COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG
LONDON LOS ANGELES NEW YORK PALO ALTO
SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Thomas O. Barnett

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5407
tbarnett@cov.com

CONFIDENTIAL TREATMENT REQUESTED UNDER 15 U.S.C. § 18A(H) AND ALL OTHER APPLICABLE STATUTES OR REGULATIONS

By Electronic Mail March 22, 2022

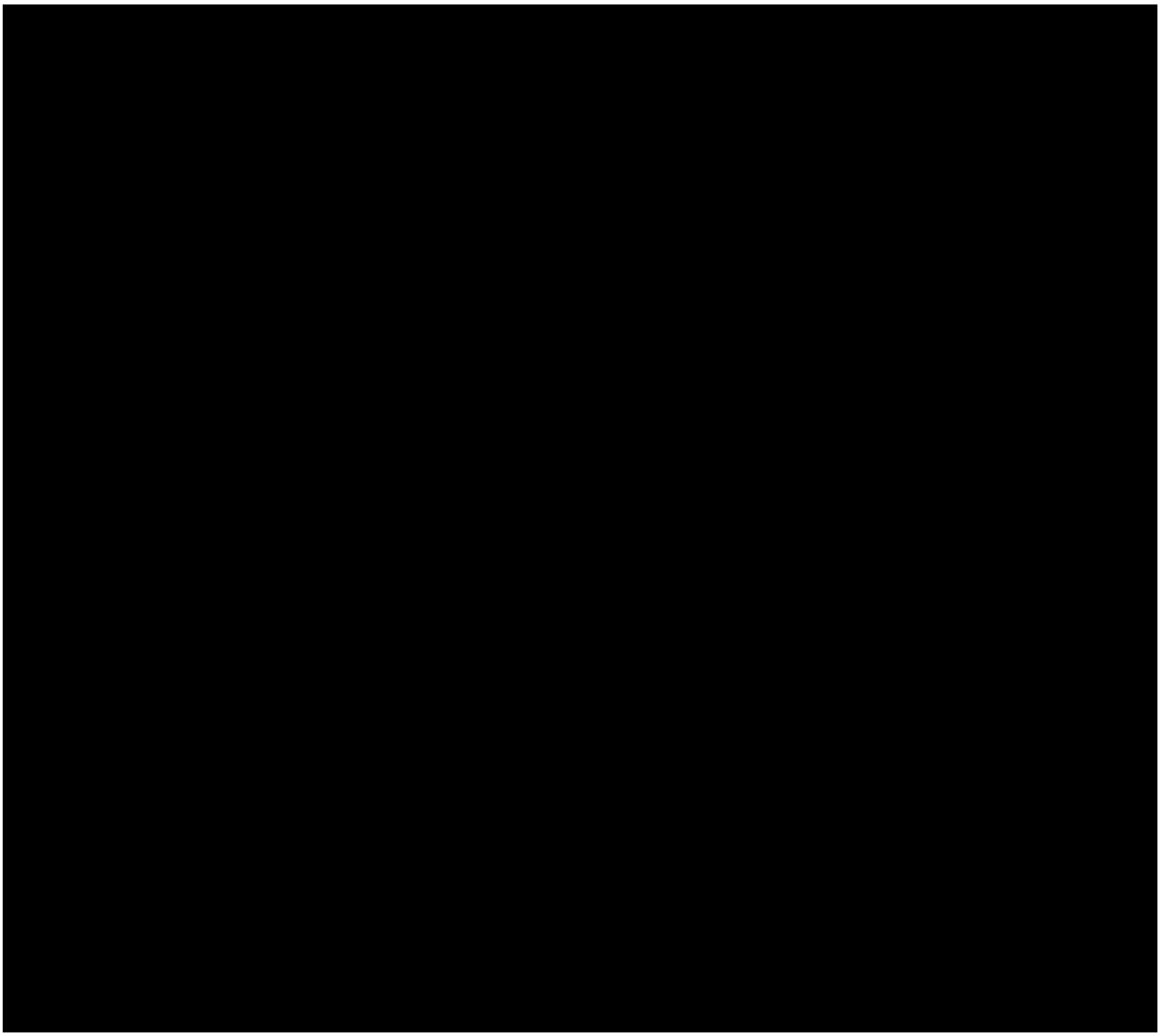
David Schwartz, Esq.
United States Federal Trade Commission
Bureau of Competition
Technology Enforcement Division
400 7th Street, SW
dschwartz1@ftc.gov

