Dear Federal Trade Commissioners,

In purchasing smart surveillance devices that record everything we do and say, consumers unknowingly supply Big Tech with endless streams of data. The data collected fuels and solidifies corporate monopolies at the expense of consumers, workers, and communities. The harms caused by this widespread, unregulated corporate surveillance pose a direct threat to the public at large, especially for Black and brown people most often criminalized using surveillance. Given these dangers, we're calling on the Federal Trade Commission (FTC) to use its rulemaking authority to ban corporate use of facial surveillance technology, ban continuous surveillance in places of public accommodation, and stop industry-wide data abuse.

With no oversight or accountability, corporations have flooded the market with Wi-Fi enabled smart devices. Though many companies sell connected devices, Amazon provides a perfect case study on how monopolistic power compounds unfair practices, and why the FTC must act to prevent further abuses wherever they occur.

One product line alone, Amazon Ring, includes doorbell and floodlight cameras, mailbox sensors, car cams, and soon indoor drones. These Ring devices collectively surveil millions of people—not only inside a purchaser's home but extending to outside public and private spaces, including sidewalks where someone may walk their dog, and to neighboring yards where young children may play.

And that's just one of the product lines in Amazon's smart home ecosystem. The technology giant also sells Alexa, Amazon's voice assistant; Echo, Amazon's smart speakers that facilitate communication with Alexa; and Sidewalk, Amazon's consumer-sourced network. While users unwittingly generate troves of lucrative data sets, Amazon owns the data and capitalizes on the insights generated by them.

Pervasive surveillance entrenches Amazon's monopoly. The corporation's unprecedented data collection feeds development of new and existing artificial intelligence products, further entrenching and enhancing its monopoly power. In turn, these artificial intelligence products require ever increasing amounts of finer grained data, creating a feedback loop, where the most intimate details of our lives are monetized.

Armed with that power, Amazon is in a position to abuse its dominance to the detriment of consumers, communities, and even bystanders who have no commercial relationship with it at all, such as those captured by their neighbors' Ring cameras. As Amazon's surveillance empire grows in size, so do the harms. Some of the harms include:

- **Amazon's Wi-Fi enabled devices have been shown to be deeply insecure** on multiple occasions. Hackers broke into Ring cameras to torment and harass families including one man who watched and spoke to a little girl in her bedroom. The Neighbors App shared the location of installed Ring devices, while the Ring device itself leaked users' Wi-Fi passwords to the public. And Alexa exposed personal information, like

home addresses and banking data, through a vulnerability that gave access to users' voice history. Recently, a whistleblower sounded the alarm on the corporation's poor data security.

Amazon's attempts at improving security are often performative. Consumers who integrate multiple Amazon's smart home products are unable to turn on the end to end encryption on their Ring devices. Sidewalk customers have to opt out instead of opt in to the network—meaning users participate in Sidewalk without consent.

- **Amazon Ring's Neighbors App gamifies the racial profiling of Black and brown people** by facilitating and rewarding self-deputized onlookers to police their neighborhood and escalate reports of "suspicious people" based on who they feel belongs there or not. In one specific instance, a woman shared footage of an unidentified man on her porch on Amazon Ring's Neighbors app, which is digitally patrolled by police. The man was later killed by sheriff's deputies. Amazon's surveillance network fuels the criminalization of Black and brown people by amplifying existing racism in our communities and policing—further subjecting communities of color to repressive police violence and feeding a system of mass incarceration.

- **Amazon collects personal information from children under 13.** In 2019 a coalition of groups filed a complaint urging an investigation of Echo Dot Kids for potentially violating Children's Online Privacy Protection Act (COPPA). Since then, concerns have been raised about other Amazon devices' surveillance of children. Amazon Ring took footage from children's Halloween outings and turned it into a commercial for a national ad campaign, seemingly without parental consent. The advertisement was later pulled.

  Despite the privacy concerns with Amazon Kindle, it is being used as an e-learning device in schools and libraries throughout the country. When it comes to the surveillance of children, Amazon has failed to be clear about what information it collects from kids and how it uses that information. It's also unclear how it obtains verifiable parental consent prior to the collection, use, and/or disclosure of kids' personal data.

