

BAILEY & GLASSER, LLP

Arthur H. Bryant (State Bar No. 208365)
abryant@baileyglasser.com
Todd A. Walburg (State Bar No. 213063)
twalburg@baileyglasser.com
1999 Harrison Street, Suite 660
Oakland, CA 94612
(304) 345-6555 (main) / (304) 342-1110 (fax)

John W. Barrett (*pending pro hac vice admission*)
jbarrett@baileyglasser.com
209 Capitol Street
Charleston, WV 25301
(304) 345-6555 / (304) 342-1110 (fax)

THE GOLAN FIRM PLLC

Yvette Golan (*pending pro hac vice admission*)
y.golan@tgfirm.com
2000 M St. NW Suite 750-A
Washington, DC 20036
(866) 298-4150 / (928) 441-8250 (fax)

Attorneys for Plaintiffs

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

FRANK D. RUSSO, KOONAN LITIGATION CONSULTING, LLC, and SUMNER M. DAVENPORT & ASSOCIATES, LLC, on behalf of a similarly situated class,
Plaintiff,

vs.

MICROSOFT CORPORATION,
Defendant.

Case No.
COMPLAINT
CLASS ACTION
DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

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
27
28

SUMMARY OF CLAIMS..... 4

INTRODUCTION 4

PARTIES AND PLAINTIFF-SPECIFIC ALLEGATIONS 6

JURISDICTION AND VENUE 10

FACTS 10

 A. MICROSOFT TRANSITIONED BUSINESS CUSTOMERS TO ITS CLOUD-BASED SERVICES, ASSURING THEM THEIR DATA WOULD BE PRIVATE AND SECURE..... 10

 B. MICROSOFT REPRESENTED TO BUSINESS CUSTOMERS IT WOULD USE THEIR DATA ONLY TO PROVIDE THE SERVICES THEY PURCHASED. 12

 C. MICROSOFT’S REPRESENTATIONS WERE FALSE. 17

 1. Microsoft shares its business customers’ data with Facebook and other third parties, without its business customers’ consent..... 17

 2. Microsoft shares its business customers’ data with third-party developers, without its business customers’ consent..... 19

 3. Microsoft shares its business customers’ data with hundreds of subcontractors when sharing is not needed to provide the services, and without requiring the subcontractors to keep the data private and secure..... 20

 4. Microsoft uses its business customers’ data to develop and sell new products and services—and otherwise benefit itself..... 21

 D. MICROSOFT MISREPRESENTS THE SECURITY IT PROVIDES FOR BUSINESS CUSTOMERS’ DATA. 22

 E. MICROSOFT’S ACTIONS HAVE INJURED PLAINTIFFS AND OTHER BUSINESS CUSTOMERS. 24

CLASS ACTION ALLEGATIONS 25

APPLICABLE LAW 27

Count One: Violations of the Wiretap Act 18 U.S.C. §§ 2511(1)(a), (1)(c), and (1)(d) On behalf of Plaintiffs and the Class 27

Count Two: Violations of the Stored Communications Act 18 U.S.C. § 2702 On behalf of Plaintiffs and the Class 30

1 Count Three: Violations of the Washington Consumer Protection Act RCW 19.86,
2 et seq. On behalf of Plaintiffs and the Class 33
3
4 Count Four: Violations of Washington Privacy Act R.C.W. §§ 9.73.010, et seq.
5 On behalf of Plaintiffs and the Class 35
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 **SUMMARY OF CLAIMS**

2 1. This is a national class action against Microsoft for misrepresenting its privacy
3 and security practices, violating federal and state law, and illegally sharing and using its
4 business-class Microsoft Office 365 and Microsoft Exchange customers’ data.¹ Contrary to
5 Microsoft’s representations and without its customers’ consent, Microsoft shares its business
6 customers’ contacts and related data with Facebook; shares the content of its business customers’
7 emails, documents, contacts, calendars, and other data with unauthorized third parties for
8 unauthorized purposes; and uses its business customers’ data to develop new products and
9 services to sell to others. Those actions violate the Wiretap Act, 18 U.S.C. § 2511; the Stored
10 Communications Act, 18 U.S.C. § 2702; and the consumer protection and privacy laws of
11 Washington.
12

13 **INTRODUCTION**

14 2. Businesses require privacy and security to protect their data, which includes
15 sensitive information belonging to them, their employees, their customers or clients, confidential
16 business plans and financial projections, and trade secrets.
17

18 3. Knowing this, Defendant Microsoft Corporation has made privacy, security,
19 transparency, and trust the core themes of its marketing efforts for its phenomenally successful
20 Office 365 (now called Microsoft 365) and Exchange Online services.² Like a mantra, Microsoft
21 has repeatedly promised business customers that it will use their content and data exclusively to
22 provide them with the purchased services; that, solely for those purposes, it will share their data
23

24 _____
25 ¹When used in this Complaint, unless the context suggests otherwise, “businesses,”
26 “business customers,” and similar terms include persons and non-governmental entities, including
27 non-profit organizations, that subscribe to or purchase business-class versions of Microsoft Office
28 365 and Microsoft Exchange, as specified in the class definition at ¶ 116, *infra*.

²On April 21, 2020, Office 365 became Microsoft 365. All references to Office 365 in this
Complaint include references to Microsoft 365 as of that date and thereafter.

1 with its subcontractors and certain others only on a need-to-know basis; and that it will never
2 share the customer's data with third parties at all.

3 4. In fact, contrary to its representations, Microsoft has regularly shared—and
4 continues to share—its business customers' data with Facebook and other third parties. The data
5 is shared even when neither the customers nor their contacts are Facebook users. And, once
6 Facebook obtains the data, harmful consequences can follow, as demonstrated by the data-
7 harvesting debacle orchestrated by Cambridge Analytica targeting the 2016 national election,
8 using data obtained by Facebook.

9
10 5. Even when sharing has not been necessary to perform the purchased services,
11 Microsoft has nonetheless shared its business customers' data with hundreds of subcontractors,
12 at least some of which have suffered data breaches and are based in countries known for
13 corporate espionage, such as Russia, China, and Libya.

14
15 6. Microsoft also has routinely used the content of business customers' emails,
16 documents, contacts, calendars, location data, audio files, and video files in order to develop new
17 products and services sold to others; to glean business intelligence; and to otherwise derive
18 commercial benefit.

19
20 7. And Microsoft has falsely represented that Office 365 complies with System and
21 Organization Controls standards 1 and 2, nationally recognized standards designed to assure the
22 security, availability, processing integrity, confidentiality, and privacy of customer data.

23
24 8. Microsoft claims transparency about how it uses data and with whom data is
25 shared. But the company has not fully and openly disclosed its data use and sharing practices to
26 its business customers. To the contrary, Microsoft has misled its customers and failed to obtain
27
28

1 their consent before using and sharing their data for its purposes. It continues that course of
2 conduct to this day.³

3 9. Microsoft's practices violate federal laws governing the acquisition, use, and
4 sharing of electronic communications; state laws prohibiting deceptive advertising and unfair
5 acts and practices; and state privacy laws.

6
7 10. Plaintiffs bring this lawsuit to hold Microsoft accountable, expose and stop its
8 illegal conduct, and obtain compensation for all Office 365 and Exchange Online business
9 customers in America who paid for services and products that were not as Microsoft claimed.

10 **PARTIES AND PLAINTIFF-SPECIFIC ALLEGATIONS**

11 11. Plaintiffs Frank D. Russo, Koonan Litigation Consulting, LLC, and Sumner M.
12 Davenport & Associates, LLC are persons or companies that have subscribed to or purchased
13 business versions of Microsoft's services and products, as specified below. They seek to
14 represent a nationwide class of similarly situated Microsoft business customers.
15

16 12. Defendant Microsoft Corporation is a Washington corporation headquartered in
17 Redmond.