Re: Amazon.com, Inc., FTC File Nos. 191-0129 & 191-0130

Dear David:

I am writing on behalf of Amazon, in response to the above-referenced matter and in follow-up to the conversation on Friday, March 4, 2022. Amazon has worked diligently and in good faith for more than two years to respond to the CID and has produced nearly one and a half million documents, as well as approximately 100 terabytes of data. Amazon undertook this collection—which required a coordinated effort across 133 custodians and numerous sources, including email, Chime instant messages, WorkDocs, Quip, SharePoint, laptops, hard copy, and mobile devices—during the midst of a disruptive, global pandemic that presented unique challenges, including the fact that virtually all of the custodians were working remotely. The breadth of the collection and extenuating, pandemic-related circumstances also contributed to limitations in Amazon's collection process, which resulted in what we believe was a *de minimis* number of potentially responsive documents that were not available for production. We have been collecting information regarding these limitations so that we could explain them when we complete the production process. During the March 4 call, you asked for an interim report on such issues, so we describe below the particular limitations of which we are currently aware in the spirit of transparency and cooperation.

[redacted]



Third, while Amazon employees rely principally on email, Chime instant messaging, and other enterprise applications for their business-related communications, the company identified 22 custodians who at times used Signal for work. Amazon's investigation has determined that most of these custodians did so principally (or exclusively) for non-substantive purposes—such as scheduling, travel, or to get someone to return a call or check their email—or for issues unrelated to the CID, such as correspondence related solely to international issues or arranging

security protection.[1] We are aware of four relevant custodians[2] who used Signal for substantive work communications potentially responsive to the CID, but Amazon learned during its collection process that there were no potentially responsive substantive Signal messages available at that time to collect from those custodians' phones.

As you are likely aware, Signal uses "state-of-the-art end-to-end encryption" to ensure that conversations remain secure.[3] Signal is used by business leaders, government officials, and other high-profile individuals because its encrypted, secure platform provides privacy protections and protects against hacking.[4] Amazon's understanding is that, while not their primary tool for work communication, certain Amazon executives began using Signal for these privacy and security benefits for some communications. As illustrated by the hacking of an Amazon executive's personal phone that was widely reported in 2019, Amazon's executive leaders are targets for individual and nation-state actors who seek to intercept sensitive business communications. Apps like Signal offer protection against not only the interception of communications, but also against improper access to information if a mobile device is lost or stolen for several reasons: (i) the messages are encrypted end-to-end as well as when stored on devices, (ii) they typically require two-factor authentication; (iii) they reduce the amount of data stored on the device.

As part of its security protections, Signal has a "disappearing message" feature that auto-deletes messages on both the sender's and recipient's devices. This feature was at times used by certain custodians, so it is possible that some responsive communications have not been preserved. Amazon understands from investigating this issue with e-discovery professionals

---

[1] Sixteen custodians used Signal on this basis: Christine Beauchamp, Jeff Carter, Natasha Chand, Dave Clark, Janette Coleman, John Connors, John Felton, Paul Kotas, Stephenie Landry, Russ Grandinetti, David Henri, Doug Herrington, Neil Lindsay, Brian Olsavsky, Cem Sibay, and Tom Taylor.

[2] These four custodians are Jeff Blackburn, Dave Limp, Peter Krawiec, and Jeff Wilke. We also note that Jeff Bezos and Mike Hopkins used Signal for substantive work communications, but their phones were outside the scope of the collection process for Amazon's response to the CID.

[3] *See* Signal, https://signal.org/en/.

[4] See Letter from Senator Ron Wyden to The Honorable Frank Larkin, May 9 2017, https://www.documentcloud.org/documents/3723701-Ron-Wyden-letter-on-Signal-encrypted-messaging.html; Shawn Snow, Kyle Rempfer, and Meghann Myers, "Deployed 82nd Airborne unit told to use these encrypted messaging apps on government cell phones," Military Times, Jan. 23 2020, https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/; Jon Porter, "Signal becomes European Commission's messaging app of choice in security clampdown," The Verge, Feb. 24 2020, https://www.theverge.com/2020/2/24/21150918/european-commission-signal-encrypted-messaging.

that any messages that were not preserved cannot be recovered, due in part to Signal's end-to-end encryption.

[redacted]

Regards,

Thomas O. Barnett
Covington & Burling LLP

[redacted]