

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074
<http://oversight.house.gov>

February 19, 2020

Mr. Brian Huseman
Vice President, Public Policy
Amazon.com, Inc.
601 New Jersey Avenue, N.W.
Washington, D.C. 20001

Dear Mr. Huseman:

The Subcommittee on Economic and Consumer Policy is writing to request documents and information about Ring's partnerships with city governments and local police departments, along with the company's policies governing the data it collects. The Subcommittee is examining traditional constitutional protections against surveilling Americans and the balancing of civil liberties and security interests.

Ring's website promises consumers a "Ring of Security around your home."¹ Ring alludes to the public's concerns regarding their personal safety through its Neighbors app, which Ring describes as "The New Neighborhood Watch."² It combines user-shared videos with data that Ring employees compile from 911 dispatch centers—sometimes available only through agreement with local law enforcement—into a geotargeted livestream of real and possible crime.³

Ring reportedly works closely with local governments and police departments to promote its surveillance tools and has entered into agreements with cities to provide discounts on Ring products to their residents in exchange for city subsidies. Reports indicate that Ring also has entered into agreements with police departments to provide free Ring products for giveaways to the public.⁴

¹ Ring, *Video Doorbells* (online at <https://shop.ring.com/pages/doorbell-cameras>) (accessed Nov. 22, 2019).

² Ring, *Neighbors App* (online at <https://shop.ring.com/pages/neighbors>) (accessed Nov. 26, 2019).

³ *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, Washington Post (Aug. 28, 2019) (online at www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/); see also *Cops Are Giving Amazon's Ring Your Real-Time 911 Caller Data*, Gizmodo (Aug. 1, 2019) (online at <https://gizmodo.com/cops-are-giving-amazons-ring-your-real-time-911-data-1836883867>) (discussing Ring's use of computer-aided dispatch feeds).

⁴ *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*, Vice (Aug. 2, 2019) (online at www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money); *Amazon's Helping Police Build a Surveillance Network with Ring Doorbells*,

Ring reportedly tightly controls what cities and law enforcement agencies can say about Ring, requiring any public statement to be approved in advance.⁵ In one instance, Ring is reported to have edited a police department's press release to remove the word "surveillance."⁶

The Subcommittee is seeking more information regarding why cities and law enforcement agencies enter into these agreements. The answer appears to be that Ring gives them access to a much wider system of surveillance than they could build themselves, and Ring allows law enforcement access to a network of surveillance cameras on private property without the expense to taxpayers of having to purchase, install, and monitor those cameras. Law enforcement agencies can view videos shared by users in the Neighbors app, request video from users through the Neighbors Portal, or request video directly from Ring.⁷ Once law enforcement agencies have access to consumers' data, Ring has made it clear that the agencies can use, store, and share that data however they want.⁸

Ring has asserted that it does not turn over "customer information in response to government demands unless required to do so to comply with a legally valid and binding order, such as a search warrant; or in an exigent or emergency circumstance."⁹ However, that assertion appears to contradict Ring's Terms of Service, which indicate that Ring can turn over information in response to a "reasonable governmental request." The Terms of Service state:

Ring may access, use, preserve and/or disclose your Content to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if we have a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with applicable law, regulation, legal process, or reasonable governmental request.¹⁰

CNET (June 5, 2019) (online at www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells).

⁵ *Amazon's Doorbell Camera Ring Is Working with Police—and Controlling What They Say*, The Guardian (Aug. 30, 2019) (online at www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor).

⁶ *Amazon's Ring Barred Cops from Using 'Surveillance' to Describe Its Products*, Gizmodo (Aug. 19, 2019) (online at <https://gizmodo.com/ring-barred-cops-from-using-surveillance-to-describe-it-1837380102>).

⁷ *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, Washington Post (Aug. 28, 2019) (online at www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach).

⁸ *Police Can Keep Ring Camera Video Forever and Share with Whomever They'd Like, Amazon Tells Senator*, Washington Post (Nov. 19, 2019) (online at www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator).

⁹ Letter from Brian Huseman, Vice President, Public Policy, Amazon, to Senator Edward Markey (Nov. 1, 2019) (online at www.markey.senate.gov/imo/media/doc/Response%20Letter_Ring_Senator%20Markey%2011.01.2019.pdf).