18 13. Plaintiff Frank D. Russo resides in Napa, California. He operates a sole
19 proprietorship called Russo Mediation & Law, which provides mediation, arbitration, and
20 alternative dispute resolution services to bring parties from conflict to resolution by establishing
21 rapport, earning trust, understanding perspectives, and overcoming legal, psychological, and
22 philosophical differences.
23

24
25
26
27
28

³ Unless specifically noted otherwise or made clear by the context, all conduct alleged in
this Complaint has taken place throughout the Class Period and is still taking place.

1 14. Since August 2015, Plaintiff Russo has paid approximately \$12.50 per month for
2 his subscription to Microsoft 365 Business Standard (formerly called “Office 365 Business
3 Premium”).

4 15. Plaintiff Russo is a regular user of Office 365 in the course of his business.

5 16. The privacy and security of Plaintiff Russo’s and his clients’ data are important
6 and material to him.

7 17. In deciding to subscribe to Office 365, Plaintiff Russo believed Microsoft would
8 keep Plaintiff Russo’s data private and secure.

9 18. Microsoft misrepresented and did not disclose to Plaintiff Russo material facts,
10 alleged more specifically below, regarding its use and protection of Plaintiff Russo’s data, and,
11 as a result, Plaintiff Russo was deceived. Had Microsoft not made these misrepresentations and
12 had it properly disclosed these facts, Plaintiff Russo would not have purchased his subscription,
13 or alternatively would have paid less for it.

14 19. Plaintiff Russo has started exploring what actions he can take, other than filing
15 this lawsuit, to protect himself from the actions by Microsoft described in this Complaint.

16 20. Plaintiff Koonan Litigation Consulting, LLC (“Plaintiff Koonan”) is a California
17 limited liability corporation headquartered in San Francisco, doing business with another
18 company as Chopra Koonan Litigation Services.

19 21. Plaintiff Koonan provides its clients with advice on how to succeed in all aspects
20 of litigation, including with case analysis, theme development, focus groups, mock trials, witness
21 preparation, opening statements, closing arguments, jury selection, and post-trial juror
22 interviews.

1 22. Since February 2016, Plaintiff Koonan has paid approximately \$119.88 annually
2 for its subscription to Microsoft 365 Business Basic (formerly called “Office 365 Business
3 Essentials”).

4 23. Plaintiff Koonan is a regular user of Office 365 in the course of its business.

5 24. The privacy and security of Plaintiff Koonan’s and its clients’ data are important
6 and material to it.

7 25. In deciding to subscribe to Office 365, Plaintiff Koonan believed Microsoft would
8 keep Plaintiff Koonan’s data private and secure.

9 26. Microsoft misrepresented and did not disclose to Plaintiff Koonan material facts,
10 alleged more specifically below, regarding its use and protection of Plaintiff Koonan’s data, and,
11 as a result, Plaintiff Koonan was deceived. Had Microsoft not made these misrepresentations and
12 had it properly disclosed these facts, Plaintiff Koonan would not have purchased its subscription,
13 or alternatively would have paid less for it.

14 27. Plaintiff Koonan has started exploring what action it can take, other than filing
15 this lawsuit, to protect itself from the actions by Microsoft described in this Complaint.

16 28. Plaintiff Sumner M. Davenport & Associates, LLC (“Plaintiff Davenport”), is a
17 Wyoming limited liability corporation. Plaintiff Davenport’s primary place of business is in
18 Woodland Hills, CA. Sumner Davenport is a California resident and has been throughout the
19 class period. Plaintiff Davenport is a marketing company that works with small businesses, and
20 charitable organizations on web accessibility, communication strategies, digital and print
21 marketing, reputation management, and research. Plaintiff Davenport serves clients throughout
22 Southern California.

23 29. Since 2016, Plaintiff Davenport has subscribed to Microsoft 365 Business
24 Standard (formerly called “Office 365 Business Premium”).
25

1 30. From approximately April 2016 through April 2018, Plaintiff Davenport paid
2 \$12.50 per month for its Microsoft 365 Business Standard account.

3 31. From approximately April 2018 through the present, Plaintiff Davenport paid an
4 annual subscription fee of \$150 for the Microsoft 365 Business Standard account.

5 32. Plaintiff Davenport purchased its subscription to Office 365 online.

6 33. Before purchasing Office 365, Plaintiff Davenport's principal, Sumner
7 Davenport, conducted online research to identify the best solution for its document management,
8 backup, and other business needs.

9 34. Plaintiff Davenport is a regular user of Office 365 in the course of its business.

10 35. The privacy and security of Plaintiff Davenport's and its clients' data are
11 important and material to Plaintiff Davenport.
12

13 36. In deciding to subscribe to Office 365, Plaintiff Davenport believed Microsoft
14 would keep Plaintiff Davenport's data private and secure.
15

16 37. Microsoft misrepresented and did not disclose to Plaintiff Davenport material
17 facts, alleged more specifically below, regarding its use and protection of Plaintiff Davenport's
18 data, and, as a result, Plaintiff Davenport was deceived. Had Microsoft not made these
19 misrepresentations and had it properly disclosed these facts, Plaintiff Davenport would not have
20 purchased its subscription, or alternatively would have paid less for it.
21

22 38. Since learning about Microsoft's improper sharing and use of business customer
23 data, Plaintiff Davenport has ceased recommending that its clients purchase Office 365.

24 39. Plaintiff Davenport is investigating replacing its Microsoft subscription with a
25 different solution, a transition that would require significant time and money.
26
27
28

JURISDICTION AND VENUE

1
2 40. The Court has subject matter jurisdiction under the Class Action Fairness Act,
3 codified at 28 U.S.C. § 1332(d)(2). The matter in controversy exceeds the sum or value of
4 \$5,000,000, exclusive of interest and costs, and is a class action in which any member of the
5 class is a citizen of a State different from the Defendant.
6

7 41. Further, this matter also arises under the Wiretap Act, 18 U.S.C. § 2511, and the
8 Stored Communications Act, 18 U.S.C. § 2702. The dispute is thus premised on a federal
9 question, for which jurisdiction resides in this Court under 28 U.S.C. § 1331.

10 42. Insofar as Plaintiffs assert claims arising under state law, supplemental
11 jurisdiction lies in this Court under 28 U.S.C. § 1367(a), as those claims are so related to
12 Plaintiffs’ federal claims that they form part of the same case or controversy.
13

14 43. In addition, Plaintiffs’ claims arose and were caused by Microsoft’s actions in
15 California. Microsoft’s misrepresentations to Plaintiffs and other actions took place in California,
16 were aimed at Plaintiffs in California, and injured Plaintiffs in California. Microsoft knew its
17 actions could reasonably and fairly subject it to suit and specific jurisdiction in California.

