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

SUMMARY OF CLAIMS

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

INTRODUCTION

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

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

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

[2] On 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.

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

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

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

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

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

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

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

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

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

PARTIES AND PLAINTIFF-SPECIFIC ALLEGATIONS

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

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

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

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

29. Since 2016, Plaintiff Davenport has subscribed to Microsoft 365 Business Standard (formerly called "Office 365 Business Premium").

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

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

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

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

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

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

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

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

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

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

JURISDICTION AND VENUE

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

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

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

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

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

FACTS

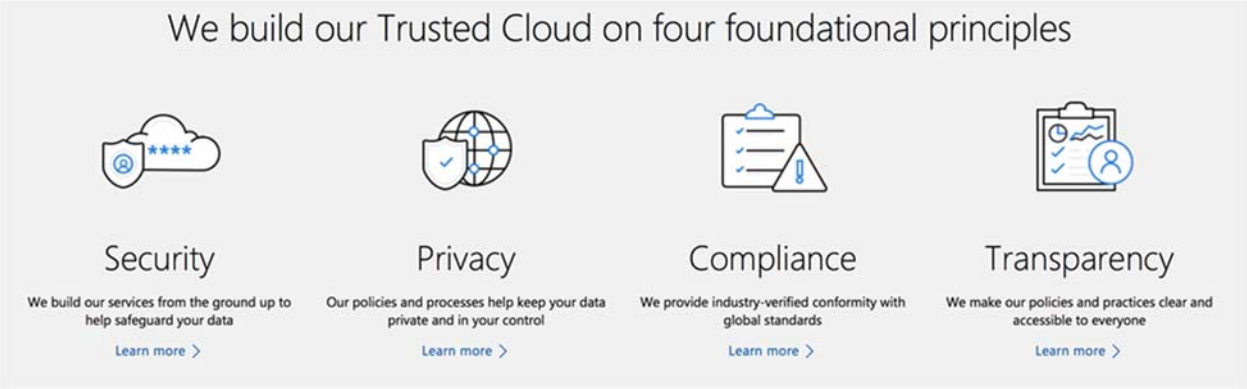
A. MICROSOFT TRANSITIONED BUSINESS CUSTOMERS TO ITS CLOUD-BASED SERVICES, ASSURING THEM THEIR DATA WOULD BE PRIVATE AND SECURE.

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

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

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

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



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

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

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

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

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

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

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

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

56. "Customer data" includes the customer's "content," *i.e.,* what Microsoft customers create, communicate, and store on or through Microsoft's services, such as the words in an email exchanged between friends or business colleagues, and the photographs and documents stored on Office 365 or Exchange Online.

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

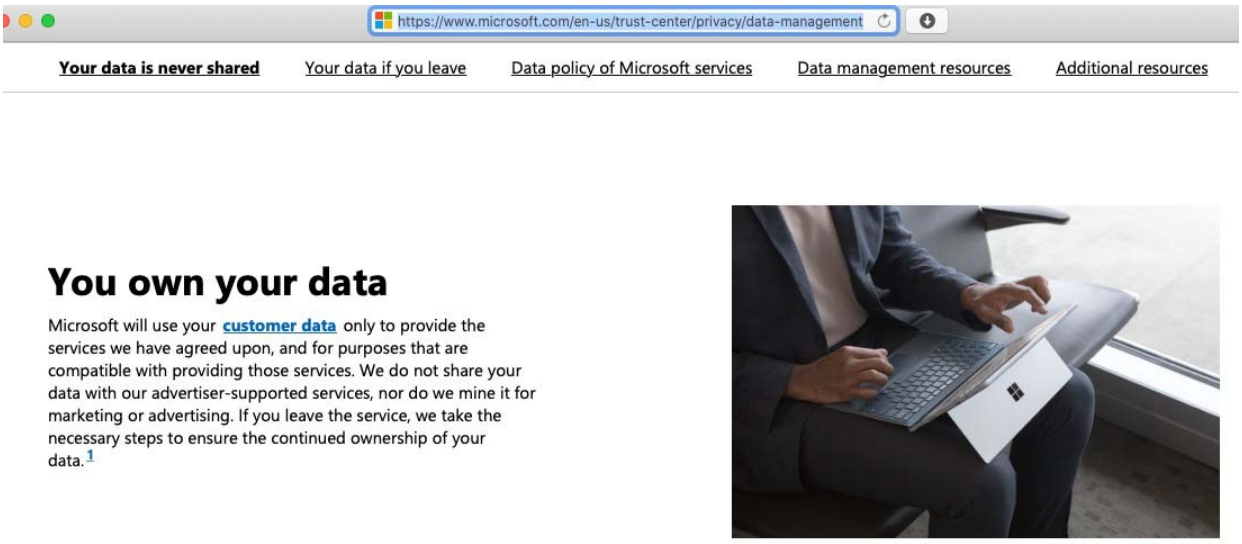
58. Throughout its Trust Center, and in its related marketing materials, whitepapers, technical instructions, and other representations and documents, Microsoft has consistently represented to its business customers that their data will not be used for any purpose other than providing the specific services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