- **Amazon's smart surveillance ecosystem sweeps up unprecedented amounts of data that can easily be paired with facial surveillance technology**. These integrations further enable the tracking of people across neighborhoods and cities. Facial recognition is a discriminatory and experimental technology with a bias that harms people of color, women, and gender-non-conforming people. Even if the prejudicial inaccuracies of this technology were somehow fixed, facial recognition would still pose a danger to everyone, not just customers.

- **In over 2,000 cities across the country, Amazon partners with police and fire departments**. For its police partners, Amazon provides warrantless access to request and store footage from thousands of Ring cameras. This backdoor, mass surveillance access gives cops unprecedented power to subvert the Fourth Amendment. Thanks to

> Amazon, police departments in many cities have their own privately-run surveillance network that they access with zero oversight. Once police have this footage, they are free to do what they please with it, including sharing it with other parties.
>
> Furthermore as our nation grapples with the violent policing of Black and brown communities, it's concerning that roughly half of the police departments partnered with Amazon "are responsible for over a third of fatal police encounters nationwide"—a shocking statistic given that only around 7% of our nation's police departments had a Ring partnership at the time.

These harms directly result from the technology giant's unfair and deceptive mass collection, use, or sharing of peoples' data. And it is further deceptive as it's not possible for Amazon to garner meaningful consent, as people can't know or judge the far-reaching future harms. Such harms include identity theft, sharing the data collected with other parties, and applications that amplify bias and discrimination. Furthermore, Amazon's power forces users with no bargaining power to accept onerous and objectionable terms of use, such as granting Amazon the right to use data taken from their private lives for biometric data and AI training.

Addressing these abuses, which are widespread and generalized across the industry, fits within the FTC's rulemaking authority, and the agency derives additional authority to protect against these abuses from the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act.

We are encouraged by the FTC's previous willingness to combat extractive and abusive data harvesting. For example, the agency's recent order against app developer Everalbum requires the company to delete not only its ill-gotten data, but also the facial recognition models or algorithms developed with users' data.

Rulemaking is needed to stop widespread systematic surveillance, discrimination, lax security, tracking of individuals, and the sharing of data. While Amazon's smart home ecosystem, facial surveillance technology, and e-learning devices provide a good case study, these rules must extend beyond this one technology corporation to include any entity collecting, using, selling, and/or sharing personal data.

It's incumbent on the FTC to exercise the full extent of their rulemaking authority to ban corporate use of facial surveillance technology, ban continuous surveillance in places of public accommodation, and stop industry wide data abuse. Until the FTC acts, no one is safe.

Sincerely,

Action Center on Race & the Economy
Athena
Center for Popular Democracy Action
Constitutional Alliance

Consumer Federation of America
Council on American-Islamic Relations
Demand Progress Education Fund
Demos
Encode Justice
Fight for the Future
For Us Not Amazon
Institute for Local Self-Reliance
Instituto de Educacion Popular del Sur de California
Jobs With Justice
Just Futures Law
La ColectiVA
Liberation in a Generation
Line Break Media
Make the Road New Jersey
Media Freedom Foundation
MediaJustice
Mercy Investment Services, Inc.
Movement Alliance Project
MPower Change
National Employment Law Project
New York Communities For Change
OLÉ
Open Markets Institute
Open MIC (Open Media & Information Companies Initiative)
OVEC-Ohio Valley Environmental Coalition
Performing Arts Alliance
Philadelphia Jobs With Justice
PowerSwitch Action formerly known as Partnership for Working Families
Presente.org
Project Censored
Public Citizen
Revolving Door Project
RootsAction.org
S.T.O.P. – Surveillance Technology Oversight Project
Secure Justice
Stand Up Nashville
SumOfUs
United for Respect
Warehouse Worker Resource Center
Warehouse Workers for Justice
Whistleblower & Source Protection Program at ExposeFacts
Woodhull Freedom Foundation
X-Lab