18 44. Microsoft’s acts and omissions giving rise to Plaintiffs’ claims were directed at
19 Plaintiffs Russo and Koonan at their respective headquarters in Napa and San Francisco, in the
20 Northern District of California. This District is therefore a proper venue for this action, as
21 prescribed by 28 U.S.C. § 1391.
22

23 **FACTS**

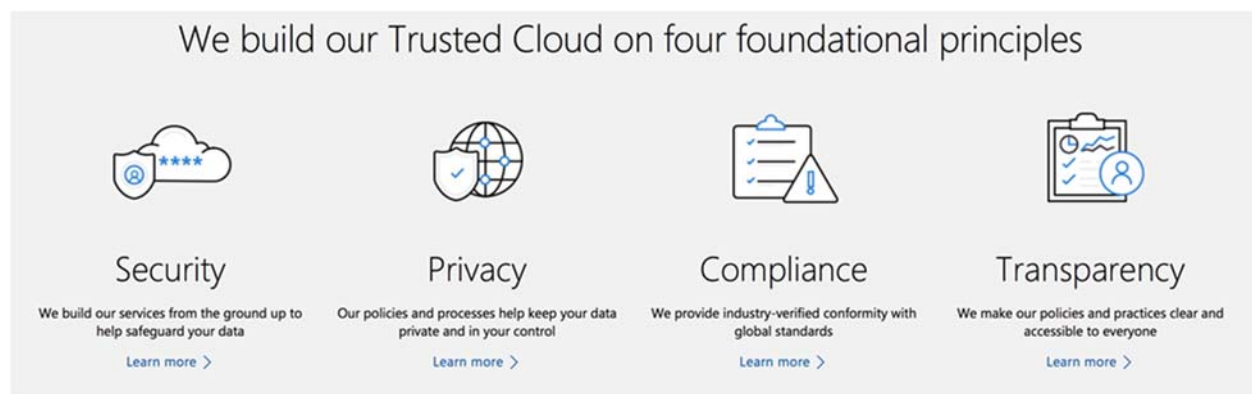
24 **A. MICROSOFT TRANSITIONED BUSINESS CUSTOMERS TO ITS**
25 **CLOUD-BASED SERVICES, ASSURING THEM THEIR DATA WOULD**
26 **BE PRIVATE AND SECURE.**

27 45. As the largest software company in the world, Microsoft led the transition to
28 cloud computing.

1 46. Building on the enormous success of its Office suite of software products
 2 (including Word, Outlook, Excel, and PowerPoint), Microsoft developed Office 365 as a cloud-
 3 based “software-as-a-service” version of those popular offerings, for which customers would pay
 4 a monthly subscription fee.

5 47. “Trust” has been—and is—the centerpiece of Microsoft’s advertising campaigns
 6 for its cloud-based business services and products. In its website “Trust Center,” Microsoft
 7 promises it abides by the most “stringent privacy standards” and provides FAQs, videos, top-10
 8 lists, and whitepapers declaring fidelity to customers’ privacy demands.

9 48. Microsoft has focused on “trust” because it recognizes that “[o]ur business can
 10 succeed only if our customers trust us to protect their privacy and use their data in the ways that
 11 they permit us.” As Microsoft Corporate Vice President and Deputy General Counsel Rich Sauer
 12 put it, Microsoft’s corporate mission “depends on our ability to win and retain our users’ trust.”
 13 And internal Microsoft documents recognize that business customers will not use Microsoft’s
 14 online services and products if they lack strong privacy protections. Microsoft touts security,
 15 privacy, compliance, and transparency as the “foundational principles” of its “Trusted Cloud”:
 16
 17



25 49. Microsoft’s marketing focus on privacy and security is also calculated to increase
 26 its bottom line. In internal documents, Microsoft identified privacy as a “competitive
 27 differentiator,” noting that “[l]oyalty goes up with choice and control.”
 28

1 50. Microsoft knew that its customers were concerned about the security of storing
2 information outside of their own networks or in a cloud infrastructure. As Microsoft put it,
3 “[C]ustomers of all kinds have the same basic concerns about moving to the cloud. They want to
4 retain control of their data, and they want that data to be kept secure and private[.]”

5
6 51. A business’s data is among the most valuable assets it owns. Business data
7 typically includes sensitive information, such as confidential financial details, secret business
8 ideas, plans for new products or services, trade secrets, and other proprietary business insights
9 and intelligence.

10 52. Business data can also include personal information about the businesses’
11 customers and employees, including banking information, social security numbers, and other
12 legally protected personally identifying information.

13
14 53. Businesses must protect their data, and they will pay more for that protection.

15 **B. MICROSOFT REPRESENTED TO BUSINESS CUSTOMERS IT WOULD**
16 **USE THEIR DATA ONLY TO PROVIDE THE SERVICES THEY**
PURCHASED.

17 54. In its agreements and marketing materials directed to its business customers,
18 Microsoft consistently represented that it would use their data only to provide them with the
19 specific services they purchased.

20 55. Microsoft’s agreements with its business customers define “customer data” as “all
21 data, including all text, sound, software, image or video files that are provided to Microsoft by,
22 or on behalf of, Customer” through the use of Office 365 or Exchange Online.

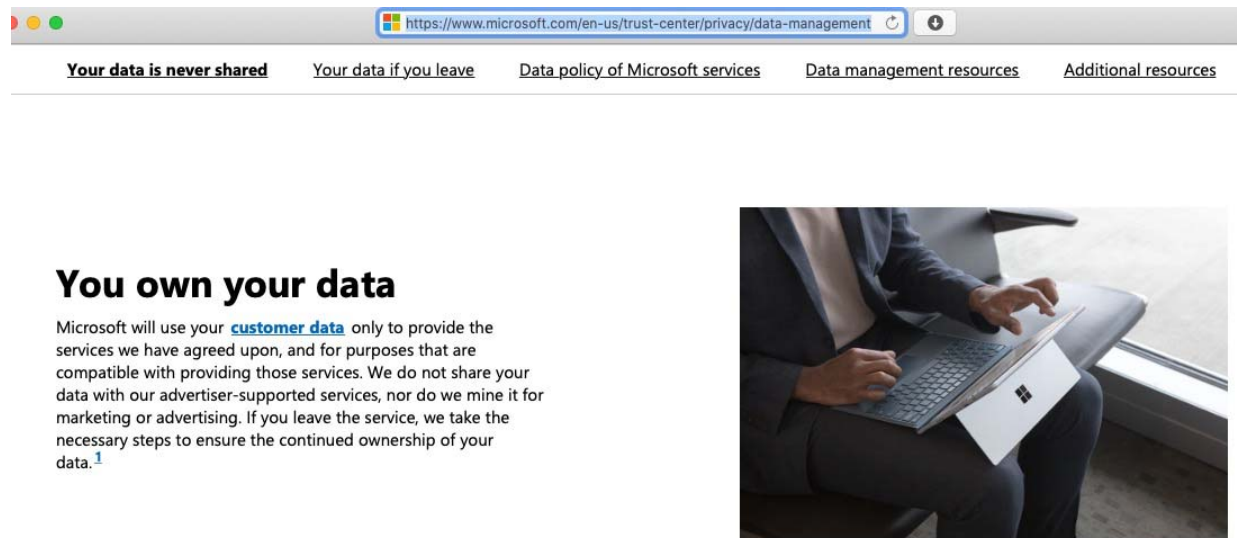
23
24 56. “Customer data” includes the customer’s “content,” *i.e.*, what Microsoft
25 customers create, communicate, and store on or through Microsoft’s services, such as the words
26 in an email exchanged between friends or business colleagues, and the photographs and
27 documents stored on Office 365 or Exchange Online.
28

1 57. Customer data also includes Exchange Online emails and attachments, Power BI
2 (business intelligence) reports, SharePoint Online site content, and instant message (“IM”)
3 conversations.