a. On a marketing page of its website, Microsoft promises, "We use your data for just what you pay us for: to maintain and provide Office 365[.] We make it our policy to not use your data for other purposes."

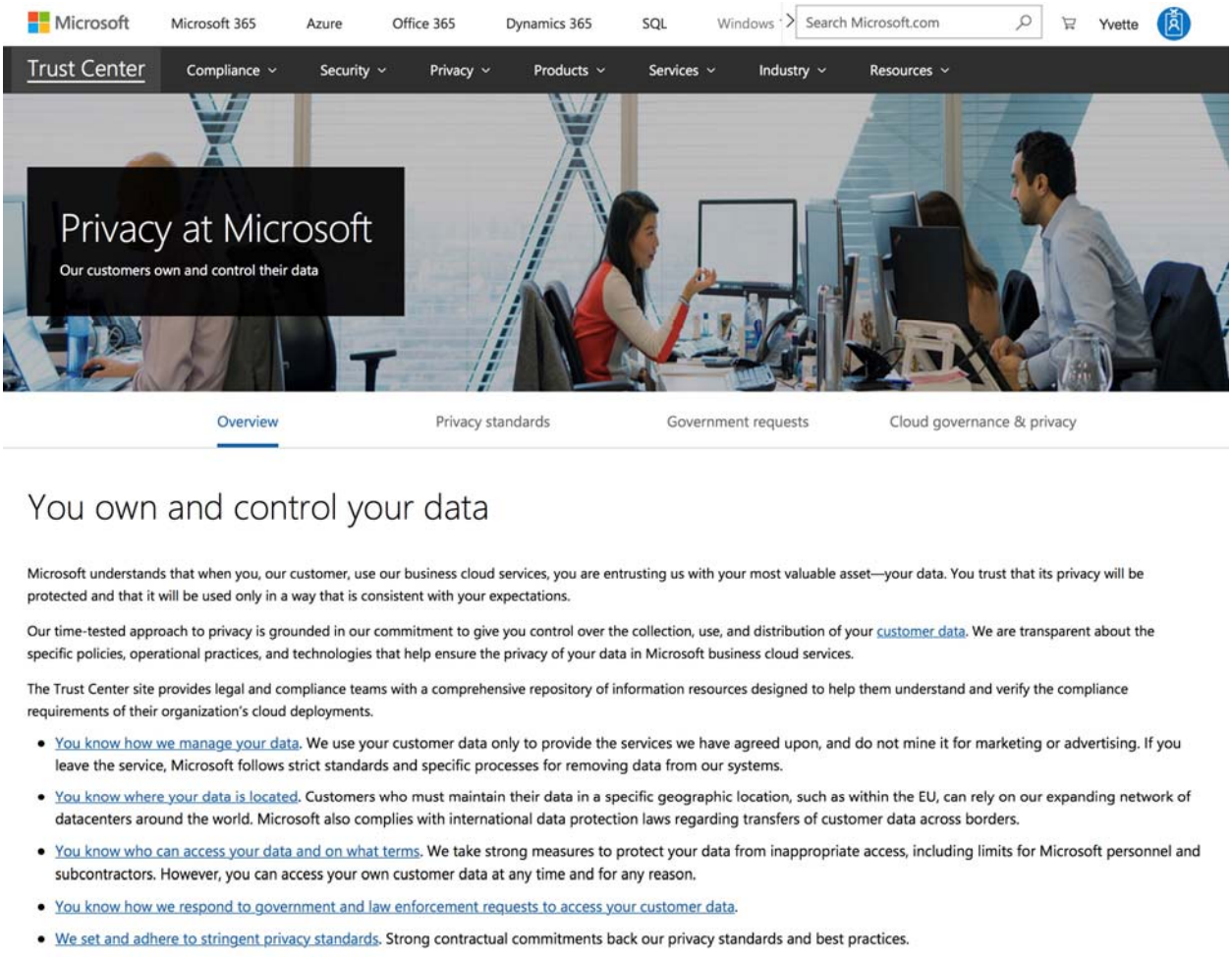
b. Similarly, in a whitepaper, Microsoft says that it "uses customer data only for providing cloud services… We also don't scan our customers' email or documents for building analytics, data mining, advertising, or improving services without our customers' permission."

c. And in webpages designed to provide more technical information, Microsoft promises: "We use customer data only to provide the services; therefore, Microsoft strictly prohibits access to customer data for any other purpose."

