Ringing Alarm Bells
A study of implicit bias in consumer surveillance device use in San Francisco

Summary

Ringing Alarm Bells is a study conducted by Oakland Privacy and Media Alliance in the spring of 2020. The study examined a sampling of content posted to the Ring "Neighbors" application in the City of San Francisco.

Volunteers reviewed videos and accompanying posted material and examined whether the videos portrayed, implied or suggested a crime taking place, whether the text accompanying the private smart doorbell videos was consistent or inconsistent with what the footage actually contained, and provided demographic data for the video sampling.

Summary of Results

- One third of the surveyed videos were poorly lit and it was difficult to impossible to see what was happening in the video footage.
- In forty percent of the surveyed videos, the text accompanying the video did not accurately reflect the contents of the video
- Black men were overwhelmingly over-represented in the videos posted on Neighbors by San Franciscan Ring owners. Black men were subjects in a third of the videos, although they are only 5.6% of the city of San Francisco's population per 2019 demographic data.
- When videos described as "unclear" by reviewers (due to poor lighting or activity out of range of the doorbell camera) are removed, the super majority of the videos (seventy-five percent) contain subjects who are people of color. San Francisco's population per 2019 demographic data is fifty-three percent white.
- When videos described as "unclear" were included, forty-seven percent contained people of color subjects, twenty-nine percent contained white subjects, and twenty-three percent were impossible to determine.
- Forty-two percent of the videos were categorized by the posters as crimes, with the largest percentage being claimed package theft, with smaller amounts for mail theft, bicycle theft, lost pets and one percent claiming house break-ins. Thirty-five percent of the videos were characterized by the posters as strangers in the neighborhood or people acting suspiciously.

- Of the videos claimed by posters to show suspicious behavior, sixty-four percent contained subjects who were people of color.
- Only fifty-seven percent of videos categorized by the posters as crimes were determined to clearly show evidence of a crime against property by objective reviewers.

Methodology

Oakland Privacy and Media Alliance wished to create a data set of typical Ring smart doorbell videos placed voluntarily into the public domain by San Francisco device owners.

The Neighbors application provided a way to acquire a sample set and to analyze the characteristics of such videos, which by their public placement on an application probably were a reasonably good match with video content that might be submitted or solicited by a law enforcement agency.

The public nature of the videos also meant they were by definition available to neighbors, neighborhood watch groups, local businesses and local state agencies who cared to look at them.

To begin our study, we spoke with researchers at the Massachusetts Institue of Technology (MIT), who had scraped the Neighbors application and were developing nationwide sample sets. They provided us with a 131 video set from the city of San Francisco.

The dataset was sub-divided into five groups (sample sub-divided set at http://www.mediafire.com/file/4nikl672zgizdg2/Ring+Data+Sample+Set.xls/file).

Five volunteers were recruited, 1 per set, to review the material and fill out a log sheet where they answered specific questions about the contents of the video and the accompanying post text. The questions were developed by project managers Tracy Rosenberg and Heather Akers-Healy.

The log sheet can be seen here.

The raw response data can be found at:

http://www.mediafire.com/file/vj8mz6my0fce205/Ring+San+Francisco+Log+Sheet+(Responses).xls/file .

Each volunteer worked independently and was encouraged to watch each video multiple times before filling out the log response sheet and to include notes as needed.

Background

San Francisco passed Proposition B in 2018. Proposition B encouraged regulation of how the city handles the personal information of its residents, including that generated by contractors, third parties and businesses. Among the guidelines in the ballot measure intended to guide city policy making:

- Discourage the collection, storage, sharing, or use of Personal Information, including Personal Information that may identify an individual's race, religion or creed, national origin, gender, sexual orientation, age, physical or mental disability, or other potentially sensitive demographic information, unless necessary to accomplish a lawful and authorized purpose.

- Allow individuals to move and organize throughout the City without being tracked or located in a manner that subjects them to collection of Personal Information without their consent.

- Evaluate and mitigate bias or inaccuracy in the collection, storage, sharing, or use of Personal Information, and anticipate potential bias in secondary uses of and algorithms used in connection with Personal Information.

Ring and Law Enforcement

San Francisco does not currently have a Ring/Law Enforcement agreement in place, although these agreements are in place in a growing number of municipalities throughout the Bay Area. Municipalities that have signed such agreements include San Jose, South San Francisco, Milpitas, Union City, Walnut Creek, Novato, Foster City, Hercules, and the Marin County Sheriff's Office, At least 2,500,000 Ring smart doorbell devices have been sold across the country.

