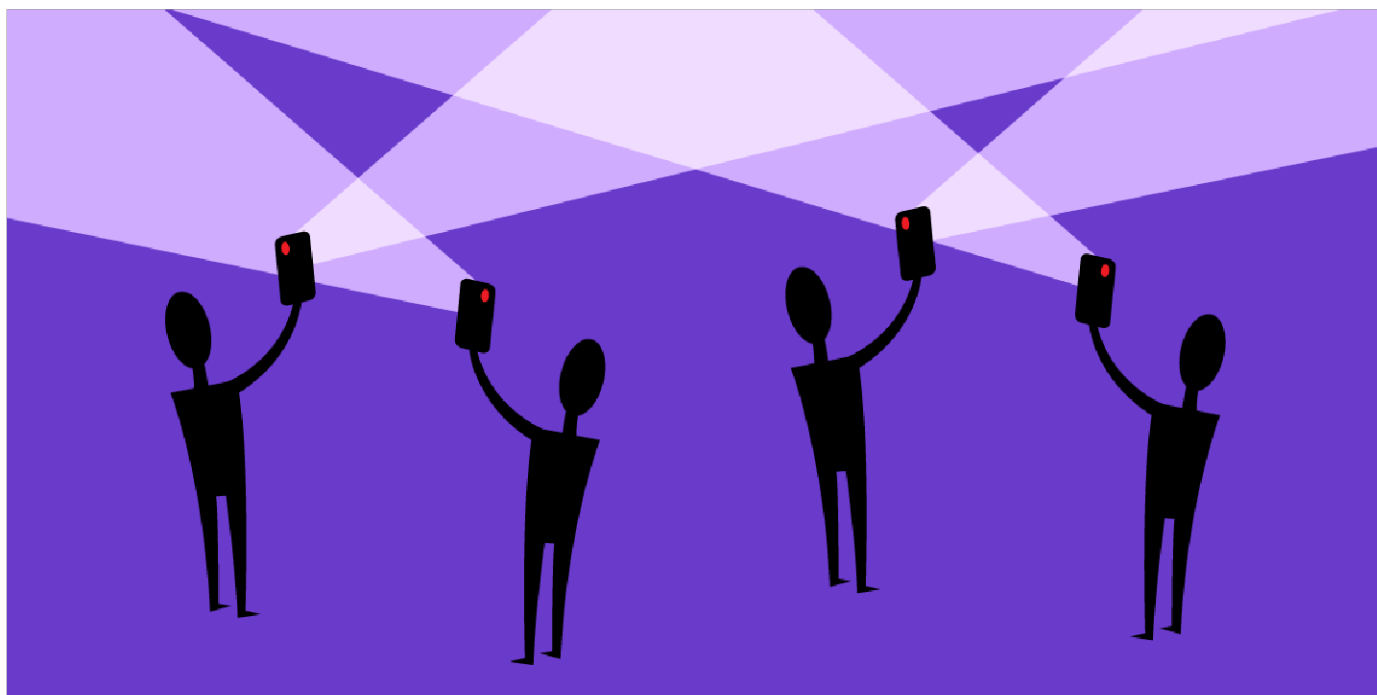


STREET LEVEL SURVEILLANCE



COMMUNITY SURVEILLANCE APPS

Technology rarely invents new societal problems. Instead, it digitizes them, supersedes them, and allows them to balloon and duplicate at the speed of light. That's exactly the problem we've seen with location-based, crowd-sourced "public safety" apps.

A slew of popular apps have flooded the market which purport to show a person the potential hazards around them and in their neighborhood. The problem is that rather than making people feel safer and better informed, they can have the opposite effect of making people feel terrified and as if their community is less safe than it actually is by amplifying and notifying users of unfounded reports on a near constant basis. There is also a very real fear that these applications, if not seriously moderated or shifted to make their objective to be more about community building and less about public paranoia, can inadvertently unleash racially biased or even vigilante violence or harassment against already marginalized people.

How it works

by posting pictures, items for sale, or local tips. Others, however, focus exclusively on things and people that users see as “suspicious” or potentially hazardous, while others generate and map alerts based on 911 calls. These alerts run the gamut from active crimes, or the aftermath of crimes, police activity, or just generally anything someone might pick up the phone to call 911 about—up to and including unconfirmed reports of what the caller interprets as suspicious behavior.