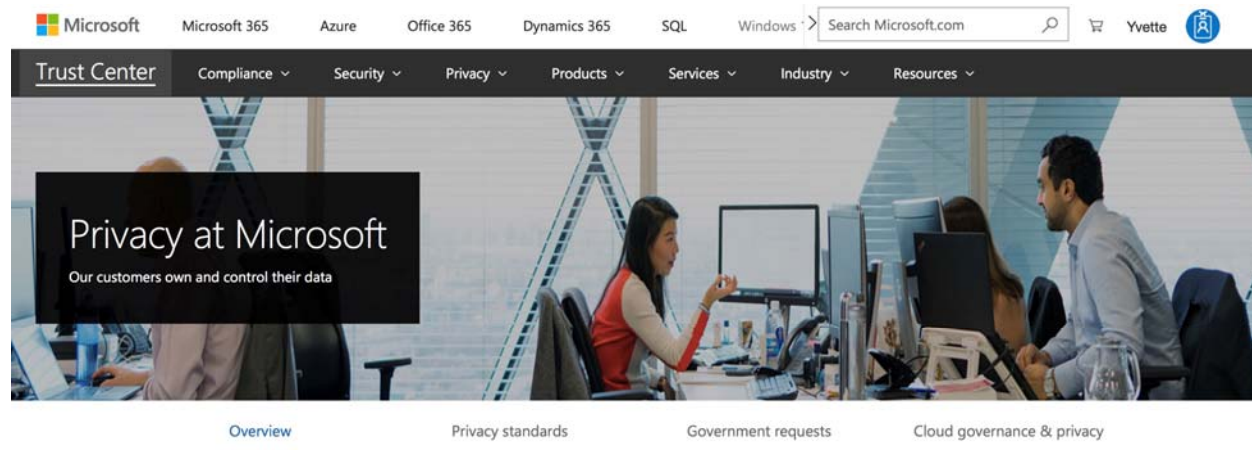
4 58. Throughout its Trust Center, and in its related marketing materials, whitepapers,
5 technical instructions, and other representations and documents, Microsoft has consistently
6 represented to its business customers that their data will not be used for any purpose other than
7 providing the specific services the customer has purchased. For example:
8

- 9 a. On a marketing page of its website, Microsoft promises, “We use
10 your data for just what you pay us for: to maintain and provide
11 Office 365[.] We make it our policy to not use your data for other
12 purposes.”
- 13 b. Similarly, in a whitepaper, Microsoft says that it “uses customer
14 data only for providing cloud services... We also don’t scan our
15 customers’ email or documents for building analytics, data mining,
16 advertising, or improving services without our customers’
17 permission.”
- 18 c. And in webpages designed to provide more technical information,
19 Microsoft promises: “We use customer data only to provide the
20 services; therefore, Microsoft strictly prohibits access to customer
21 data for any other purpose.”

22 59. Microsoft has also repeatedly guaranteed its business customers that they—and
23 they alone—have control of their data. The Trust Center screenshot below is typical of the tone,
24 tenor, and content of Microsoft’s efforts and promises in this regard:
25
26
27
28



10 60. This representation has remained consistent throughout the class period. For
11 example, prior versions of Microsoft's webpages similarly promised:



20 You own and control your data

21 Microsoft understands that when you, our customer, use our business cloud services, you are entrusting us with your most valuable asset—your data. You trust that its privacy will be
22 protected and that it will be used only in a way that is consistent with your expectations.

23 Our time-tested approach to privacy is grounded in our commitment to give you control over the collection, use, and distribution of your [customer data](#). We are transparent about the
24 specific policies, operational practices, and technologies that help ensure the privacy of your data in Microsoft business cloud services.

25 The Trust Center site provides legal and compliance teams with a comprehensive repository of information resources designed to help them understand and verify the compliance
26 requirements of their organization's cloud deployments.

- 27 • [You know how we manage your data](#). We use your customer data only to provide the services we have agreed upon, and do not mine it for marketing or advertising. If you
28 leave the service, Microsoft follows strict standards and specific processes for removing data from our systems.
- [You know where your data is located](#). Customers who must maintain their data in a specific geographic location, such as within the EU, can rely on our expanding network of
datacenters around the world. Microsoft also complies with international data protection laws regarding transfers of customer data across borders.
- [You know who can access your data and on what terms](#). We take strong measures to protect your data from inappropriate access, including limits for Microsoft personnel and
subcontractors. However, you can access your own customer data at any time and for any reason.
- [You know how we respond to government and law enforcement requests to access your customer data](#).
- [We set and adhere to stringent privacy standards](#). Strong contractual commitments back our privacy standards and best practices.

1 61. These guarantees have been repeated to Microsoft’s business customers in myriad
2 materials. For example:

- 3 a. “As a customer of Office 365, you own and control your data. We
4 do not use your data for anything other than providing you with the
5 service that you have subscribed for.... You own your data and
6 retain all rights, title, and interest in the data you store with Office
7 365.”
8 b. “Our cloud services allow you to control who has access to your
9 data, and how it’s shared And you can take your data with you
10 when you leave.”

11 62. To that end, Microsoft has promised its customers that they can easily learn who
12 has access to their data, and that they can terminate that access if they wish. For example:

- 13 a. “We are transparent about our privacy practices and offer
14 meaningful privacy choices.”
15 b. “We will be transparent about data collection and use so you can
16 make informed decisions. . . . Also, you can take your data with you
17 if you end your subscription.”
18 c. “With Office 365, it’s your data. You own it. You control it And it
19 is yours to take with you if you decide to leave the service You
20 know where your data resides and who has access.”
21 d. “We provide you with clear explanations about . . . who can access
22 [your data] and under what circumstances.”

23 63. Microsoft has also regularly represented that it “will not transfer to any third party
24 (not even for storage purposes) data that you provide to Microsoft through the use of our
25 business cloud services that are covered under the Microsoft Online Services Terms.”

26 64. Microsoft has made—and continues to make—these and similar representations
27 in many other marketing materials, too numerous and voluminous to list.

28 65. Microsoft has also made—and continues to make—these representations in its
Online Service Terms, which apply to all business customers. In the Online Service Terms, and
more specifically its 2020 Data Protection Agreement (“DPA”), Microsoft promised all business

1 customers in the putative class that it would use their data “only (a) to provide Customer the
2 Online Services in accordance with Customer’s documented instructions, and (b) for Microsoft’s
3 legitimate business operations, each as detailed and limited below.” The DPA clarifies that the
4 customer, not Microsoft, “retains all right, title and interest in and to Customer Data,” and
5 narrowly defines the provision of online service as “[d]elivering functional capabilities” of the
6 product purchased, troubleshooting problems, and improving the product through updates to
7 improve “user productivity, reliability, efficacy, and security.”

9 66. And the DPA specifies that Microsoft will not use business customer data for a
10 broad range of activities unrelated to providing the purchased product, including “(a) user
11 profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at
12 creating new functionalities, services, or products or any other purpose, unless such use or
13 processing is in accordance with Customer’s documented instructions.”

15 67. Though Microsoft amends the Online Service Terms from time to time, they have
16 not materially changed vis-à-vis the putative class members and their claims during the class
17 period.

18 68. For example, in the 2015 Online Service Terms, Microsoft promised its business
19 customers:

21 Customer Data will be used only to provide Customer the Online Services
22 including purposes compatible with providing those services. Microsoft
23 will not use Customer Data or derive information from it for any
24 advertising or similar commercial purposes. . . . Microsoft will not disclose
Customer Data or Support Data outside of Microsoft or its controlled
subsidiaries and affiliates except (1) as Customer directs, (2) as described
in the [Online Service Terms], or (3) as required by law.

25 69. Microsoft further “agrees and warrants . . . to process the personal data only on
26 behalf of” the Microsoft business customer.

1 70. Microsoft commits, moreover, that it “shall not subcontract any of its processing
2 operations performed on behalf of” the Microsoft business customer without the customer’s prior
3 written consent.

4 71. Microsoft’s subscription and licensing agreements with class members reinforce
5 these representations. For example, Microsoft’s Business and Services Agreement says it will
6 use business customer data “only for purposes of the parties’ business relationship. [Microsoft
7 will not] disclose [customer data] to third parties, except to its employees, Affiliates, contractors,
8 advisors, and consultants (‘Representatives’) and then only on a need-to-know basis[.]”

