amazon

January 6, 2020

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Chris Van Hollen
United States Senate
110 Hart Senate Office Building
Washington, DC 20510

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Christopher A. Coons
United States Senate
218 Russell Senate Office Building
Washington, DC 20510

The Honorable Gary C. Peters
United States Senate
724 Hart Senate Office Building
Washington, DC 20510

Dear Senators Wyden, Van Hollen, Markey, Coons, and Peters:

Thank you for your letter dated November 20, 2019, regarding Ring's products and services.

Ring's mission is to make neighborhoods safer, and our vision is to provide affordable, accessible, and convenient security solutions for people's home and neighborhoods. With Ring's security cameras, customers can see, hear, and speak to visitors from anywhere through their smartphones, tablets, and PCs.

We feel strongly that when communities work together, safer homes and safer neighborhoods become a reality, which is why we created the Neighbors app. We continue to see examples of Ring devices and the Neighbors app making neighborhoods safer, including by getting stolen guns off the street, helping locate missing senior citizens, and recovering stolen medical supplies. Additionally, in late December, we were proud to announce a partnership with the National Center for Missing and Exploited Children to increase awareness of missing children and leverage the power of neighborhood communities in the Neighbors app to help reunite missing children with their families.

At Ring, customer trust is at the center of everything we do and we take customer privacy and protection of customer data very seriously. As part of this commitment, we are always iterating on ways to provide more transparency and control to our customers. As expected for any rapidly growing company, Ring's data security and privacy practices have evolved over time. Unfortunately, recent media reports have inaccurately portrayed Ring's security practices, and we hope our letter today will correct some of those inaccuracies. Ring will continue to prioritize privacy, security, and user control as we pursue and improve technologies to help achieve our mission of making neighborhoods safer.

The answers to your questions are as follows:

1. **How many units has Ring sold to Americans?**

   We do not disclose the specific numbers of devices sold, but there are millions of customers who have purchased a Ring device. Ring customers place their trust in us to help protect their homes and communities and we take that responsibility very seriously.

2. **Does Ring delete users' video footage generated by Ring devices?**

   a. **Does Ring ever delete a user's video footage it has retained?**

      Yes. Ring automatically deletes user video in accordance with our subscription plans. See the response below for details on subscription plans. Customers can always delete their videos (individual videos or their entire footage history) at any time by logging into their account on the Ring app or at Ring.com.

   b. **Please detail Ring's default data retention policy.**

      Ring has instituted routine deletion schedules to align the retention of Ring video data with the storage period under Ring's customer subscription plans. If a customer subscribes to a Ring Protect plan, recordings are stored securely in the customer's Ring account for up to 60 days, unless deleted earlier by the customer. For customers who signed up for a Ring Protect plan prior to June 2017 (after which, we changed new customer subscription policies), videos are stored for up to 180 days, unless deleted earlier by the customer. As noted above, customers can always delete their videos (individual videos or their entire footage history) at any time by logging into their account on the Ring app or at Ring.com. For customers who do not have a subscription plan no video is recorded or stored by Ring.

3. **Please detail the security measures Ring has employed in order to protect data generated by or stored on Ring devices.**

   Ring has developed and implemented a robust information security program that protects its customers' data. Ring modeled its information security program on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, a widely-accepted comprehensive approach to cybersecurity that was designed with a specific focus on protecting sensitive information. As expected for any rapidly growing company, Ring's data security and privacy practices have continued to evolve and mature over time. Ring regularly assesses risks and makes adjustments based on those risks to enhance the safety and security of its customers' information.

   a. **Does Ring encrypt video footage, both in storage and transmission? If not, please explain why this is not a current practice.**

      Yes. Ring encrypts video footage both in storage and transmission, and Ring stores video on encrypted Amazon Web Services servers.