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



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



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

a. "As a customer of Office 365, you own and control your data. We do not use your data for anything other than providing you with the service that you have subscribed for…. You own your data and retain all rights, title, and interest in the data you store with Office 365."

b. "Our cloud services allow you to control who has access to your data, and how it's shared . . . . And you can take your data with you when you leave."

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

a. "We are transparent about our privacy practices and offer meaningful privacy choices."

b. "We will be transparent about data collection and use so you can make informed decisions. . . . Also, you can take your data with you if you end your subscription."

c. "With Office 365, it's your data. You own it. You control it And it is yours to take with you if you decide to leave the service . . . . You know where your data resides and who has access."

d. "We provide you with clear explanations about . . . who can access [your data] and under what circumstances."

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

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

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

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

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

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

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

> Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any 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.

69. Microsoft further "agrees and warrants . . . to process the personal data only on behalf of" the Microsoft business customer.

70. Microsoft commits, moreover, that it "shall not subcontract any of its processing operations performed on behalf of" the Microsoft business customer without the customer's prior written consent.

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

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

73. Reaffirming that message, Microsoft's Cloud Agreement and Open License Agreement say that the customer consents only "to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement."

C. MICROSOFT'S REPRESENTATIONS WERE FALSE.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

> What sets Microsoft Audience Ads apart is their rich user understanding that powers high performance. The Microsoft Graph consists of robust data sets, including search and web activity, LinkedIn professional profiles, demographics and more. The data is continually updated every second based 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.

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

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

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

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

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

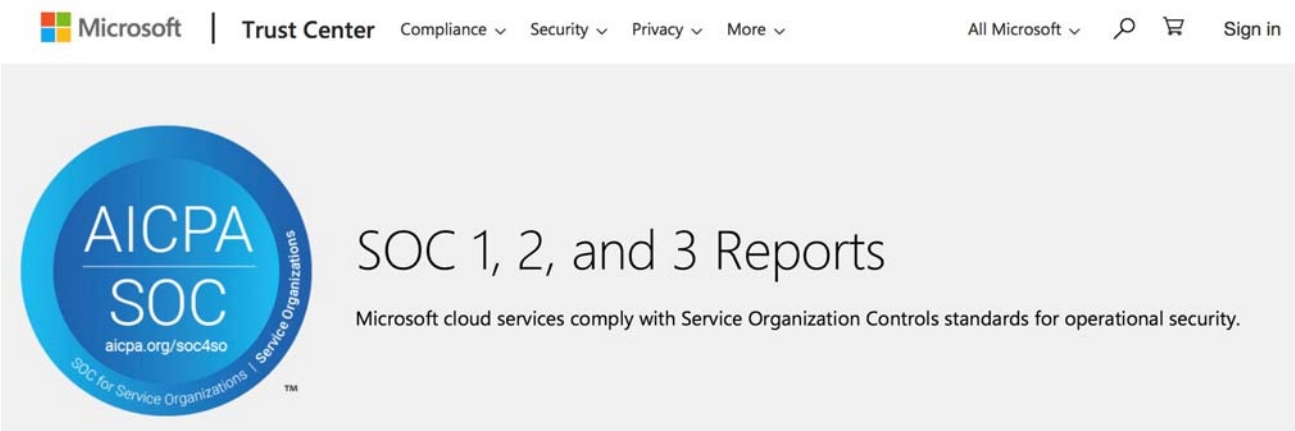
100. Microsoft not only misleads its business customers as to how it shares and uses their data, but also regarding how it protects and processes that data.

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

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

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

104. Microsoft promises business customers that it complies with SOC 1 and SOC 2 standards. For example, in Microsoft's "Trust Center," Microsoft states:



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.

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

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

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

112. As Microsoft admits in its own documentation, Graph complies with neither 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

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

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

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

115. Microsoft's use and sharing of Plaintiffs' and Microsoft's other business customers' data also reduced their data's privacy and security.