9
10 72. Similarly, Microsoft’s Open Value Agreement states that it will use business
11 customer data “only for purposes of the parties’ business relationship under this Agreement.
12 [Microsoft will not] disclose that information to third parties, except to its employees, Affiliates,
13 resellers, contractors, advisors, and consultants (collectively, ‘Representatives’) and then only on
14 a need-to-know basis[.]”

15
16 73. Reaffirming that message, Microsoft’s Cloud Agreement and Open License
17 Agreement say that the customer consents only “to the processing of personal information by
18 Microsoft and its agents to facilitate the subject matter of this agreement.”

19 **C. MICROSOFT’S REPRESENTATIONS WERE FALSE.**

20
21 **1. Microsoft shares its business customers’ data with Facebook and other third
parties, without its business customers’ consent.**

22 74. Facebook is the world’s largest social media network, with over two billion active
23 users. Its business model relies on using and sharing its users’ data.

24
25 75. Although Facebook is not necessary to provide Office 365 or Exchange Online
26 services to Microsoft’s business customers, Microsoft routinely and automatically shares its
27 business customers’ contacts with Facebook—without those customers’ consent— whether or
28 not the customers or their contacts are Facebook users.

1 76. Even if a customer discovers and disables this Facebook-sharing “feature” after
2 activating Office 365 or Exchange Online services, the damage has already been done. At that
3 point, the business customer’s contacts have been shared with Facebook. As Microsoft explains
4 in an obscure technical instruction, “[o]nce contacts are transferred to Facebook, they cannot be
5 deleted from Facebook’s systems except by Facebook.”
6

7 77. Because Microsoft shares its business customers’ contact data with Facebook, its
8 customers’ data is accessible not just by Facebook, but also by whomever Facebook shares the
9 data with, and whomever *those* entities decide to share the data with, *ad infinitum*.

10 78. For example, after Facebook gave limited data access to University of Cambridge
11 psychology lecturer Aleksandr Kogan, data of 87 million persons were exploited by Cambridge
12 Analytica, a data mining firm that focuses on opposition research and intelligence gathering for
13 political campaigns.
14

15 79. With Facebook’s data, Cambridge Analytica was able to create a political
16 microtargeting platform that identified which issues mattered to the voter and, with eerie
17 precision, use machine learning and sentiment manipulation to influence them to vote (or not
18 vote).
19

20 80. Cybercriminals and hackers use Facebook data to tie an individual or company to
21 datasets previously scrubbed of identifying information. By piecing together seemingly random
22 data points, hackers and cybercriminals are able to sell sensitive commercial information in the
23 black market or the dark web, from login passwords to inside information that make for
24 profitable stock trades.
25
26
27
28

1 **2. Microsoft shares its business customers’ data with third-party developers,**
2 **without its business customers’ consent.**

3 81. Despite its promises, Microsoft shares its business customers’ data with third-
4 party developers, so they can develop and sell new services and products, at additional profit to
5 Microsoft, either directly or indirectly.

6 82. For instance, even if a business customer did not download a third-party
7 application (and thus did not consent to sharing its data with the third-party), Microsoft
8 nonetheless transmits the non-consenting business customer’s data to third-party developers if
9 *another* Office 365 user consented to the application.

10 83. Among other things, Microsoft gives third-party developers information about the
11 documents and projects those non-consenting business customers worked on. Microsoft allows
12 those third-party developers to search the content of its business customers’ emails and to access
13 their schedules, locations, and availability status, *i.e.*, whether they are “available” or “away.”

14 84. In advertising its developer platform to third-party developers, Microsoft touts the
15 enormous value of its customers’ data, highlighting how developers will get data not just about
16 the authorized user, but also about other users who communicate with the authorized user. For
17 example, Microsoft explains to developers that they can “perform searches for people who are
18 relevant to the [Microsoft] user and have expressed an interest in communicating with that user”
19 about specific topics, such as pizzas. Microsoft explains that “[t]opics in this context are just
20 words that have been used most by users in email conversations. Microsoft extracts such words
21 and creates an index for this data to facilitate . . . searches.”
22

23 85. Microsoft does not require those third-party developers to employ the security
24 measures that Microsoft has promised its business customers. Instead, Microsoft only requests
25 that they employ “reasonable security measures.” The actual level of security used by those
26 third-party developers is unknown and not reasonably knowable to Plaintiffs.
27
28

1 86. Microsoft profits from sharing its business customers' Office 365 data by
2 charging the developers directly for access, accepting a commission from sales of the products
3 developed from its customers' data, or other means.

4 **3. Microsoft shares its business customers' data with hundreds of**
5 **subcontractors when sharing is not needed to provide the services, and**
6 **without requiring the subcontractors to keep the data private and secure.**

7 87. Microsoft uses and shares business customers' data—including the content of
8 their documents, emails, email attachments, text, audio, and video files—with hundreds of
9 subcontractors (or "subprocessors," as Microsoft sometimes calls them), not only to provide
10 customers with the services they purchased, but also to serve Microsoft's separate commercial
11 ventures, including discovering new business insights and developing new services, products, or
12 features for Microsoft's benefit, such as artificial intelligence applications and development
13 interfaces.

14 88. Microsoft does not anonymize or obscure business customers' data before
15 transmitting it to third-party subcontractors. Instead, Microsoft anonymizes only a minuscule
16 portion of customers' data, *e.g.*, social security numbers or credit card numbers, and does not
17 disclose that fact to its business customers.

18 89. Microsoft does not require its subcontractors to encrypt business customers' data
19 and does not disclose that fact to its business customers. Rather, Microsoft requires these
20 subcontractors to encrypt only a limited subset of the data (and only when at rest)—usernames
21 and passwords, credit card and bank account numbers, medical record numbers or biometric
22 identifiers, and government-issued identification data.

23 90. Microsoft's sharing of its business customers' data with its subcontractors creates
24 a security and privacy risk, is not disclosed, and is contrary to the representations Microsoft
25 makes to its business customers regarding data privacy and security.
26
27
28

1 **4. Microsoft uses its business customers’ data to develop and sell new products**
2 **and services—and otherwise benefit itself.**

3 91. Contrary to its disclosures to and agreements with its business customers,
4 Microsoft uses its business customers’ data to develop and sell new products and services that
5 benefit only Microsoft.

6 92. Despite Microsoft’s repeated assurances that it will use its business customers’
7 data only to provide them with the services they purchased, Microsoft mines that data to develop
8 new products that it sells to other customers.

9 93. Microsoft harvests business customer data to develop and sell other products,
10 including Security Graph API, an application program interface Microsoft sells to software
11 developers so they can create new security-related products.

12 94. Microsoft boasts that Security Graph API is built off the “uniquely broad and
13 deep” insights Microsoft obtained for itself by scanning “400 billion” of its customers’ emails
14 and “data from 700 million Azure user accounts.”

15 95. Microsoft also harvests business customer data to develop and sell to others a
16 marketing product called Microsoft Audience Network, which Microsoft admits derives
17 enormous value from processing customer data. In Microsoft’s own words:
18

19 What sets Microsoft Audience Ads apart is their rich user understanding that
20 powers high performance. The Microsoft Graph consists of robust data sets,
21 including search and web activity, LinkedIn professional profiles,
22 demographics and more. The data is continually updated every second based
23 on user activities. By mapping audience data on such an enormous scale, the
Graph helps us spot trends and uncover insights, both of which allow you to
effectively reach your customers.

24 96. Microsoft also uses business customer data to create other applications it sells to
25 other customers, including Windows Defender Application Control, Azure Advanced Threat
26 Protection, and Advanced Threat Protection.
27
28

1 97. As another example, through a default setting that applies when the customer first
2 installs Office 365, Microsoft collects and uses business customer data (including documents,
3 contacts, and calendar information) to develop and improve its virtual personal assistant
4 “Cortana.” It does so even if the customer is not using Cortana.

