc.*, 554 P.2d 349 (1976).

333. The Washington Plaintiff, Washington Class, and Washington Subclasses hold a legally protected privacy interest in their private data described herein that Defendant has unfairly collected, intercepted, and used through deceptive acts and practices.

334. The Washington Plaintiff, Washington Class, and Washington Subclasses had a reasonable expectation of privacy in their private data described herein as well as in the collection and processing of their unique user identifiers in connection with that content.

335. The Washington Plaintiff, Washington Class, and Washington Subclasses reasonably expected that their private data described herein would not be collected and intercepted by the Microsoft Edge browser. It is not necessary for the operation of the browser for users’ private data described herein to be collected, intercepted, and used by Defendant.

336. These unfair or deceptive acts or practices taken by Defendant include failing to inform the user that Edge collects and intercepts the user’s private data described herein, not ensuring relevant disclosures are immediately apparent, and failing to disclose the extent of the

1 information collected, intercepted, or used, or the result of information that is collected,
2 intercepted, or used.

3 337. The Washington Plaintiff, Washington Class, and Washington Subclasses can
4 claim that these deceptive acts and practices are injurious to the public interest because they injure
5 other persons and have the capacity to injure other persons.

6 338. Defendant owned and operated the Microsoft Edge browser. Defendant collected
7 and intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses'
8 private data described herein through Versions 90, 92, 93 and earlier and later versions of Edge.
9 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
10 for various purposes, including, but not limited to, improving its software, services, and devices,
11 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
12 learning systems.

13 339. By associating the collected data with the unique user identifiers and cookies,
14 Defendant is able to determine individual users' precise internet browsing activities and habits.
15 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions
16 of the Edge browser to collect and process users' unique user identifiers and cookies.

17 340. Defendant was actively involved in designing and programming the data flows for
18 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
19 collection interception alleged herein, and promoted the use of the Microsoft Edge browser to
20 California and U.S. residents, knowing about the privacy violations alleged herein.

21 341. Defendant acted with deceit and disregard for the Washington Plaintiff's, Washington
22 Class's, and Washington Subclasses' privacy by collecting, intercepting, and using their private data
23 described herein without authorization.

24 342. Defendant's conduct violated the Washington Plaintiff's, Washington Class's, and
25 Washington Subclasses' privacy interests, were highly offensive to a reasonable person, and
26 constituted and continues to constitute an egregious breach of social norms. Not only did

1 Defendant take and use this information, Defendant either did not disclose at all, or failed to make
2 an effective disclosure, that it would take and use the Washington Plaintiff's, Washington Class's,
3 and Washington Subclasses' private and personally-identifiable information. Defendant
4 intentionally invaded the Washington Plaintiff's, Washington Class's, and Washington Subclasses'
5 privacy interests by intentionally designing its Edge browser to surreptitiously obtain, improperly
6 gain knowledge of, review, and retain the Washington Plaintiff's, Washington Class's, and
7 Washington Subclasses' private data described herein.

8 343. These intrusions are highly offensive to a reasonable person, as evidenced by
9 substantial research, literature, and governmental enforcement and investigative efforts to protect
10 consumer privacy against surreptitious technological intrusions.

11 344. The intentionality of Defendant's conduct, and the steps it has taken to disguise it
12 also show the highly offensive nature of its conduct.

13 345. Further, Defendant's conduct targeted the Washington Plaintiff's, Washington
14 Class's, and Washington Subclasses' computer devices, which the United States Supreme Court
15 has characterized as almost a feature of human anatomy, and which contain the Washington
16 Plaintiff's, Washington Class's, and Washington Subclasses' private and personally-identifiable
17 information.

18 346. The Washington Plaintiff, Washington Class, and Washington Subclasses were
19 harmed by the intrusion as detailed throughout this Complaint.

20 347. Defendant's conduct was a substantial factor in causing the harm suffered by the
21 Washington Plaintiff, Washington Class, and Washington Subclasses.

22 348. The Washington Plaintiff, Washington Class, and Washington Subclasses seek the
23 amount of their actual damages to not exceed more than \$7,500 for each violation, plus reasonable
24 attorneys' fees and costs, and any other relief this court deems just.

25 349. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
26 nominal and punitive damages as a result of Defendant's actions. Punitive damages are warranted

1 because Defendant's malicious, oppressive, and willful actions were calculated to injure the
2 Washington Plaintiffs, Washington Class, and Washington Subclasses and were made in conscious
3 disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in
4 future misconduct.

5 350. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
6 injunctive relief to remedy Defendant's actions, including, but not limited to, requiring Defendant to
7 stop taking private information from users' electronic devices; to make clear disclosures of the
8 information that is reasonably necessary to operate the Microsoft Edge browser; and to recall and
9 destroy all information already taken in contravention of the Washington Plaintiff's, Washington
10 Class's, and Washington Subclasses' privacy rights.

