THE SPY NEXT DOOR

The Danger of Neighborhood Surveillance Apps

PAULA GARCIA-SALAZAR NINA LOSHKAJIAN ALBERT FOX CAHN, ESQ. ELENI MANIS, PHD, MPA

NOVEMBER 30, 2021





I. <u>Introduction</u>

Everyone sees them: signs "welcoming" you to a neighborhood with the warning that "All Suspicious Persons and Activities Reported to Law Enforcement." In the 1960's, Neighborhood Watch groups proliferated in supposed response to increased burglaries. In fact, the groups appear to have been a direct response to increased residential integration. A brainchild of the National Sheriffs Association, Neighborhood Watch groups were touted as a way to increase community involvement in crime prevention by encouraging residents to patrol their own streets and act as the eyes and ears of the local police. But too often, local residents have interpreted this as a chance to become vigilantes, in many cases acting purely on bias to raise false alarms and profile fellow community members, endangering the very people these groups are allegedly designed to protect. The groups have proliferated across the country even as they have been demonstrated to promote profiling and distract from actual public safety, there being little evidence that Neighborhood Watch programs reduce crime.

Now, a new form of Neighborhood Watch is here: smartphone-based apps that supplant the classic program with online forums for local neighborhoods. Nextdoor (27 million regular users), Neighbors by Ring (10 million users), Citizen (7 million users), and recently piloted Facebook Neighborhoods deliver "hyperlocal" updates to geographic "neighbors." Nextdoor and Facebook Neighborhoods invite users to post on a range of local-interest content: upcoming events, business reviews, goods for sale, and so on. But the backbone of neighborhood surveillance apps is crime, both real and imagined. Apps encourage users to upload video footage, photos and descriptions of suspected crimes and supposedly "suspicious" people near their homes, producing reports riddled with dog whistles and overt racism. Apps court a police audience for these posts and enable police to request app users' video footage, photos, and input. Apps even drive user engagement by inviting bystanders join in on the crime-oriented conversation: as on Facebook, users can comment, "like" and otherwise interact with posts with the click of a button.

¹ About National Neighborhood Watch, National Neighborhood Watch, http://www.nnw.org/about-national-neigborhood-watch.

² Adeoye Johnson, "Neighborhood Watch: Invading the Community, Evading the Constitutional Limits," Univ. of Pennsylvania Journal of Law and Social Change, Vol. 18.5, 2016,

https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1194&context=jlasc.

³ Katy Holloway, Trevor Bennett, and David P Farrington, "Does Neighborhood Watch Reduce Crime?," Crime Prevention Research Review No. 3 (U.S. Department of Justice, 2008), https://journalistsresource.org/wp-content/uploads/2012/03/e040825133-res-review3.pdf.

⁴ Johnson, "Neighborhood Watch," at 470.

⁵ Holloway, "Neighborhood Watch Reduce Crime?"

⁶ Alex Wilhelm, "Nextdoor's SPAC Investor Deck Paints a Picture of Sizable Scale and Sticky Users," *TechCrunch*, July 6, 2021, https://social.techcrunch.com/2021/07/06/nextdoors-spac-investor-deck-paints-a-picture-of-sizable-scale-and-sticky-users/.

⁷ Lauren Bridges, "Amazon's Ring Is the Largest Civilian Surveillance Network the US Has Ever Seen | Lauren Bridges," *The Guardian*, May 18, 2021, sec. Opinion, http://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us. *See also* Rani Molla, "Amazon Ring Sales Nearly Tripled in December despite Hacks," Vox, January 21, 2020, https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data.

⁸ Theo Wayt, "Citizen Pays New Yorkers \$25 an Hour to Livestream Crime Scenes," New York Post (blog), July 25, 2021, https://nypost.com/2021/07/25/citizen-pays-new-yorkers-25-an-hour-to-livestream-crime-scenes/.

These exchanges on neighborhood surveillance apps imagine threats where they don't exist, endangering communities and making the public no safer. Amazon claims that a pilot of Ring surveillance doorbells (whose footage users post on the Neighbors app) reduced crime in a Los Angeles neighborhood by 55%, but a follow-up study showed a much smaller reduction and a dramatic uptick in robberies the following year. An investigation of 40 police departments in eight states found no evidence of crime reduction due to Ring and Neighbors—but did find that precincts reported officers spent too much time "reviewing clips of non-criminal issues such as racoons."