Having access to 911 call data through police scanners or other important tools of citizen journalism or government transparency work comes with a grain of salt—people who use these tools often know they are listening to raw information that could turn out to be false suspicions or can easily be taken out of context—but when these calls are presented as big red dots on a map near your home, it’s much more likely to be taken as a real imminent threat rather than an initial report in need of follow up.

As the [New York Times](#) writes, Citizen is “converting raw scanner traffic—which is by nature unvetted and mostly operational—into filtered, curated digital content, legible to regular people, rendered on a map in a far more digestible form.” In other words, they’re turning static into content with the same formula the long-running show *Cops* used to [normalize](#) both paranoia and police violence.

Apps like Citizen have also been known to be [triggered by ShotSpotter](#), acoustic gunshot detection technology used in cities which studies have shown is [wildly inaccurate and which we fear leads to heavily armed police being called to confront gun violence](#) and finding only unarmed pedestrians and a false positive alert.

Who Sells It

A number of different companies have created various products that live somewhere on the spectrum of “community forum and discussion board” to “real-time alerts of police activity and 911 calls in your area.” Amazon has its Neighbors app which links to the popular surveillance doorbell [Amazon Ring](#) as well as Nextdoor and Citizen. Facebook closed down its version, called [Neighborhoods](#), in 2022.

Threats Posed by It

These apps are often designed with a goal of crowd-sourced surveillance, like a digital neighborhood watch. A way of turning the aggregate eyes (and phones) of the neighborhood into an early warning system. But instead, they often exacerbate the

outcome to posting a suspicious sight to the app isn't just to warn your neighbors—it's to summon authorities to address the issue.

And even worse than incentivizing people to share their most paranoid thoughts and racial biases on a popular platform are the experimental new features constantly being rolled out by apps like Citizen. First, it was a private security force, available to be summoned at the touch of a button. Then, it was a service to help make it (theoretically) even easier to summon the police by giving users access to a 24/7 concierge service who will call the police for you. There are scenarios in which a tool like this might be useful—but to charge people for it, and more importantly, to make people think they will eventually need a service like this—adds to the idea that companies benefit from your fear.

It's well known that Citizen began its life as "Vigilante," and much of its DNA and operating procedure continue to match its former moniker. Citizen, more so than any other app, is unsure if it wants to be a community forum or a Star Wars cantina where bounty hunters and vigilantes wait for the app to post a reward for information leading to a person's arrest.

When a brush fire broke out in Los Angeles in May 2021, almost a million people saw a notification pushed by Citizen offering a \$30,000 reward for information leading to the arrest of a man they thought was responsible but was in fact an unhoused man who was unrelated to the fire. Citizen incentivizing, with money, its users to target and report on an innocent person exemplifies the danger these apps impose.

Make no mistake, this kind of crass stunt can get people hurt. It demonstrates a very narrow view of who the "public" is and what "safety" entails.

EFF's Work Related to It

Paranoia about crime and racial gatekeeping in certain neighborhoods is not a new problem. Citizen takes that old problem and digitizes it, making those knee-jerk sightings of so-called suspicious behavior capable of being broadcast to hundreds, if not thousands of people in the area.

But focusing those forums on crime, suspicion, danger, and bad-faith accusations can create havoc. No one is planning their block party on Citizen like they might be on other apps, which is filled with notifications like "unconfirmed report of a man armed with pipe" and "unknown police activity." Neighbors aren't likely to coordinate trick-or-treating on a forum they exclusively use to see if any cars in their neighborhood were

you were formerly comfortable in is now under siege, you're going to use it not just to doom scroll your way through strange sightings, but also to report your own suspicions.

These apps are part of the larger landscape that law professor Elizabeth Joh calls “networked surveillance ecosystems.” The dearth of laws governing private surveillance networks like Amazon Ring and other home surveillance systems—in conjunction with social networking and vigilante apps—is only exacerbating age-old problems. EFF believes this is one ecosystem that would be much better contained.

Suggested Additional Reading

Joh, Elizabeth E., *Networked Self-Defense and Monetized Vigilantism: Private Surveillance Systems* (July 26, 2021). [Available at SSRN](#)

[The rise of fear-based social media like Nextdoor, Citizen, and now Amazon's Neighbors \(Vox\)](#)

TECHNOLOGIES