5 98. These separate products, including Security Graph, Microsoft Audience Network,
6 and Cortana, are not necessary to provide Office 365 services.

7 99. In sum, despite its promises to use business customers’ data only for the purpose
8 of providing the customers with the purchased services, Microsoft uses the data for its own
9 purposes: to create and sell new products to others.

10
11 **D. MICROSOFT MISREPRESENTS THE SECURITY IT PROVIDES FOR**
12 **BUSINESS CUSTOMERS’ DATA.**

13 100. Microsoft not only misleads its business customers as to how it shares and uses
14 their data, but also regarding how it protects and processes that data.

15 101. Microsoft knows that business customers would not share their data with a service
16 provider whose security that did not comply with “System and Organization Controls” or “SOC”
17 standards.

18 102. “SOC” is the standard adopted by the American Institute of Certified Public
19 Accountants for controls that safeguard the confidentiality and privacy of information stored and
20 processed in the cloud.

21 103. Microsoft also knows that many business customers must satisfy SOC compliance
22 for their own business operations. For example, businesses performing services for governmental
23 or quasi-governmental entities must satisfy SOC compliance requirements.

24 104. Microsoft promises business customers that it complies with SOC 1 and SOC 2
25 standards. For example, in Microsoft’s “Trust Center,” Microsoft states:
26
27
28



SOC 1, 2, and 3 Reports

Microsoft cloud services comply with Service Organization Controls standards for operational security.

105. Microsoft represents in addition:

Microsoft cloud services comply with Service Organization Controls standards for operational security.

....

Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports.

106. Microsoft makes this representation for all products at issue in this action – including Office 365 and Exchange Online.

107. Microsoft encourages its customers to rely on its promises of SOC compliance. For example, as Microsoft explains through one of its marketing materials:

Q. Can I leverage Microsoft’s compliance in my organization’s certification process?

Yes. When you migrate your applications and data to Microsoft’s covered cloud services, you can build on the audits and certifications that Microsoft holds. The independent reports attest to the effectiveness of controls Microsoft has implemented to help maintain the security and privacy of your data.

108. These promises are false.

1 109. By default, automatically and without its customers' knowledge or consent,
2 Microsoft harvests its business customers' data into a separate product, Graph.

3 110. As Microsoft recognizes, Graph collects "the things they care about most: their
4 mail, calendars, contacts, users and groups, files, and folders."

5 111. Microsoft's Graph also analyzes the relationships between pieces of business
6 customer data. For example, for Outlook contacts, Graph aggregates information about a
7 particular contact from across e-mail, social networks, Skype, and others, and exposes the
8 relationships between the data.

9 112. As Microsoft admits in its own documentation, Graph complies with neither
10 SOC-1 nor SOC-2 standards:

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Microsoft Graph	Yes	Yes	Yes	No	No

13
14 113. Because Microsoft's Graph automatically gathers all business customers' Office
15 365 and Exchange Online data, and Graph does not comply with SOC standards, Microsoft's
16 handling and use of business customers' Office 365 and Exchange Online data also does not
17 comply with SOC standards.

18 **E. MICROSOFT'S ACTIONS HAVE INJURED PLAINTIFFS AND OTHER**
19 **BUSINESS CUSTOMERS.**

20 114. Plaintiffs and Microsoft's other business customers would not have purchased (or
21 would have paid less for) Microsoft's services if Microsoft had not made the misrepresentations
22 discussed above and had disclosed its sharing and use of its customers' data.

23 115. Microsoft's use and sharing of Plaintiffs' and Microsoft's other business
24 customers' data also reduced their data's privacy and security.
25
26
27
28

CLASS ACTION ALLEGATIONS

1
2 116. Plaintiffs make these allegations on their own behalf, and on behalf of a class of
3 similarly situated Microsoft business customers (“Class Members”), defined as:

4 All persons and non-governmental entities in the United States who
5 subscribed to or purchased Microsoft Office 365 Business, Microsoft
6 Office 365 Business Essentials, Microsoft Office 365 Business Premium,
7 Exchange Online Plan 1, Exchange Online Plan 2, Microsoft Office 365
8 Enterprise, Office 365 Enterprise, Microsoft 365 Enterprise, Microsoft 365
9 Business, Office 365 Business, Office 365 Pro Plus, Office 365 Business
10 Essentials, Office 365 Business Premium, Microsoft 365 Business Basic,
11 Microsoft 365 Business Standard, or Microsoft 365 Business Premium, but
12 did not subscribe to or purchase Microsoft Cognitive Services, from July
13 17, 2016 through the present (the “Class Period”).

14 117. Excluded from the Class are governmental entities, Microsoft and any entity in
15 which Microsoft has a controlling interest, Microsoft’s employees, any Judge to whom this
16 action is assigned, any member of the Judge’s staff or immediate family, and counsel for any
17 party.

18 118. Plaintiffs reserve the right to alter their proposed class definition as warranted by
19 the evidence obtained through discovery.

20 119. Class Members are readily ascertainable based on Microsoft’s own records.

21 120. The proposed class meets all certification requirements of Federal Rules of Civil
22 Procedure 23(a) and 23(b)(3).

23 121. Because there are millions of Class Members, the Class is sufficiently numerous.

24 122. There are many questions of law or fact common to Plaintiffs and Class Members,
25 including:

- 26 a. Whether Microsoft engaged in false, deceptive, or misleading
27 business practices;
- 28 b. Whether Microsoft used the Class Members’ data for its own
unauthorized, commercial purposes;

- 1 c. Whether Microsoft shared the Class Members' data with
- 2 unauthorized third parties;
- 3 d. Whether the Class Members consented to Microsoft's sharing and
- 4 use of their data;
- 5 e. Whether the Class Members are entitled to statutory damages for
- 6 Microsoft's actions;
- 7 f. Whether Microsoft's conduct violated the statutes as alleged below;
- 8 g. Whether the Class Members are entitled to compensatory damages
- 9 for Microsoft's actions;
- 10 h. Whether the Class Members are entitled to punitive damages for
- 11 Microsoft's actions; and
- 12 i. Whether the Class Members are entitled to declaratory and
- 13 injunctive relief for Microsoft's actions.

14 123. Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs have
15 suffered the same injuries as other Class Members, and their interests are aligned with the
16 interests of the other Class Members.

17 124. Plaintiffs subscribed to or purchased substantially the same services or products
18 as all Class Members; Microsoft made the same material misrepresentations and omissions to
19 each Class Member; these misrepresentations were false and omissions were wrongful for the
20 same reasons; each Class Member's data was wrongfully used and shared, and Microsoft
21 otherwise violated Plaintiffs' and the Class Members' rights in the same way.

22 125. Plaintiffs are adequate representatives of the Class with no conflicts of interest
23 who have obtained capable and experienced counsel to prosecute the Class Members' claims.

24 126. Questions and issues common to the Class will predominate over any
25 individualized inquiries.

26 127. A class action is superior to individual cases, especially because the costs of
27 litigating individual Class Members' claims would far surpass their individual recoveries.

APPLICABLE LAW

1
2 128. The federal claims in this case are based on the statutes cited in Counts One and
3 Two below.

4 129. The state law claims are based on Washington statutory and common law because
5 Microsoft has chosen the nationwide application of Washington law to its business customers.
6

7 130. For example, Microsoft’s Open Value Agreement provides: “Applicable law. The
8 terms of this agreement entered into with any Microsoft Affiliate located outside of Europe will
9 be governed by and construed in accordance with the laws of the State of Washington and
10 federal laws of the United States.”