Neighborhood surveillance apps erode our sense of safety and social trust, substituting racial profiling, vigilantism, and neighbor-on-neighbor spying. Apps are hotbeds for racial profiling and harassment of BIPOC individuals. Apps promote vigilantism by showing users a constant stream of fear and rage-inducing reports on supposed crimes and suspects just a few blocks or a few feet away. Apps recruit neighbors to spy on one another, extending the police surveillance state to locations where officers themselves cannot record video. The web of public and private cameras available to police increasingly encapsulates whole cities, leaving no corner unwatched. Apps also collect sensitive personal data about users and the individuals they target in posts, putting both at grave risk in the event of security lapses, data breaches or unscrupulous data sharing by apps.

II. How Neighborhood Surveillance Apps Work

As of September 2021, there are three major neighborhood surveillance apps in the US: Nextdoor, Citizen, and Neighbors by Ring. Facebook piloted a fourth app, Neighborhoods, in late 2020.

1. Nextdoor and racial profiling

Nextdoor, the oldest neighborhood surveillance app, launched in 2011.¹² It appears to be the largest as well: Nextdoor reported 27 million weekly users in July 2021¹³ and claimed that "one in three U.S. households are on the platform."¹⁴ The app has achieved this scale by pushing key functions of its platform onto unpaid users. ¹⁵ Users set the boundaries of Nextdoor neighborhoods, with the first member of the website in any given area able to choose their neighborhood's name and set its parameters. ¹⁶ Users provide all content for Nextdoor, ranging from reports of perceived crimes to

⁹ Mark Harris, "Video Doorbell Firm Ring Says Its Devices Slash Crime—but the Evidence Looks Flimsy," MIT Technology Review, October 19, 2018, https://www.technologyreview.com/2018/10/19/103922/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/.

¹⁰ Cyrus Francisco, "Cute Videos, but Little Evidence: Police Say Amazon Ring Isn't Much of a Crime Fighter," NBC News, February 15, 2020, https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026.

¹¹ Jessi Hempel, "For Nextdoor, Eliminating Racism Is No Quick Fix," Wired, February 16, 2017, https://www.wired.com/2017/02/for-nextdoor-eliminating-racism-is-no-quick-fix/.

¹² Ellen Lee, "Nextdoor Offers Online Forum for Neighborhoods," SFGATE, March 2, 2012, sec. Tech and Social Media, https://www.sfgate.com/tech/article/Nextdoor-offers-online-forum-for-neighborhoods-3375382.php.

¹³ Wilhelm, "Nextdoor's SPAC Investor Deck."

¹⁴ Kim Hart, "The Next Big Social Network: Nextdoor," Axios, June 14, 2021, https://www.axios.com/the-next-big-social-network-nextdoor-2bc336aa-e50b-4ea8-b097-f273bd5994d6.html.

network-nextdoor-2bc336aa-e50b-4ea8-b097-f273bd5994d6.html.

15 Makena Kelly, "Inside Nextdoor's 'Karen Problem," The Verge, June 8, 2020, https://www.theverge.com/21283993/nextdoor-app-racism-community-moderation-guidance-protests.

Nextdoor states on its website that the company "reserves the right to make corrections to name and boundaries based on feedback from other neighbors or to adhere to Nextdoor's guidelines on neighborhood names." "How to Create Your Neighborhood," Nextdoor Help Center, https://help.nextdoor.com/s/article/How-to-create-your-neighborhood?language=en_US.

local news and business reviews. 17 Users lead content moderation—for free—for Nextdoor, 18 while Nextdoor provides primarily automated oversight of posts. ¹⁹ This cost-cutting approach to moderating has allowed racism to fester on Nextdoor, which has for years failed to stop racial profiling by its users and subsequent harassment of profiled individuals by the police. 20 Evidence for this harassment is anecdotal but abundant, ranging from a Black real estate agent who was interrogated by police after Nextdoor users reported his door knocking²¹ to a high schoolerorganized Black Lives Matters protest that police investigated after a Nextdoor moderator suggested the protest was a riot.²²

2. Citizen and vigilante behavior

Citizen, launched in 2016 as "Vigilante," is a crime-focused neighborhood surveillance app that encourages civilians to investigate suspected crimes.²³ It had more than 7 million users in July 2021²⁴ and is growing fast: at the time of this writing, Citizen was the 5th most popular "News & Magazines" free app for iPhones²⁵ and the 10th most popular app in the same category for Android phones.²⁶ Citizen employees generate the first layer of the app's content, transcribing and posting police and fire departments' two-way radio communications in real time.²⁷ Citizen then prompts nearby users to record and upload video of "crime sites" in the style of investigative reporters. ²⁸ (As of July 2021, employees masquerading as ordinary users also record and post videos.)²⁹ Despite dropping its "Vigilante" branding, Citizen still encourages vigilantism—in May 2021, it went so far as to mistakenly put a large bounty on an innocent man's head. 30 Given users' patterns of racial profiling, vigilante behavior on Citizen disproportionately endangers BIPOC communities.