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.**

Ring has implemented a wide range of robust Amazon and Ring-specific information security policies and procedures, including Amazon's vulnerability standards and Ring's own vulnerability management standard for reporting and remediating security vulnerabilities. Ring also implements industry standard measures to safeguard and mitigate information security risks.

c. **How regularly does Ring perform in-depth security tests, audits, vulnerability scans, source code reviews and penetration testing?**

Ring routinely conducts assessments, penetration testing, and source code reviews addressing the security and privacy of Ring video data and Ring's security practices, including two audits conducted by Amazon's internal audit team in 2019. Information concerning our audits is confidential because information obtained from these audits is used to protect against future attempts by bad actors.

d. **Are independent security audits performed? If so, how often are these audits performed on a routine basis?**

Ring routinely conducts assessments by internal and external parties to test our systems for vulnerabilities. Some of our audits are conducted by independent security teams within Amazon that include security experts with a depth of knowledge in closing device vulnerabilities. Our security assessments are driven by identified risks and risks modeling. Additionally, Ring routinely conducts penetration testing, source code reviews, and other assessments to identify and close vulnerabilities.

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.**

Ring has always taken customer privacy and the protection of customer data seriously, and we are always iterating on ways to improve our security mechanisms.

Ring is not aware of any breach of a customer's personally identifiable information that would require reporting to government agencies. We are aware of incidents discussed below where employees violated our policies. Unfortunately, we also continue to see stolen credentials and passwords (from other applications and sites) that have led to some bad actors gaining access to Ring devices. Our security team investigated these incidents and found no evidence of an unauthorized intrusion or compromise of Ring's systems or network.

Like any rapidly growing company, we recognize that we must continually evolve and enhance our data and security practices to block efforts by bad actors. We recently launched an ongoing campaign to educate our customers on how to better protect their online accounts – a campaign that includes prompts both in-app and via email to encourage usage of two-factor authentication. Ring now also proactively monitors whether any of our customers' credentials might have been compromised in third-party data breaches and takes proactive steps to notify customers and protect any potentially impacted Ring accounts from unauthorized access resulting from such third-party breaches. In addition, Ring notifies account owners when any new device accesses their account. We will continue investing in and rolling out enhanced security features to ensure that our customers are protected.

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.**

No employees or contractors have unrestricted access to customer's camera data, regardless of where they are based. Ring has always sought to provision access to Ring video data in a manner that best serves its customers, including ensuring quality performance of Ring's services and protection of customers' personal data. The R&D team in Ukraine do not have unrestricted access to Ring's video database. The R&D team in Ukraine can only access publicly available videos and videos available from Ring employees, contractors, and friends and family of employees or contractors with their express consent. We use these videos to deliver high-quality services and to maintain and improve the customer experience.

a. **How many employees of Amazon and Ring have access to American users' camera data?**

As noted, our R&D teams can only access publicly available videos and videos available from Ring employees, contractors, and friends and family of employees or contractors with their express consent. Additionally, customers may give their express consent to our customer service department to provide temporary access to their live camera feed when troubleshooting a specific customer issue. Aside from this, a very limited number of employees (currently three) have the ability to access stored customer videos for the purpose of maintaining Ring's AWS infrastructure.

Ring logs and monitors all access, and employees and contractors are informed that improper access to, or use of, confidential information or technology could result in termination.

b. **How is employee access to customer video data controlled, logged, and audited?**

All employees and the service providers with which Ring engages are at all times required to protect Ring’s proprietary and confidential information, including Ring video data. All Ring employees, including those with access to Ring video data, are subject to Amazon’s Confidential Information and NDA Guidelines Policy, Amazon’s Code of Conduct, and Amazon’s Zero Tolerance Policy. The Confidential Information and NDA Guidelines Policy prohibits employees from accessing or using confidential data, unless that access or use is necessary to perform a job function. That policy also prohibits disclosing confidential information except in narrow circumstances. Under Amazon’s Code of Conduct, Ring requires its employees to process Ring video data lawfully, ethically, and in the best interests of the company. Ring disciplines employees for violating that requirement and does not tolerate behavior that jeopardizes the security of Ring video data. Finally, Amazon’s Guide to Employment informs Ring employees of its high expectations with respect to the security of all company information including Ring video data.