¹⁰ Ring, *Ring Terms of Service* (online at <https://shop.ring.com/pages/terms>) (accessed Feb. 11, 2020) emphasis added

For these reasons, the Subcommittee requests that you produce by March 4, 2020, the following documents and information for the period of January 1, 2013, to the present:

1. All agreements with:
 - a. cities and law enforcement agencies, including those to provide free Ring products, discounted Ring products, and access to the Neighbors Portal; and
 - b. neighborhood watch groups, including those to provide free Ring products, discounted Ring products, and testimony in legal proceedings; and
2. A list of:
 - a. all law enforcement agencies that have access to the Neighbors Portal, including the name and location of the agency, the date on which the agency gained access to the Neighbors Portal, and whether the agency has a contract for Rekognition;
 - b. all instances in which a law enforcement agency has requested video footage from Ring, including the requesting agency, a description of the nature of the request (e.g., search warrant, subpoena, writ of assistance, informal request), whether Ring complied with the request, and whether the user consented or had knowledge of the footage request;
 - c. all service providers, business partners, and third-party analytics services with which Ring has shared consumers' personal information and video footage; and
 - d. all of Ring's sources of computer-aided dispatch (CAD) data, specifying whether the source is publicly available and including the specific elements of data collected from that source; and
3. All current and past versions of Ring's:
 - a. Privacy Notice, Terms of Service, and Law Enforcement Legal Process Guidelines, indicating their effective dates;
 - b. policies and procedures regarding using footage shared in the Neighbors app in marketing materials, including policies for obtaining consent from individuals in the footage and any special policies for footage featuring children; and
 - c. policies and procedures regarding employee access to stored and live video; and
4. All documents referring or relating to:
 - a. the integration, or potential integration, of facial recognition tools, including Rekognition, in Ring products;

- b. the use of live or stored video footage from Ring products or shared in the Neighbors app to train facial recognition tools, including Rekognition;
 - c. the integration, or potential integration, of automated license plate reader technology in Ring products;
 - d. Ring's potential partnership with Axon;
 - e. Ring's "Community Alerts" Facebook campaign;
 - f. unauthorized access by Ring employees to stored and live video footage, including any disciplinary actions taken in response;
 - g. activation, except in response to consumer requests for technical support, of video or audio recording by Ring;
 - h. research, studies, consultation, or advice Ring undertook or received about how to design the Neighbors app to encourage consumers to share footage with law enforcement;
 - i. research and studies of Ring products' effect on crime;
 - j. research, studies, consultation, or advice Ring undertook or received about Ring products' and the Neighbors apps' implications for civil liberties, including but not limited to issues of privacy and racial profiling;
 - k. customer complaints regarding security vulnerabilities or breaches, privacy concerns, law enforcement requests for footage via the Neighbors app, and racial profiling related to the Neighbors app;
 - l. the heat map feature in the Neighbors Portal; and
 - m. the number of ring user accounts with and without two-factor authentication engaged; and
5. All documents that Ring or Amazon has produced to state attorneys general, the Federal Trade Commission, the Department of Justice, or Congress in response to investigations into Ring.

We also request a briefing, to be completed by February 27, 2020, covering topics including, but not limited to:

1. The circumstances in which Ring will disclose information and content to law enforcement, including in response to a "reasonable governmental request";
2. Whether Ring allows consumers to permanently delete all stored video footage or whether Ring retains copies of footage even after a consumer deletes it;
3. The status of Ring's development of a facial recognition feature and the timeline for the release of any such feature;
4. Which Ring products have audio recording enabled by default;
5. The number and percentage of Ring customers that have used the privacy zones feature; and

6. Whether Ring will commit to requiring two-factor authentication, by default, for all users including users with existing accounts.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. An attachment to this letter provides additional instructions for responding to the Committee's request. If you have any questions regarding this request, please contact Subcommittee staff at (202) 225-5051.

Sincerely,



Raja Krishnamoorthi
Chairman
Subcommittee on Economic and Consumer Policy

Enclosure

cc: The Honorable Michael Cloud, Ranking Member

Responding to Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committees.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committees' preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
 - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - b. Document numbers in the load file should match document Bates numbers and TIF file names.
 - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - d. All electronic documents produced to the Committees should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.

7. Documents produced to the Committees should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committees' letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee on Oversight and Reform, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building. When documents are produced to the Committee on Financial Services, production sets shall be delivered to the Majority Staff in Room 2129 of the Rayburn House Office Building and the Minority Staff in Room 4340 of the O'Neill House Office Building. When documents are produced to the Permanent Select Committee on Intelligence, production sets shall be delivered to Majority and Minority Staff in Room HVC-304 of the Capital Visitor Center.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a

part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.