11 **THIRTEENTH CAUSE OF ACTION**

12 **(Restitution / Unjust Enrichment)**

13 **(All Plaintiffs, Classes, and Subclasses Against MICROSOFT CORP.)**

14 351. Plaintiffs, the Classes, and Subclasses repeat and incorporate by reference all
15 preceding paragraphs as if fully set forth herein.

16 352. Plaintiffs, the Classes, and Subclasses have conferred substantial benefits on
17 Defendant by downloading and using Defendant's Edge browser. These benefits include
18 Defendant's collection and use of the Plaintiffs', the Classes', and the Subclasses' private data
19 described herein and the revenues and profits resulting from using this data for various purposes,
20 including, but not limited to, those described herein.

21 353. Defendant has knowingly and willingly accepted and enjoyed these benefits.

22 354. Defendant either knew or should have known that the benefits rendered by
23 Plaintiffs, the Classes, and Subclasses were given and received with the expectation that it would
24 not take and use the private data described herein that Defendant has taken without permission.
25 For Defendant to retain those benefits under these circumstances is inequitable.
26

1 355. Through deliberate violation of the Plaintiffs', the Classes', and the Subclasses'
2 privacy interests and statutory and constitutional rights, Defendant reaped benefits that led to
3 Defendant wrongfully receiving profits.

4 356. Equity demands disgorgement of Defendant's ill-gotten gains. Defendant will be
5 unjustly enriched unless they are ordered to disgorge those profits for the benefit of Plaintiffs, the
6 Classes, and Subclasses.

7 357. As a direct and proximate result of Defendant's wrongful conduct and unjust
8 enrichment, Plaintiffs, the Classes, and Subclasses are entitled to restitution from Defendant and
9 institution of a constructive trust disgorging all profits, benefits and other compensation obtained
10 by Defendant through this inequitable conduct.

11 **PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiffs request relief against Defendant as set forth below:

13 A. Entry of an order certifying the proposed Classes and Subclasses pursuant to Federal
14 Rule of Civil Procedure 23;

15 B. Entry of an Order appointing Plaintiffs as representatives of the Classes and
16 Subclasses;

17 C. Entry of an Order appointing Plaintiffs' counsel as co-lead counsel of the Classes and
18 Subclasses;

19 D. Entry of an Order for injunctive relief preventing Defendant from continuing to
20 intercept, receive, collect, or use Plaintiffs, the Classes, and Subclasses' data in the ways alleged
21 herein.

22 E. Entry of judgment in favor of each Class and Subclass member for statutory
23 damages, actual damages suffered as a result of the conduct alleged herein, punitive damages,
24 restitution, and disgorgement, including interest and prejudgment interest;

25 F. Award Plaintiffs' reasonable attorneys' fees and costs; and
26

1 G. Grant such other and further legal and equitable relief as the Court deems just and
2 equitable.

3 **DEMAND FOR JURY TRIAL**

4 Plaintiffs demand a trial by jury on all issues so triable.

5 DATED this 21st day of July 2023.

6 Respectfully submitted,

7 SUMMIT LAW GROUP, PLLC

8 By s/ Alexander A. Baehr

9 Alexander A. Baehr, WSBA No. 25320
10 315 Fifth Avenue S., Suite 1000
11 Seattle, Washington 98104
12 Telephone: (206) 676-7000
13 Email: alexb@summitlaw.com

14 BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
15 DROOKS, LINCENBERG & RHOW, PC

16 Ekwan E. Rhow (*pro hac vice forthcoming*)
17 Marc E. Masters (*pro hac vice forthcoming*)
18 Barr Benyamin (*pro hac vice forthcoming*)
19 1875 Century Park East, 23rd Floor
20 Los Angeles, California 90067
21 Telephone: (310) 201-2100
22 Email: erhow@birdmarella.com
23 mmasters@birdmarella.com
24 bbenjamin@birdmarella.com

25 GLANCY PRONGAY & MURRAY LLP

26 Jonathan Rotter (*pro hac vice forthcoming*)
Raymond D. Sulentic (*pro hac vice
forthcoming*)
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
Email: jrotter@glancylaw.com
kwolke@glancylaw.com
prajesh@glancylaw.com

CLARKSON LAW FIRM, P.C.

Glenn A. Danas (*pro hac vice forthcoming*)
Yana Hart (*pro hac vice forthcoming*)
Katelyn M. Leeviraphan (*pro hac vice
forthcoming*)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070
Email: gdanas@clarksonlawfirm.com
yhart@clarksonlawfirm.com
kleeviraphan@clarksonlawfirm.com

Attorneys for Plaintiffs and
the Putative Classes and Subclasses

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26