

United States Senate

WASHINGTON, DC 20510

November 20, 2019

Mr. Jeffrey Bezos
Chief Executive Officer
Amazon.com, Inc.
410 Terry Avenue N.
Seattle, WA 98109

Dear Mr. Bezos:

We write to request information about the data security practices of Ring, the home security company Amazon purchased last year.

Millions of consumers use Ring's products and services, which include internet-connected video doorbells, spotlight cameras and alarm systems. Ring devices routinely upload data, including video recordings, to Amazon's servers. Amazon therefore holds a vast amount of deeply sensitive data and video footage detailing the lives of millions of Americans in and near their homes. If hackers or foreign actors were to gain access to this data, it would not only threaten the privacy and safety of the impacted Americans; it could also threaten U.S. national security. Personal data can be exploited by foreign intelligence services to amplify the impact of espionage and influence operations.

Ring's emphasis on safety and security has not always extended to the massive amount of data it amasses, retains and shares, according to public reports. Last week, researchers discovered a now-patched vulnerability in Ring doorbells that left Wi-Fi network passwords exposed to hackers. Security experts have similarly discovered a number of vulnerabilities in Ring products that, though since patched, left customer video feeds vulnerable to eavesdropping and manipulation by malicious actors.

In addition to these security incidents, we are concerned about media reports suggesting a lack of respect for the privacy of Ring customers. Earlier this year, *The Intercept* and other outlets indicated that Ring employees in Ukraine were provided with "virtually unfettered access" to a folder containing every video created by every Ring camera around the world. That same report also detailed how Ring executives and engineers in the U.S. were given "highly privileged access to the company's technical support video portal, allowing unfiltered, round-the-clock live feeds from some customer cameras." These reports raise serious questions about Ring's internal cybersecurity and privacy safeguards, particularly if employees and contractors in foreign countries have access to American consumers' data.

Americans who make the choice to install Ring products in and outside their homes do so under the assumption that they are — as your website proclaims — "making the neighborhood safer." As such, the American people have a right to know who else is looking at the data they provide to Ring, and if that data is secure from hackers. To that end, please provide us with responses to the following questions by January 6, 2020:

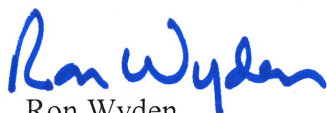
1. How many units has Ring sold to Americans?
2. Does Ring delete users' video footage generated by Ring devices?
 - a. Does Ring ever delete a user's video footage it has retained?
 - b. Please detail Ring's default data retention policy.
3. Please detail the security measures Ring has employed in order to protect data generated by or stored on Ring devices.
 - a. Does Ring encrypt video footage, both in storage and transmission? If not, please explain why this is not a current practice.
 - b. Please detail Ring's policies and practices regarding third-party disclosed security vulnerabilities, including whether or not Ring has implemented the International Organization for Standardization's ISO/IEC 29147:2014 guidelines for vulnerability disclosure.
 - c. How regularly does Ring perform in-depth security tests, audits, vulnerability scans, source code reviews and penetration testing?
 - d. Are independent security audits performed? If so, how often are these audits performed on a routine basis?
 - e. How many security incidents have you detected over the past two years? Please describe the severity of each incident, how each incident was remedied, and which federal, state, or local government agencies were notified about the incidents.
4. According to media reports, Ring has provided its Ukraine-based research and development team with unrestricted access to Ring's entire camera database in unencrypted form, with each video file reportedly linked to a specific Ring user.
 - a. How many employees of Amazon and Ring have access to American users' camera data?
 - b. How is employee access to customer video data controlled, logged, and audited?
 - c. Do employees have access to live feeds?
 - d. Do employees have access to any other information regarding the customer's account other than camera data (e.g. user name(s), email address(es), physical address, geolocation)?
 - e. Do employees have access to any previously tagged information in video feeds that specifically identify a person or vehicle (e.g. are employees able to determine the homeowner or specific license plates from the data which they have access to)?
 - f. To your knowledge, have there been any documented instances of this access being abused?
5. Ring's online career postings suggest that the company is still hiring Ukrainians to view and tag videos of Americans. Please confirm this practice and explain its purpose.
 - a. Please describe the process by which Americans' data is accessed by employees or contractors in Ukraine or any other country outside the United States and the standards by which they are held.
 - b. Please detail in how many other countries employees have access to Americans' Ring data.
 - c. Please detail, for each country where employees have access to Americans' Ring data, what data privacy and retention policies are in place and any ability for a

foreign government to access (through a legal process within that country or otherwise) any Americans' Ring data stored within that country.

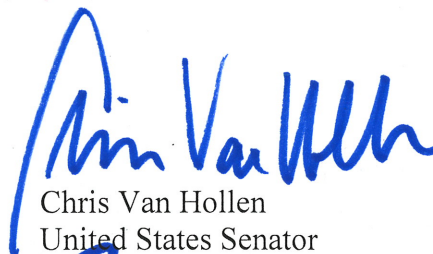
6. According to media reports, Ring employs a "head of facial recognition research" and has applied for a "facial recognition patent." Please describe Ring's plans regarding the addition of facial recognition capabilities to its products.
 - a. Does Ring intend to use, currently use, or has it used, any type of image matching software capable of facial recognition, including Amazon's Rekognition?
 - i. Has Amazon submitted the Rekognition tool to the NIST face recognition vendor test?
 - ii. Please provide as an addendum any relevant guidance Amazon may have on the development and intended use of facial recognition technology.
 - b. Does Ring contract out to, or request assistance from, any entity regarding facial recognition? Which entities or agencies? Please provide any relevant guidelines or memoranda outlining this relationship, including any audits or analysis you have undertaken to evaluate the use of facial recognition.

Thank you for your prompt attention to this important matter.

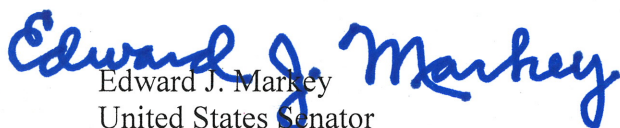
Sincerely,



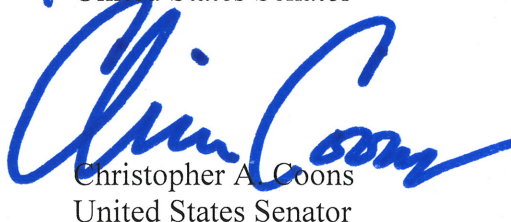
Ron Wyden
United States Senator



Chris Van Hollen
United States Senator



Edward J. Markey
United States Senator



Christopher A. Coons
United States Senator



Gary C. Peters
United States Senator