November 21, 2025

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

Dear Senator Markey,

Thank you for your October 30, 2025 letter regarding Ring's recently announced Familiar Faces feature.

Ring is deeply committed to safeguarding our customers' privacy, safety, and security. Our customers entrust us with protecting what matters most to them — their families, homes, and communities. We honor this trust with robust privacy protections, security measures, and safety innovations that put customers in control.

We believe Familiar Faces represents responsible innovation that addresses real customer needs and honors privacy expectations. Facial recognition is a common feature in smart security cameras and therefore one that customers expect. Familiar Faces is an optional feature that helps users recognize people who regularly appear on their Ring camera. The feature is disabled by default; a customer must choose to enable the feature on their eligible devices. After enabling the feature, customers can identify and tag familiar faces when they appear on their camera. Once tagged, the system will recognize these individuals and send personalized alerts, such as "Emma at Front Door," rather than generic "person detected" notifications. This feature gives customers the ability to reduce notifications triggered by familiar people's routine activities, allowing them to be notified of unique, non-routine events. The feature will start rolling out to customers in the U.S. and Canada in December.

The answers to your specific questions are as follows:

1) Please detail Amazon's Ring FRT privacy practices:

a. How will Ring obtain informed consent from every individual whose biometric data is captured by its devices, including passersby, delivery workers, and guests?

Customers agree to use our products and features in accordance with applicable laws. When they turn on Familiar Faces, we inform them that the feature uses biometric data and we display an in-app message to remind customers that they should comply with applicable laws that may require obtaining consent.

b. How does Amazon notify individuals that their biometric data may be collected without their consent when approaching a home equipped with Ring technology?

See answer to question 1. a. above.

c. How long will Amazon retain biometric data and what policies govern its deletion?

Customers maintain control over their familiar faces and can delete them at any time. Reference data for a familiar face is stored until a customer chooses to delete it. The feature automatically removes reference data for unnamed faces after 30 days.

d. Are Ring owners and all those subjected to video recording, voice recording and facial recognition able to formally request that Amazon delete their data? If so, how will Amazon ensure data is deleted in a timely manner?

Ring complies with applicable data protection laws regarding customer data deletion requests. Ring device owners control their video recordings and non-owners who appear in someone else's Ring recording should contact the device owner directly, as device owners are best positioned to identify and manage specific videos in which individuals may appear. Ring customers who wish to delete their personal information may do so within their account Control Center or by contacting Customer Support for assistance.

e. Does Amazon use biometric data to train machine learning models or improve facial recognition algorithms? If so, are all individuals subjected to FRT informed and given the opportunity to opt out?

Outside of limited data sets where participants have expressly consented to the use of their Ring data, for example beta trials, Ring does not use its customers' biometric data for algorithm or machine learning model training purposes.

f. Has Amazon conducted any privacy impact assessments or third-party audits of Ring's biometric surveillance practices?

Ring conducts privacy impact assessments of data practices through dedicated internal privacy and security teams with specialized expertise in privacy compliance and data protection.

2) Please describe how Amazon will mitigate harmful biases and discrimination often prevalent when using facial recognition technology:

a. Does Amazon test Ring's FRT across different demographic groups, including accuracy rates and potential biases? If so, does Amazon publicly disclose those results?

Ring implements comprehensive bias mitigation measures for facial recognition technology through systematic data collection and testing across diverse demographic groups, including gender, ethnicity, age, and appearance variations. Ring carefully reviews performance metrics of facial recognition models across all demographic categories to ensure they meet quality requirements before deployment. Ring conducts rigorous testing to evaluate accuracy rates and identify potential biases across different demographic groups as part of our commitment to responsible AI development and deployment. We do not publicly disclose detailed test results or specific performance metrics from these assessments.

b. What steps has Amazon taken to ensure Ring's biometric technologies do not disproportionately harm communities of color, immigrants, or other vulnerable populations?

See answer to question 2. a. above.

3) Please describe Amazon's policies for sharing facial recognition and biometric data with law enforcement:

a. Does Amazon share biometric data — including any outputs of facial recognition use collected by Ring doorbells — either voluntarily or in response to legal process, with law enforcement agencies, including the Department of Homeland Security (DHS)?

For information about how Ring receives and responds to law enforcement requests for information, please visit our Law Enforcement Guidelines[1].

[1] https://ring.com/support/articles/oi8t6/Learn-About-Ring-Law-Enforcement-Guidelines

b. Can law enforcement request access to Ring doorbell live streams from Amazon? If so, does Amazon share live stream access with law enforcement agencies, including DHS, either voluntarily or in response to legal process?

Ring does not have a mechanism to provide law enforcement with access to live views.

c. Does Amazon notify users when law enforcement requests access to biometric data collected by Ring devices?

Unless Ring is prohibited from doing so or has clear indication of illegal conduct in connection with the use of Ring products or services, Ring notifies an account owner before disclosing user information in response to a valid and binding legal demand.

d. Will Amazon share any biometric data or data collected from Ring's FRT through NPSS?

Neighbors Public Safety Service (NPSS) is a feature that allows public safety agencies to communicate with communities in the Neighbors app. Ring does not share biometric data through NPSS.

e. Please identify how many of each of the following entities use the NPSS: (i) police departments; (ii) fire departments; (iii) public health agencies; (iv) animal services; (v) agencies that primarily address homelessness, drug addiction, or mental health; and (vi) others (please specify).

Police departments: 2,723
Fire departments: 626
Public health agencies: 0
Animal services: 43
Agencies addressing homelessness, drug addiction, mental health and related social services: 27
Others: 157 (these include local government, neighborhood associations, community art centers, and theater/music organizations)

Ring remains committed to protecting customer privacy and security as we offer new products and services, and we appreciate your interest in these matters.

Sincerely,

Brian Huseman
Vice President, Public Policy