¹⁷ "About Nextdoor," accessed October 31, 2021, https://about.nextdoor.com/.

¹⁸ "Keeping Conversations Neighborly," Nextdoor Help Center, accessed August 9, 2021, https://help.nextdoor.com/s/article/Keeping-conversations-neighborly?language=en US. See also "About Nextdoor Leads," Nextdoor Help Center, accessed August 9, 2021, https://help.nextdoor.com/s/article/About-Nextdoor-Leads?language=en_US. ¹⁹ Daniel Masquelier, "The Kindness Reminder," Nextdoor Engineering, October 16, 2019, https://engblog.nextdoor.com/the-kindness-reminder-868252995140.

²⁰ Hempel, "For Nextdoor, Eliminating Racism."

²¹ Martha Ross, "Nextdoor: When a Neighborhood Website Turns Unneighborly," Mercury News, September 1, 2015, https://www.mercurynews.com/2015/09/01/nextdoor-when-a-neighborhood-website-turns-unneighborly/. ²² Kelly, "Inside Nextdoor's 'Karen Problem."

²³ Sarah Wallace, Kristina Pavlovic, and Dave Manney, "NYC Crime-Fighting App Once Booted From Tunes Is Back, But Law Enforcement Concerns Persist," NBC New York (blog), June 16, 2017, https://www.nbcnewyork.com/news/local/citizen-appcrime-fighting-watchdog-new-york-city-store-itunes-safe-police-cops-fight-investigation-i-team/120111/.

²⁴ Wayt, "Citizen Pays New Yorkers."

²⁵ "Today's Top App Store Rankings [iPhone]," App Annie, accessed July 26, 2021, https://www.appannie.com/en/apps/ios/top/united-states/news/iphone/.

²⁶ "Today's Top App Store Rankings [Google Play]," App Annie, accessed July 26, 2021, https://www.appannie.com/en/apps/google-play/top/united-states/news-and-magazines/.

²⁷ John Herrman, "All the Crime, All the Time: How Citizen Works," New York Times, March 17, 2019, sec. Style, https://www.nytimes.com/2019/03/17/style/citizen-neighborhood-crime-app.html.

²⁸ Herrman, "All the Crime."

²⁹ Wayt, "Citizen Pays New Yorkers."

³⁰ Jenny Gross, "Devin Hilton Falsely Accused by Citizen App of Starting Wildfire," New York Times, May 18, 2021, https://www.nytimes.com/2021/05/18/business/citizen-app-arson-wildfire-devin-hilton.html.

3. Neighbors by Ring and police partnerships with "civilian spies" and big tech

Ring, an Amazon subsidiary that sells video-recording doorbells, introduced the Neighbors neighborhood surveillance app in 2018.³¹ Neighbors had 10 million users in September 2020 and could eventually rival Nextdoor in size, based on the number of Ring devices sold. ³² Like Citizen, Neighbors focuses on crime, inviting users to "[g]et real-time crime and safety alerts from your neighbors and local law enforcement."33 Amazon actively recruits local law enforcement agencies to join Neighbors, and as of May 2021, 1 in 10 US police precincts have joined the app. 34 Neighbors massively extends the reach of police surveillance by recruiting civilians—"neighbors"—to spy on one another, increasing police surveillance of everyday life in residential neighborhoods. This volunteered labor adds up to serious surveillance work: police precincts made 22,000 individual requests for Ring footage in the year ending April 2021. 35 Initially, law enforcement was provided a special portal on the app³⁶ through which they could request content even if users had not posted it publicly. Starting in June 2021, in response to public outcry about the police overreach that portal enabled, police are no longer able to request video footage by contacting app users directly via email, but they may still make "Requests for Assistance," a new type of post that users can respond to publicly or privately.³⁷ While this new system may allow for slightly greater transparency, the partnership with the police has not ceased, meaning that Ring continues to play a central role in building up the surveillance apparatus of the state.