CLASS ACTION ALLEGATIONS

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

> All persons and non-governmental entities in the United States who subscribed to or purchased Microsoft Office 365 Business, Microsoft Office 365 Business Essentials, Microsoft Office 365 Business Premium, Exchange Online Plan 1, Exchange Online Plan 2, Microsoft Office 365 Enterprise, Office 365 Enterprise, Microsoft 365 Enterprise, Microsoft 365 Business, Office 365 Business, Office 365 Pro Plus, Office 365 Business Essentials, Office 365 Business Premium, Microsoft 365 Business Basic, Microsoft 365 Business Standard, or Microsoft 365 Business Premium, but did not subscribe to or purchase Microsoft Cognitive Services, from July 17, 2016 through the present (the "Class Period").

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

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

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

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

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

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

a. Whether Microsoft engaged in false, deceptive, or misleading business practices;

b. Whether Microsoft used the Class Members' data for its own unauthorized, commercial purposes;

c. Whether Microsoft shared the Class Members' data with unauthorized third parties;

d. Whether the Class Members consented to Microsoft's sharing and use of their data;

e. Whether the Class Members are entitled to statutory damages for Microsoft's actions;

f. Whether Microsoft's conduct violated the statutes as alleged below;

g. Whether the Class Members are entitled to compensatory damages for Microsoft's actions;

h. Whether the Class Members are entitled to punitive damages for Microsoft's actions; and

i. Whether the Class Members are entitled to declaratory and injunctive relief for Microsoft's actions.

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

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

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

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

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

APPLICABLE LAW

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

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

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

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

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

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

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

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

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

b. intentionally discloses or endeavors to disclose to any other person the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication, *id*. § 2511(1)(c); or

c. intentionally uses or endeavors to use the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication, *id*. § 2511(1)(d).

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

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

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

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

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

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

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

a. Microsoft obtained the content of their emails, documents, contacts, calendars, location data, audio files, photographs, and video files;

b. Microsoft shared that data with unauthorized third parties, including Facebook, software application developers, and hundreds of subcontractors, who use the data for their own purposes, or for purposes that benefit Microsoft; and

c. Microsoft used the data to glean business intelligence and develop new products – such as Microsoft Graph, Security Graph API, 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.

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

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

144. Microsoft's intentional interception of Plaintiffs' and Class Members' data is not necessary or incidental to and does not facilitate the transmission of Plaintiffs' and Class Members' data. It is not needed to provide Plaintiffs and Class Members the Microsoft services for which they subscribed.

145. Through its use and sharing of business customer data as alleged above, Microsoft has intentionally **disclosed** or endeavored to disclose to other persons the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of an electronic communication, without consent, in violation of 18 U.S.C. § 2511(1)(c).

146. Through its use and sharing of business customer data as alleged above, Microsoft has intentionally **used** or endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of an electronic communication, without consent, in violation of 18 U.S.C. § 2511(1)(d).

147. Under 18 U.S.C. § 2520(a), Plaintiffs and Class Members are entitled to:

a. injunctive and declaratory relief;

b. for each Plaintiff and Class Member, damages equal to the greater of $1,000 or the sum of the actual damages suffered by that plaintiff and any profits made by Microsoft as a result of the violation;

c. punitive damages;

d. litigation costs; and

e. reasonable attorney's fees.

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

148. The Stored Communications Act, 18 U.S.C. § 2707, provides for damages and other relief against any person who:

a. knowingly divulges to others the contents of electronic communications while in Microsoft's electronic storage, *id.* § 2702(a)(1);

b. knowingly divulges to others the contents of electronic communications maintained on Microsoft's service on behalf of, and received by means of electronic transmission from, Plaintiffs and Class Members, *id.* § 2702(a)(2)(A); or

c. knowingly divulges to others the contents of electronic communications carried or maintained on Microsoft's service solely for the purpose of providing storage or computer processing services to Plaintiffs and Class Members, *id.* § 2702(a)(2)(B).

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

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

151. Plaintiffs' and Class Members' electronic communications are in "electronic storage" because, incidental to their electronic transmission, they are kept in temporary, intermediate storage. *Id.* § 2510(17).

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

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

a. Microsoft obtained the content of their emails, documents, contacts, calendars, location data, audio files, photographs, and video files, without consent;

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

c. Microsoft used the data to glean business intelligence and develop new products – such as Microsoft Graph, Security Graph API, 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, without consent.