Law enforcement/Ring agreements contain a confidentiality clause regarding the terms of the program which is contrary to public transparency best practices. Ring agreements, in particular, constrain via contract, the language municipal agencies can use in speaking about the Ring product line or the Neighbors application. The written agreements give Ring some level of editorial control over some City and County public safety announcements.

Law enforcement/Ring agreements ask municipalities to promote and sometimes subsidize the cost of Amazon product purchases by residents in exchange for access to the surveillance footage, making the city complicit in the growth of privatized video surveillance. Local law enforcement agencies can become proxy Amazon salespeople.

Law enforcement/Ring agreements state the consent of the owner is required before turning video and accompanying post commentary over to law enforcement. But as our study shows, the Neighbors application content, as easily downloaded from app stores, makes a substantial amount of doorbell video a public matter.

The subjects captured in video, regardless of whether what is recorded suggests criminal activity, can not and do not give their consent.

Much of the material captured by smart doorbells does not consist of verified or even suspected criminal behavior, but can include looking suspicious or out of place in the eyes of a device owner.

This can direct extra scrutiny to often-targeted populations like homeless individuals, young black and brown men, and the mentally ill.

Law enforcement/Ring agreements come with a map interface of where the devices are located, without owner consent, so that private households making private purchases to secure their private property are drafted into a neighborhood surveillance map.[1]

1 https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true

If law enforcement requests Ring video from a device owner, and that owner does not give their consent:

"If we ask within 60 days of the recording and as long as it's been uploaded to the cloud, then Ring can take it out of the cloud and send it to us legally so that we can use it as part of our investigation. According to what police have been told by Amazon, most people "play ball". [2]

The company coaches participating law enforcement agencies in how to encourage smart doorbell owners to surrender their footage upon request and without a warrant. [3]

Absent a) reasonable suspicion that a crime is or has been committed or b) the completely voluntary submission of privately recorded footage by the owner of a private security device; the state has no claim to obtain, or reason to browse, privately recorded footage taken on private property.

Yet Amazon's Ring devotes itself to creating structures, including a public smartphone application and a network of law enforcement cooperative agreements to enable that state scrutiny, thus blurring the lines between private security and state surveillance.

2 https://www.govtech.com/security/Amazons-Ring-Video-Camera-Alarms-Privacy-Advocates.html
3 https://www.vice.com/en_us/article/43kga3/amazon-is-coaching-cops-on-how-to-obtain-surveillance-footage-without-a-warrant

Implicit Bias

The implicit bias found in this study, as represented by the exaggerated presence of people of color as subjects in videos posted to Neighbors from San Francisco Ring smart doorbell owners, shouldn't be a surprise. Highly technical algorithims designed for biometric identification have been demonstrated to be less trained on and less effective with Black and brown and female populations who are less present in the coding and engineering communities. To expect a better result from a random group of San Francisco property owners would have been idealistic.

But the specific nature of Amazon Ring's product and surveillance network should ring alarm bells due to its unique qualities. Like Next Door, Citizen and various transit watch apps, neighbors aggregates publicly random information provided without any standards for accuracy, fact-checking (do the videos match their characterization by the poster?), and a definition of crime or at least potential crime that falls woefully short of any legal standard like reasonable suspicion or probable cause. Moreover, information that is publicly distributed on a smartphone application anyone can download, [4] contains no information about the poster, their prejudices, biases or motivations. Posters can certainly be motivated by altruistic concerns about safety in their neighborhoods, but other motivations including personal feuds or political leanings are possible. Characterizing a person as a thief or a robber, as our study demonstrates, requires only a video of a visit and a creative way with language. Similarly, none of us are exempt, and some of us are especially prone, to be characterized as a “stranger danger” source of general suspicion.

Unlike those other applications, Amazon's Ring products are accompanied by an ever-expanding web of collateral agreements with law enforcement agencies, who push the devices and then actively engage with the footage. The well-established record of discriminatory policing doubles down with the widely held implicit bias of much of the public to co-opt property owners into amplifying racially biased policing.

The use of the understandable concerns of property owners about the security of their personal property to expand the surveillance state is deeply cynical on the part of Amazon Ring. It lifts up neighborhood watch dynamics to a new and dangerous double feedback loop that makes the implicit all too explicit.

Your kind ain't welcome here. With a picture relayed to the men with the guns.

---

4 The author of this paper does not own a Ring device and downloaded the Neighbors app and activated it easily. The user is able to enter any street address, including one that may not be their own, and view postings from that area.