4. Facebook Neighborhoods and privacy concerns

Facebook piloted the Neighborhoods app in Calgary, Canada in October 2020 and has since expanded to San Diego, Baton Rouge, Charlotte, and Newark. Neighborhoods offers Nextdoor's suite of offerings for local communities: event postings, business reviews, goods for sale—and crime. ³⁸ Like Nextdoor, it relies on users' free labor to moderate posts, introducing the same risk of racial profiling. ³⁹ The app also raises serious privacy concerns for individuals targeted by users as "suspicious" and for users themselves. Given Facebook's history of data breaches, ⁴⁰ its violative sharing of user data with other companies, ⁴¹ and its willingness to monetize user data, ⁴² individuals identified in users' posts have no reason to trust that Facebook will safeguard their names, images,

https://play.google.com/store/apps/details?id=com.ring.neighborhoods&hl=en_US&gl=US.

³¹ Kurt Schlosser, "In First Move since Amazon Acquisition, Ring Launches Neighbors App to Help Users Fight Crime," GeekWire, May 8, 2018, https://www.geekwire.com/2018/first-move-since-amazon-acquisition-ring-launches-neighbors-app-help-users-fight-crime/.

³² Bridges, "Ring Civilian Surveillance Network." See also Molla, "Amazon Ring Sales Tripled."

³³ See opening line of Neighbors by Ring app store description:

³⁴ Bridges, "Ring Civilian Surveillance Network."

³⁵ Bridges, "Ring Civilian Surveillance Network."

³⁶ Ring Neighbors Portal Quickstart Guide, https://www.documentcloud.org/documents/21063649-public-safety-quickstart-guide.

³⁷ David Priest, "Ring Will Stop Sending Video Requests from Police to Neighbors App Users," CNET, June 3, 2021, https://www.cnet.com/home/security/ring-will-stop-sending-video-requests-from-police-to-neighbors-app-users/.

³⁸ Abbie Alford, "Facebook Testing Neighborhood App in San Diego," CBS8, May 10, 2021, https://www.cbs8.com/article/news/local/facebook-testing-neighborhood-app-in-san-diego/509-3f592013-0c4f-4c9d-908f-92cae630df57.

³⁹ Rebecca Heilweil, "Facebook Is Copying Nextdoor with New Community Moderator Features - Vox," Vox, June 16, 2021, https://www.vox.com/recode/2021/6/16/22537219/facebook-nextdoor-misinformation-content-moderation-private-groups. ⁴⁰ Lily Hay Newman, "What Really Caused Facebook's 500M-User Data Leak?," Wired, April 6, 2021, https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/.

⁴¹ Alexis C. Madrigal, "Facebook Didn't Sell Your Data; It Gave It Away," Atlantic, December 19, 2018, https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599/.

⁴² Matthew Johnston, "How Facebook Makes Money," Investopedia, January 30, 2021,

https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp.

reputations, or safety. For the same reasons, app users would be foolish to trust that Facebook will treat any sensitive personal data they entrust to Neighborhoods with care.

III. Key Concerns with Neighborhood Surveillance Apps

Profiling Endangers BIPOC Communities

Racial profiling is common on neighborhood surveillance apps and poorly checked by app companies. Nextdoor users have targeted BIPOC people with allegations of criminality since its inception. The company failed repeatedly to address the problem, relying on low-cost interventions that fail to stop racial profiling—automated warnings that discourage race-only descriptions of "suspects" that can easily be bypassed. An investigation of the Neighbors app found similar racial profiling: a majority of reports in affluent parts of Brooklyn and Manhattan targeted BIPOC individuals, frequently using explicitly racist language. Ease Citizen has engaged in several high-profile examples of profiling. The CEO and founder, Andrew Flame, accused an innocent unhoused man of arson and put a bounty on his head. There are also commonly false alarms raised on the platform, as was the case when a user in Oakland flagged a family gathering as "30 men armed with guns." Profiling drives engagement on these platforms, which operate by inflaming users' fear.

Indeed, profiling and stereotyping are a feature, not a bug, for neighborhood surveillance apps. Apps invite users to report not only confirmed crimes but perceived crimes and even people whom users perceive as suspicious. Neighbors allows users to post any Ring-generated videos with nearly any accusation. Nextdoor has a similarly permissive posting policy. Citizen does not confirm the validity of crime posts. These apps are free to indulge their basest, most racist instincts to target those who are simply going about their day. Anyone who users view as "out of place" is vulnerable. Particularly suspicious users have taken apps' posting liberty to extremes, jumping to conclusions and alarming their neighbors before important facts are established. One woman posted Ring video footage of someone approaching her home and taking a package from the doorstep on the Neighbors app with the title "Package thief?" Other users aroused to fear and suspicion by the post replied, some offering innocent explanations for the woman's behavior and others accusing her of theft, only for the original poster to reveal that she had discovered that the woman in the video was her own daughter. There is no due process on neighborhood surveillance apps, just suspicion, allegations, and all too often, a call to the police. The police.