11 131. Similarly, Microsoft’s Business and Services Agreement provides as follows:
12 “Applicable law. The terms of this agreement and/or any Supplemental Agreement entered into
13 with any Microsoft Affiliate located outside of Europe will be governed by and construed in
14 accordance with the laws of the State of Washington and federal laws of the United States.”
15

16 132. Microsoft’s other subscription and license agreements for business customers also
17 state that its terms are to be governed by federal law and Washington state law.

18 133. State choice of law principles also make the application of Washington state law
19 appropriate in this case.
20

21 **Count One**
22 **Violations of the Wiretap Act**
23 **18 U.S.C. §§ 2511(1)(a), (1)(c), and (1)(d)**
24 **On behalf of Plaintiffs and the Class**

25 134. The Wiretap Act, 18 U.S.C. § 2520, provides for damages and other relief against
26 any person who:

- 27 a. intentionally intercepts or endeavors to intercept the contents of any
28 electronic communication, *id.* § 2511(1)(a).

- 1 b. intentionally discloses or endeavors to disclose to any other person
- 2 the contents of any electronic communication, knowing or having
- 3 reason to know that the information was obtained through the
- 4 interception of an electronic communication, *id.* § 2511(1)(c); or
- 5 c. intentionally uses or endeavors to use the contents of any electronic
- 6 communication, knowing or having reason to know that the
- 7 information was obtained through the interception of an electronic
- 8 communication, *id.* § 2511(1)(d).

9 135. Business customer data transferred to Microsoft at the time of transmission
10 through the customer’s use of Office 365 or Exchange Online is an “electronic communication,”
11 which is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence
12 of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or
13 photooptical system that affects interstate or foreign commerce.” *Id.* § 2510(12).

14 136. Plaintiffs and Class Members are “persons” under the Wiretap Act because they
15 are an “individual, partnership, association, joint stock company, trust, or corporation.” *Id.*
16 § 2510(6).

17 137. Plaintiffs and Class Members are “users” under the Wiretap Act because they use
18 Office 365 or Exchange Online, each of which is “an electronic communication service,” and
19 they are “duly authorized by [Microsoft] to engage in such use.” *Id.* § 2510(13).

20 138. Plaintiffs and Class Members are “aggrieved persons” under the Wiretap Act
21 because they are “a person who was a party to any intercepted . . . electronic communication or a
22 person against whom the interception was directed[.]” *id.* § 2510(11), and they assert violations
23 of 18 U.S.C. §§ 2511(1)(a), (1)(c), and (1)(d) for Microsoft’s unlawful interception, disclosure,
24 and use of their electronic communications.

25 139. Microsoft is a “person” under 18 U.S.C. § 2510(6) because it is an “individual,
26 partnership, association, joint stock company, trust, or corporation.”
27
28

1 140. Microsoft’s cloud infrastructure is a “device” because it “can be used to intercept
2 [an] . . . electronic communication[.]” *Id.* § 2510(5).

3 141. As alleged more fully above, Microsoft unlawfully intercepted in transmission,
4 disclosed, and used without consent the Plaintiffs’ and Class Members’ data in the following
5 non-exhaustive ways:

- 6 a. Microsoft obtained the content of their emails, documents, contacts,
7 calendars, location data, audio files, photographs, and video files;
- 8 b. Microsoft shared that data with unauthorized third parties, including
9 Facebook, software application developers, and hundreds of
10 subcontractors, who use the data for their own purposes, or for
11 purposes that benefit Microsoft; and
- 12 c. Microsoft used the data to glean business intelligence and develop
13 new products – such as Microsoft Graph, Security Graph API,
14 Audience Network, Windows Defender Application Control, Azure
Advanced Threat Protection, and Advanced Threat Protection – to
sell to others, and to improve products such as Cortana, regardless
of whether the business customer uses Cortana.

15 142. Through its use and sharing of business customer data as alleged above, Microsoft
16 has intentionally **intercepted** or endeavored to intercept the contents of Plaintiffs’ and Class
17 Members’ electronic communications, without consent, in violation of 18 U.S.C. § 2511(1)(a).

18 143. Microsoft is not the intended recipient of the electronic communications and is
19 not a party to those communications. For example, in the case of emails sent by Plaintiffs and
20 Class Members, the intended recipient was not Microsoft, but the person or entity to whom the
21 email was addressed.

22 144. Microsoft’s intentional interception of Plaintiffs’ and Class Members’ data is not
23 necessary or incidental to and does not facilitate the transmission of Plaintiffs’ and Class
24 Members’ data. It is not needed to provide Plaintiffs and Class Members the Microsoft services
25 for which they subscribed.
26
27
28

- 1 b. knowingly divulges to others the contents of electronic
2 communications maintained on Microsoft’s service on behalf of,
3 and received by means of electronic transmission from, Plaintiffs
4 and Class Members, *id.* § 2702(a)(2)(A); or
- 5 c. knowingly divulges to others the contents of electronic
6 communications carried or maintained on Microsoft’s service solely
7 for the purpose of providing storage or computer processing
8 services to Plaintiffs and Class Members, *id.* § 2702(a)(2)(B).

9 149. Plaintiffs assert claims under the Stored Communications Act in the alternative to
10 the Wiretap Act claim, in the event the Court finds that Microsoft obtains Plaintiffs’ and Class
11 Members’ data while they are in “storage” rather than in “transit.”

12 150. Microsoft provides an “electronic communications service” because it “provides
13 to users thereof the ability to send or receive wire or electronic communications.” *Id.* § 2510(15).

14 151. Plaintiffs’ and Class Members’ electronic communications are in “electronic
15 storage” because, incidental to their electronic transmission, they are kept in temporary,
16 intermediate storage. *Id.* § 2510(17).

17 152. Microsoft provides “remote computing service[s]” because it provides to the
18 public “computer storage or processing services by means of an electronic communications
19 system.” *Id.* § 2711(2).

20 153. As alleged more fully above, Microsoft violated the Stored Communications Act
21 with respect to the Plaintiffs and Class Members in the following non-exhaustive ways:

- 22 a. Microsoft obtained the content of their emails, documents, contacts,
23 calendars, location data, audio files, photographs, and video files,
24 without consent;
- 25 b. Microsoft shared that data with unauthorized third parties, including
26 Facebook, software application developers, and hundreds of
27 subcontractors, who use the data for their own purposes, or for
28 purposes that benefit Microsoft, without consent; and

1 c. Microsoft used the data to glean business intelligence and develop
2 new products – such as Microsoft Graph, Security Graph API,
3 Audience Network, Windows Defender Application Control, Azure
4 Advanced Threat Protection, and Advanced Threat Protection – to
sell to others, and to improve products such as Cortana, regardless
of whether the business customer uses Cortana, without consent.

5 154. Microsoft accessed without authorization its cloud infrastructure, which is “a
6 facility through which an electronic communication service is provided,” and obtained access to
7 Plaintiffs’ and Class Members’ electronic communications, in violation of 18 U.S.C. §
8 2701(a)(1).

9 155. Through its use and sharing of business customer data as alleged above, Microsoft
10 knowingly divulged to other entities the contents of Plaintiffs’ and Class Members’ electronic
11 communications while in electronic storage by Microsoft, in violation of 18 U.S.C. § 2702(a)(1).

12 156. Through its use and sharing of business customer data as alleged above, Microsoft
13 (as a provider of remote computing services) knowingly divulged to other entities the contents of
14 Plaintiffs’ and Class Members’ electronic communications carried or maintained on Microsoft’s
15 service, in violation of 18 U.S.C. § 2702(a)(2).

16 157. Under § 2702(a)(2)(A), Plaintiffs’ and Class Members’ electronic
17 communications are maintained on Microsoft’s servers on their behalf, as they are subscribers
18 and customers of Microsoft’s service. Microsoft receives their electronic communications by
19 means of electronic transmission (or by means of computer processing of communications
20 received by means of electronic transmission) from them.