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

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

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

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

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

159. Under 18 U.S.C. § 2707(b) and § 2707(c), Plaintiffs and Class Members are entitled to:

a. injunctive and declaratory relief;

b. for each Plaintiff and Class Member, damages equal to the greater of $1,000 or the sum of the actual damages suffered by that plaintiff and any profits made by Microsoft as a result of the violation;

c. punitive damages;

d. litigation costs; and

e. reasonable attorney's fees.

Count Three
Violations of the Washington Consumer Protection Act
RCW 19.86, et seq.
On behalf of Plaintiffs and the Class

160. Washington's Consumer Protection Act ("CPA"), RCW 19.86, *et seq*., prohibits unfair competition and unfair and deceptive acts or practices in trade or commerce in order to protect both consumers and businesses, and to foster fair and honest competition.

161. Microsoft is a "person" within the meaning of the CPA, particularly RCW 19.86.010(1), and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

162. Each Plaintiff is a "person" within the meaning of the CPA, particularly RCW 19.86.010(1).

163. As set forth above, Microsoft represented to business customers that it would use business customers' data only to provide the services they purchased; that it would share their data with certain representatives only on a need-to-know basis; that it will never share the customers' data with third parties at all; and that security used for business customers' data complied with SOC standards. Those representations were false.

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

a. making representations, omissions, and solicitations that, considering their net impression and viewed as a whole, have the capacity to deceive the purchasing public regarding Microsoft's use and sharing of business customer data, and its compliance with SOC standards;

b. failing to disclose material facts regarding its use and sharing of business customer data and compliance with SOC standards;

c. diminishing the security and privacy of its customers' data through its use and sharing of that data and noncompliance with SOC standards;

d. diminishing the security and privacy of its customers' data through its failure to adopt and enforce adequate data security protections, including SOC standards, both on its own systems and in the systems of third parties and representatives with which Microsoft has shared or transferred business customer data; and

e. falsely holding itself out as transparent and deserving of its customers' trust.

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

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

a. Microsoft injured thousands of persons who paid for or paid more for a service advertised as having certain qualities, when in fact the product did not have those qualities, and whose data was used and shared without consent; and

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;

e. Microsoft occupies an unequal bargaining position with respect to the businesses to which it sells its cloud-based services;

f. Microsoft is the largest software company in the world, and has enormous resources and extraordinary sophistication regarding use and sharing of business customer data, yet has abused that position in order to exploit its customers' data, and has done so through deception, nondisclosure, and inadequate disclosure.

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

a. they paid for a service or product advertised as having certain qualities as alleged above, when in fact the product did not have those qualities;

b. they paid more for a service or product advertised as having certain qualities as alleged above, when in fact the product did not have those qualities; and

c. their data has been placed at risk through Microsoft's use and sharing of it, and its noncompliance with SOC standards.

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

a. a cease and desist order;

b. restitution;

c. actual damages;

d. treble damages;

e. costs; and

f. attorney fees.

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

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.

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

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

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

174. Microsoft used that content to glean business intelligence and develop new products – such as Microsoft Graph, Security Graph API, 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, without consent.

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

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

a. actual damages;

b. liquidated damages at the rate of $100 per day for each violation, up to $1,000;

c. litigation costs; and

d. reasonable attorney fees.

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

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

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

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

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

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

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

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

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

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

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

187. Plaintiffs and Class Members are entitled to:

a. restitution of the profits unjustly obtained;

b. recovery of payments for Microsoft's services;

c. punitive damages;

d. interest; and

e. other damages for Microsoft's invasion of privacy.

PLAINTIFFS DEMAND A TRIAL BY JURY.

DATED: July 17, 2020

BAILEY & GLASSER, LLP

/s/Todd A. Walburg
Todd A. Walburg
Attorneys for Plaintiff

Complete counsel listing on Page 1

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Frank D. Russo; Koonan Litigation Consulting, LLC; and, Sumner Davenport & Associates, LLC

(b) County of Residence of First Listed Plaintiff Napa County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
See attachment.

DEFENDANTS
Microsoft Croporation

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
18 U.S.C. § 2511; 18 U.S.C. § 2702
Brief description of cause:
Misrepresentation of its privacy and security practices

VII. REQUESTED IN COMPLAINT:
✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.
DEMAND $
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*
JUDGE DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)
(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 07/17/2020 **SIGNATURE OF ATTORNEY OF RECORD** /s/Arthur H. Bryant

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.

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)