44 Nirav Tolia, "Reducing Racial Profiling on Nextdoor," Nextdoor Blog, August 24, 2016, https://blog.nextdoor.com/2020/06/11/a-nextdoor-where-everyone-belongs/.

⁴³ Hempel, "No Quick Fix."

⁴⁵ Caroline Haskins, "Amazon's Home Security Company Is Turning Everyone Into Cops," Vice, February 7, 2019, https://www.vice.com/en/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops.

⁴⁷ Jacob Silverman, "The Citizen App's Gamification of Vigilantism," *The New Republic*, June 15, 2021, https://newrepublic.com/article/162747/citizen-app-crime-stats-private-security.

⁴⁷ Jacob Silverman, "The Citizen App's Gamification of Vigilantism," *The New Republic*, June 15, 2021, https://newrepublic.com/article/162747/citizen-app-crime-stats-private-security.

⁴⁸ Haskins, "Amazon's Home Security Company."

⁴⁹ Michael Finch II, "California Police Partnerships with Amazon Ring Raise Alarms about Racial Bias, Privacy," The Fresno Bee, July 6, 2020, https://www.fresnobee.com/article243970017.html

⁵⁰ Sharon Finegan, "Watching the Watchers: The Growing Privatization of Criminal Law Enforcement and the Need for Limits on Neighborhood Watch Associations," *University of Massachusetts Law Review* 8, no. 1 (March 24, 2014), https://scholarship.law.umassd.edu/umlr/vol8/iss1/3.

Profiling on neighborhood surveillance apps isn't just offensive, it is dangerous. Even a mundane encounter with police can be fatal, especially for BIPOC individuals and members of other marginalized groups. Police are nearly 3 times as likely to fatally shoot a man who is Black versus one who is white,⁵¹ and Black drivers and passenger are the victims of a third of fatal traffic stops.⁵² While every police killing is a tragedy, Black victims are twice as likely as white victims to be unarmed.⁵³ Americans with disabilities also face heightened police threats, comprising 30-50% of the victims of police use of force.⁵⁴ In a country where mental health crises are often met with a baton or a gun, surveillance apps can be a deadly threat to those in need of medical assistance. LGBTQ+ individuals⁵⁵ and members of other marginalized groups have faced additional threats.⁵⁶ Neighborhood surveillance apps are also used to criminalize dissent. The Los Angeles Police Department used Ring/Neighbors to investigate Black Lives Matter protestors in 2020.⁵⁷

Neighborhood Surveillance Apps Invite Dangerous Vigilantism

Neighborhood surveillance apps also invite dangerous interactions with self-deputizing users who use apps to take the law into their own hands. Citizen (then "Vigilante") was initially booted from app stores after the New York City Police Department objected to its users' behavior and to the app encouraging bystanders to become involved in potentially dangerous situations at active crime scenes. The app, even rebranded, has failed to learn from those mistakes. In May 2021, Citizen orchestrated its first paid manhunt, offering \$30,000 for tips leading to the arrest of an "arson suspect." But Citizen broadcast the name and image of an innocent man. It took 15 hours to remove the bounty on the innocent, unhoused individual. Citizen and other neighborhood surveillance apps routinely set the stage for vigilantism by showing users eager for confrontation where they can find people branded as "suspects" or "suspicious." Apps' failure to control racial profiling only increases the deadly threat of racialized vigilantism to BIPOC communities. Unfortunately, building platforms on a foundation of fear isn't only dangerous, it's also profitable. In July 2021, Citizen started peddling private security services to its scared users.

_

⁵¹ Lynne Peeples, "What the Data Say about Police Brutality and Racial Bias — and Which Reforms Might Work," *Nature* 583, no. 7814 (June 19, 2020): 22–24, https://doi.org/10.1038/d41586-020-01846-z.

⁵² Wesley Lowery, "A Disproportionate Number of Black Victims in Fatal Traffic Stops," *Washington Post*, December 24, 2015, sec. National, https://www.washingtonpost.com/national/a-disproportionate-number-of-black-victims-in-fatal-traffic-stops/2015/12/24/c29717e2-a344-11e5-9c4e-be37f66848bb story.html.

⁵³ Peeples, "Police Brutality Racial Bias."