21 158. Under § 2702(a)(2)(B), Plaintiffs’ and Class Members’ electronic
22 communications are carried or maintained on Microsoft’s service solely for the purpose of
23 providing storage or computer processing services to them, and Microsoft is not authorized to
24 access the contents of their communications for purposes of providing any services other than
25 storage or computer processing.
26
27
28

1 164. As set forth above, Microsoft engaged in unfair and deceptive acts or practices by
2 adopting patterns and practices of:

- 3 a. making representations, omissions, and solicitations that,
4 considering their net impression and viewed as a whole, have the
5 capacity to deceive the purchasing public regarding Microsoft's use
6 and sharing of business customer data, and its compliance with
7 SOC standards;
- 8 b. failing to disclose material facts regarding its use and sharing of
9 business customer data and compliance with SOC standards;
- 10 c. diminishing the security and privacy of its customers' data through
11 its use and sharing of that data and noncompliance with SOC
12 standards;
- 13 d. diminishing the security and privacy of its customers' data through
14 its failure to adopt and enforce adequate data security protections,
15 including SOC standards, both on its own systems and in the
16 systems of third parties and representatives with which Microsoft
17 has shared or transferred business customer data; and
- 18 e. falsely holding itself out as transparent and deserving of its
19 customers' trust.

20 165. Based on the conduct alleged above, and other conduct that will be revealed
21 through discovery, Microsoft has engaged in unfair methods of competition and unfair or
22 deceptive acts or practices in the conduct of trade or commerce, in violation of RCW 19.86.020.

23 166. Microsoft's conduct affects the public interest because, *inter alia*:

- 24 a. Microsoft injured thousands of persons who paid for or paid more
25 for a service advertised as having certain qualities, when in fact the
26 product did not have those qualities, and whose data was used and
27 shared without consent; and
- 28 b. Microsoft's unfair or deceptive acts or practices were committed in
the course of its business;
- c. Microsoft aggressively advertises its cloud-based services to the
public in general;
- d. Microsoft actively solicits businesses to subscribe to its cloud-based
services;

- 1 e. Microsoft occupies an unequal bargaining position with respect to
- 2 the businesses to which it sells its cloud-based services;
- 3 f. Microsoft is the largest software company in the world, and has
- 4 enormous resources and extraordinary sophistication regarding use
- 5 and sharing of business customer data, yet has abused that position
- 6 in order to exploit its customers' data, and has done so through
- 7 deception, nondisclosure, and inadequate disclosure.

8 167. Plaintiffs and Class Members have been injured by Microsoft's conduct, in the
9 following, non-exhaustive ways:

- 10 a. they paid for a service or product advertised as having certain qualities as
- 11 alleged above, when in fact the product did not have those qualities;
- 12 b. they paid more for a service or product advertised as having certain
- 13 qualities as alleged above, when in fact the product did not have those
- 14 qualities; and
- 15 c. their data has been placed at risk through Microsoft's use and sharing of it,
- 16 and its noncompliance with SOC standards.

17 168. Under RCW 19.86.090, Plaintiffs and Class Members are entitled to:

- 18 a. a cease and desist order;
- 19 b. restitution;
- 20 c. actual damages;
- 21 d. treble damages;
- 22 e. costs; and
- 23 f. attorney fees.

24 **Count Four**
25 **Violations of Washington Privacy Act**
26 **RCW §§ 9.73.010, et seq.**
27 **On behalf of Plaintiffs and the Class**

28 169. Washington's Privacy Act, RCW. §§ 9.73.010, *et seq.*, prohibits the interception
of a private communication transmitted by device between two or more individuals without first
obtaining the consent of the participants in the communication. *Id.* § 9.73.030(1)(a).

170. Microsoft is not exempted from Privacy Act liability under RCW § 9.73.070.

1 171. Through its use and sharing of business customer data as alleged above, Microsoft
2 has intercepted private communications in violation of RCW § 9.73.030(1)(a), without first
3 obtaining the consent of the participants in the communications.

4 172. Microsoft obtained the content of Plaintiffs' and Class Members emails and other
5 private communications, without consent.

6 173. Microsoft shared that content with unauthorized third parties, including Facebook,
7 software application developers, and hundreds of subcontractors, who use the data for their own
8 purposes, or for purposes that benefit Microsoft, without consent.

9 174. Microsoft used that content to glean business intelligence and develop new
10 products – such as Microsoft Graph, Security Graph API, Audience Network, Windows
11 Defender Application Control, Azure Advanced Threat Protection, and Advanced Threat
12 Protection – to sell to others, and to improve products such as Cortana, regardless of whether the
13 business customer uses Cortana, without consent.

14 175. As alleged above, Plaintiffs and Class Members were injured in their business,
15 person or reputation. Plaintiffs and Class Members paid for Microsoft's services, without
16 knowledge or consent that Microsoft was using and sharing their private communications as
17 alleged above.

18 176. Under RCW § 9.73.060, Plaintiffs and Class Members are entitled to:

- 19
- 20
- 21 a. actual damages;
- 22 b. liquidated damages at the rate of \$100 per day for each violation, up to
23 \$1,000;
- 24 c. litigation costs; and
- 25 d. reasonable attorney fees.
- 26
- 27
- 28

Count Five
Violations of Washington Common Law
Intrusion Upon Seclusion
On behalf of Plaintiffs and the Class

1
2
3
4 177. By surreptitiously accessing, using, and/or sharing Plaintiffs' and Class Members'
5 data, including their contents, Microsoft intentionally intruded upon Plaintiffs' private affairs.

6 178. By repeatedly and purposefully accessing, using, and/or sharing Plaintiffs' and
7 Class Members' data for Microsoft's own commercial use, including developing new features,
8 new software, or reducing its costs, Microsoft's intrusion was intentional.

9
10 179. Plaintiffs and Class Members did not consent to, authorize, or know of
11 Microsoft's intrusions. Microsoft knew it lacked knowing consent to access, use, or share
12 Plaintiffs' and Class Members' data.

13 180. Plaintiffs and Class Members had a legitimate subjective expectation of privacy in
14 their data.

15 181. Plaintiffs and Class Members also had a reasonable objective expectation of
16 privacy in their data.

17
18 182. Microsoft's pervasive and recurring intrusions would be highly offensive to a
19 reasonable person.

20 183. Microsoft's conduct was highly offensive and outrageous to a reasonable person.

21 184. By simultaneously assuring Plaintiffs and Class Members that Microsoft would
22 use their data only to provide the agreed-upon services while in fact using the data for its own
23 purposes, Microsoft acted with deceit and disregard, reinforcing the offensive and outrageous
24 nature of its intrusions.

25
26 185. Microsoft's deception was deliberately orchestrated to conceal its intrusions from
27 Plaintiffs and Class Members.

1 186. Plaintiffs and Class Members have suffered extensive damages as a direct and
2 proximate cause of Microsoft's intrusions into its private affairs.

3 187. Plaintiffs and Class Members are entitled to:

- 4 a. restitution of the profits unjustly obtained;
- 5 b. recovery of payments for Microsoft's services;
- 6 c. punitive damages;
- 7 d. interest; and
- 8 e. other damages for Microsoft's invasion of privacy.

9
10 **PLAINTIFFS DEMAND A TRIAL BY JURY.**

11 DATED: July 17, 2020

12
13 **BAILEY & GLASSER, LLP**

14
15 */s/Todd A. Walburg* _____

16 Todd A. Walburg
17 *Attorneys for Plaintiff*

18 *Complete counsel listing on Page 1*
19
20
21
22
23
24
25
26
27
28