Ring logs access to the customer service interface used for customer account information, device configuration, and device settings. Employees and contractors are informed that improper access to, or use of, confidential information or technology could result in discipline, including termination. Ring periodically reviews the access privileges it grants to its team members to verify that access to customer information is for the sole purpose of maintaining and improving the customer experience.

c. **Do employees have access to live feeds?**

Employees have access to live feeds only when the customer has granted access to a specific team member for the express, limited purpose of troubleshooting a device issue where such access is required.

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)?**

Employees have access to the primary customer service interface used for customer account information, device configuration, and device settings. There are multiple security control layers to access information, which includes customer information necessary to conduct standard customer service operations. Employees have access to this information only for the sole purpose of maintaining and improving the customer experience.

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)?**

No.

f. **To your knowledge, have there been any documented instances of this access being abused?**

Over the last four years, Ring has received four complaints or inquiries regarding a team member's access to Ring video data. Although each of the individuals involved in these incidents was authorized to view video data, the attempted access to that data exceeded what was necessary for their job functions. In each instance, once Ring was made aware of the alleged conduct, Ring promptly investigated the incident, and after determining that the individual violated company policy, terminated the individual. In addition to taking swift action to investigate and take appropriate disciplinary action in each of these cases, Ring has taken multiple actions to limit such data access to a smaller number of team members. Ring periodically reviews the access privileges it grants to its team members to verify that they have a continuing need for access to customer information for the purpose of maintaining and improving the customer experience.

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.**

Ring's research and development team in Ukraine access Ring video data for the purpose of making improvements to Ring's devices and services to maintain the customer experience. Our R&D teams in Ukraine and elsewhere can only access publicly available videos and videos available from employees, contractors, and friends and family of employees or contractors with their express consent. We take customer data seriously and Ring logs and monitors all access, and employees and contractors are informed that improper access to, or use of, confidential information or technology could result in termination. Ring periodically reviews the access privileges it grants to its team members to verify that their access to customer information is for the purpose of maintaining and improving the customer experience.

b. **Please detail in how many other countries employees have access to Americans' Ring data.**

Team member access to data is always for the purpose of maintaining and improving the customer experience. Ring is a global company with staff in countries around the world. Ring provisions team member access to customer data with the same policies and restrictions globally.

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.**

The same Ring privacy and retention policies (outlined above) apply globally. Ring complies with the legal requirements in each jurisdiction where we operate, including Ukraine and the United States. Ring objects to over broad or otherwise inappropriate government requests for customer data.

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?**

Ring does not currently offer facial recognition technology, including Amazon Rekognition, in any Ring products. We do frequently innovate based on customer demand, and facial recognition features are increasingly common in consumer security cameras today, such as: Google Nest Hello, Tend Secure Lynx, Netamo Welcome, Wisenet Smartcam, and Honeywell Smart Home Security. If our customers want these features in Ring security cameras, we will release these features only with thoughtful design including privacy, security, and user control, and we will clearly communicate with our customers as we offer new features.

i. **Has Amazon submitted the Rekognition tool to the NIST face recognition vendor test?**

Amazon has not yet submitted Rekognition to NIST's facial recognition vendor test. However, we are committed to quickly submitting our algorithms to NIST and working very closely with the agency. We are very supportive and committed to investing in the development of standardized testing methodologies, including independent standards for facial recognition technology by entities like NIST, that seek to improve accuracy by removing bias from facial recognition technology.

ii. **Please provide as an addendum any relevant guidance Amazon may have on the development and intended use of facial recognition technology.**

Amazon provides extensive documentation and support to our customers to guide development and use of Rekognition, which is made available at https://docs.aws.amazon.com/rekognition/index.html. We have also made clear that we recommend law enforcement customers use Rekognition at a 99% confidence threshold, particularly when a person's rights are at stake. Additionally, we strongly recommend that law enforcement conduct human review of facial recognition matches. More guidance on the development and intended use of facial recognition technology can be found at https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

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.**

Ring does not contract out to, or request assistance from, any external entity regarding facial recognition, but to reiterate, Ring does not currently offer facial recognition technology in Ring products.

Thank you for your attention to this important topic.

Sincerely,

Brian Huseman
Vice President, Public Policy