⁵⁴ "Policing and Racial Injustice: A Disability Rights Perspective" (Disability Rights Ohio, November 10, 2020), https://www.disabilityrightsohio.org/assets/documents/policing--racial-injustices-a-disability-rights-perspective 11.10.2020 new format.pdf.

perspective 11.10.2020 new format.pdf.

55 Victoria A. Brownworth, "Police Violence Is LGBTQ History, Past and Present," Philadelphia Gay News, April 14, 2021, https://epgn.com/2021/04/14/police-violence-is-lgbtq-history-past-and-present/.

⁵⁶ Disability Rights Ohio, "Policing and Racial Injustice."

⁵⁷ Matthew Guariglia and Dave Maass, "LAPD Requested Ring Footage of Black Lives Matter Protests," Electronic Frontier Foundation, February 16, 2021, https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests.

⁵⁸ Wallace, "NYC Crime-Fighting App."

⁵⁹ Gross, "Falsely Accused by Citizen."

⁶⁰ Gross, "Falsely Accused by Citizen."

⁶¹ Sara Morrison, "Citizen, the Controversial Safety App, Is Ready to Profit from Its Fear-Based Platform," Vox, August 3, 2021, https://www.vox.com/recode/2021/8/3/22605791/citizen-protect-safety-app.

Civilian "Spies" Expand Police Power and Boost Big Tech Profits

Neighborhood surveillance app users volunteer their spying labor to the police for free, expanding police surveillance to places it couldn't otherwise go. ⁶² Apps, for their part, make it easy for police to access this free civilian labor. Neighbors invites government employees to the Neighbors Public Safety Service, a dedicated interface for requesting users' video footage. ⁶³ Until recently, police could directly request footage from customers within a specified half square mile. Nextdoor until recently allowed individuals to forward posts directly to their local police precinct, ⁶⁴ which police could access on Nextdoor for Public Agencies. ⁶⁵

These interfaces are designed primarily to expand police surveillance. In concession to civil rights activists, apps have made changes around the margins: for example, police now post public "Requests for Assistance" on Neighbors that appear in users' feeds, not their inboxes. 66 Requests for Assistance must "reference an active investigation with a valid agency reference number." But Ring's privacy policy spells out broads exceptions to this rule, including that a user's videos will be turned over "if disclosure is required by law, such as to comply with a warrant," or "to prevent physical or other harm or financial loss," or when "in connection with an investigation of suspected or actual illegal activity." The result of these broad exceptions is that police access to Neighbors users' videos has not been constrained by this change in a meaningful way.

Civilian surveillance adds up to serious business. Behind apps' extraordinary partnerships between police and civilians are carefully cultivated business partnerships between police and app companies. Nextdoor's advertising revenue is directly linked to the size of its user base, ⁶⁹ and police are the company's best marketing tool. As one Nextdoor executive put it, the main "strategy we used when we first launched in the U.S. [was to] recruit the major Police Departments and have them help us grow membership and engagement quickly." Nextdoor also goes beyond police partnerships, courting quasigovernmental agencies such as the National Sheriff's Association, the country's original Neighborhood Watch organization. ⁷¹

7

⁶² Alfred Ng, "Amazon's Helping Police Build a Surveillance Network with Ring Doorbells," CNET, June 5, 2019, https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/.

⁶³ "How Public Safety Agencies Use Neighbors," Ring, https://support.ring.com/hc/en-us/articles/360031595491-How-Public-Safety-Agencies-Use-Neighbors.

⁶⁴ Allyson Waller, "Nextdoor Removes App's 'Forward to Police' Feature," New York Times, June 23, 2020, https://www.nytimes.com/2020/06/23/us/nextdoor-forward-to-police-.html.

⁶⁵ Nextdoor Help Center, "What is the Nextdoor for Public Agencies Program?," accessed August 9, 2021, https://help.nextdoor.com/s/article/what-is-the-nextdoor-for-public-agencies-program?language=en US.

⁶⁶ Matthew Guariglia, "Ring Changed How Police Request Door Camera Footage: What it Means and Doesn't Mean," Electronic Frontier Foundation, June 7, 2021, https://www.eff.org/deeplinks/2021/06/ring-changed-how-police-request-door-camera-footage-what-it-means-and-doesnt-mean.

⁶⁷ Rachel Cericola, "Ring Neighbors is the Best and Worst Neighborhood Watch App," New York Times Wirecutter, June 3, 2021, https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/.

⁶⁸ Cericola, "Ring Neighbors is the Best and Worst Neighborhood Watch App."

⁶⁹ Nextdoor Help Center, "How Does Nextdoor Make Money?," accessed August 9, 2021, https://help.nextdoor.com/s/article/how-does-nextdoor-make-money?language=en_US.

⁷⁰ Sarah Holder, "How Nextdoor Courts Police and Public Officials," Bloomberg CityLab, May 21, 2020, https://www.bloomberg.com/news/articles/2020-05-21/nextdoor-s-delicate-partnership-with-local-police.

⁷¹ National Neighborhood Watch, last visited July 31, 2021, https://nnw.org/nextdoor.

Ring has cultivated close partnerships with 1,800 US police departments through its Neighbors app. 72 Like Nextdoor, Neighbors generates revenue from advertising partners and relies on police for marketing.⁷³ But Neighbors also supports the market for Ring devices and for its parent company Amazon's police services. Until recently, that suite of services included facial recognition tools. Amazon also has explored expanded surveillance services, filing a patent in 2018 to create a "database of suspicious persons" using facial recognition on individuals flagged by Ring users.⁷⁴ Public backlash forced Amazon to largely pause its plan to sell facial recognition to police agencies, 75 but the company still does ample business with police agencies providing more mundane services such as web hosting. 76 At the federal level alone, a 2020 inquiry revealed 447 contracts between Amazon or its major intermediaries and law enforcement and military agencies. 77 Close partnerships with local police departments established around Ring/Neighbors support Amazon's broader business relationships with law enforcement agencies across the nation.

Privacy Concerns

Facebook's recent entry into the neighborhood surveillance app market highlights another serious problem with neighborhood surveillance apps: the potential for misuse of surveillance data by companies themselves. Consider the sensitive nature of the data stored by neighborhood surveillance apps. Users post images and video footage of individuals to apps, from which sensitive biometric information—voice prints, face measurements, retina scans—can be extracted. Apps collect sensitive data about app users, as well: where they live, their current locations, their various preferences.

Beyond the threats of how tech companies will misuse and monetize the data, there are open questions about who else will gain access. Bad actors could easily weaponize this data where they find a weakness, and there's no shortage of weaknesses. One Neighbors security flaw allowed journalists to map the probable "locations of up to tens of thousands of Ring cameras." Another Neighbors security flaw made the exact locations and home addresses of users who posted to the app available.⁷⁹ Nextdoor has a real name policy: were it to experience this kind of hack, it would reveal users' actual names along with their addresses. The Citizen app was hacked by an activist

⁷² 1,800 U.S. police departments partner with Ring as of May 2021, an increase of roughly 500 precincts over the past year. Audrey Conklin, "1 in 10 Police Departments Can Now Access Videos from Millions of Consumers' Ring Security Cameras," Fox Business, May 19, 2021, https://www.foxbusiness.com/technology/1-in-10-police-departments-amazon-ring, and Jason Kelley and Matthew Guariglia, "Amazon Must End its Dangerous Partnership with the Police," Electronic Frontier Foundation, June 10, 2020, https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police.

⁷³ Jeramy Johnson, "How to Use the Ring Control Center to Opt Out of Third-Party Ads and Services," Android Central, February 25, 2020, https://www.androidcentral.com/how-use-ring-control-center-opt-out-third-party-ads-and-services. ⁷⁴ Matt McFarland, "Amazon May Want to Identify Burglars with Facial Recognition Tech," CNN Business, November 30,

^{2018,} https://www.cnn.com/2018/11/30/tech/amazon-patent-doorbell-facial-recognition/index.html. ⁷⁵ Karen Weise, "Amazon Indefinitely Extends a Moratorium on the Police Use of its Facial Recognition Software," New York Times, May 18, 2021, https://www.nytimes.com/2021/05/18/business/amazon-police-facial-recognition.html.

⁷⁶ Kari Paul, "Amazon Says 'Black Lives Matter.' But the Company Has Deep Ties to Policing," Guardian, June 9, 2020,

https://www.theguardian.com/technology/2020/jun/09/amazon-black-lives-matter-police-ring-jeff-bezos.

77 Jack Poulson, "Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated," Tech Inquiry, July 8, 2020, https://techinquiry.org/SiliconValley-Military/.

⁷⁸ Dell Cameron and Dhruv Mehrotra, "Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network," Gizmodo, December 9, 2019, https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279. ⁷⁹ Zach Whittaker, "Amazon's Ring Neighbors App Exposed Users' Precise Locations and Home Addresses," TechCrunch, January 14, 2021, https://techcrunch.com/2021/01/14/ring-neighbors-exposed-locations-addresses/.

hacker in May 2021.80 When Citizen launched a COVID-19 contact tracing app, it collected more personal data than necessary (e.g., copies of government IDs)⁸¹ and then revealed specific users' health data on the internet for anyone to see. 82

Neighbors' users are at additional risk of device hacking. In 2020, a group of Ring owners filed a class action lawsuit against Amazon after being harassed by hackers due to Ring's inadequate device security. 83 Hacks of Ring devices can allow total strangers to see into the interior of a home, into intimate and private of spaces like bedrooms and bathrooms, exposing customers to the very types of crimes they feared when purchasing Ring technology. While Ring added end-to-end encryption in early 2021 (primarily to stop police access to video without permission or a warrant), Amazon does not automatically grant this additional security to customers, requiring them to turn on encryption themselves rather than making it the default.⁸⁴

While the crime-related fear these apps spread is overblown, fear of their privacy impact is quite justified. None of these firms have shown that they deserve to be stewards of our most intimate moments. Amazon is "disturbingly quiet, evasive and reluctant to act" on privacy issues regarding its data sharing practices. 85 Facebook, a newcomer to the neighborhood surveillance app arena, is famous for its repeated privacy violations 86 and its willingness to monetize users' data. 87 Both Neighbors and Nextdoor have expressed astonishing disrespect for the privacy and reputations of people featured in ads featuring images and videos from user posts. 88 Neighbors insists that users agree to share their posts as part of accessing the app, but the targets of surveillance are never asked before their likenesses are broadcast and their reputations and safety are endangered.

IV. **Legal Remedies**

Neighborhood surveillance app companies are powerful. Neighbors by Ring and Facebook's Neighborhoods have the financial backing of global tech giants. Nextdoor and Neighbors have wellestablished relationships with police precincts nationwide. But there are avenues for restraining the worst abuses that these apps enable.

⁸⁰ Joseph Cox, "Hacktivist Posts Massive Scrape of Crime App Citizen to Dark Web," Vice, May 26, 2021, https://www.vice.com/en/article/pkbg89/hacker-hacktivist-citizen-app-scrape-dark-web.

⁸¹ Ryan Johnston, "LA's Use of Citizen for Contact Tracing Has Some Privacy Advocates Worried," September 10, 2020, StateScoop, https://statescoop.com/los-angeles-contact-tracing-citizen/.

⁸² Joseph Cox, "Crime App Citizen Exposed Users' COVID Data," Vice, May 24, 2021, https://www.vice.com/en/article/qj8kwg/citizen-safepass-privacy-covid-data-exposed.

⁸³ Neil Vigdor, "Somebody's Watching: Hackers Breach Ring Home Security Cameras," New York Times, December 15, 2019, https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html.

⁸⁴ Matthew Guariglia, Erica Portnoy, and Bill Budington, "Amazon Ring's End-to-End Encryption: What It Means," Electronic Frontier Foundation, February 2, 2021, https://www.eff.org/deeplinks/2021/02/amazon-rings-end-end-encryption-what-it-means. 85 Garfield Benjamin, "Hey, Alexa! Who Will You Share My Data With?," National Interest Blog, February 25, 2020, https://nationalinterest.org/blog/buzz/hey-alexa-who-will-you-share-my-data-126822.

86 Madrigal, "Facebook Didn't Sell."

⁸⁷ Johnston, "How Facebook Makes Money."

⁸⁸ Davey Alba and Ryan Mac, "Ring Is Using Its Customers' Doorbell Camera Video for Ads. It Says It's Allowed To.," BuzzFeed News, June 7, 2019, https://www.buzzfeednews.com/article/daveyalba/amazon-ring-doorbell-company-using-securityfootage-for-ads.

Biometric Privacy Laws

Illinois's groundbreaking Biometric Information Privacy Law (BIPA) and analogues in states such as Washington, Texas, Arkansas, and California require companies to obtain individuals' consent before collecting, using, or sharing their biometric data—measurements, unique to a person, that include their face geometry and voice print. 89 BIPA and laws like it cannot prevent Neighbors, Nextdoor, and other neighborhood surveillance apps from hosting video or photographs of individuals. They do forbid companies from extracting biometric data from that media without notifying individuals and obtaining their consent. This may prevent neighborhood surveillance apps from adding facial recognition and related police tech to their platforms—at least in Illinois and states with similar laws. For example, a class action lawsuit filed against Ring in August 2020 alleges that the company violated BIPA when it analyzed video from Ring cameras to collect and use "the biometrics of millions of unwitting individuals whose faces appear in video footage captured by Ring cameras and stored by Ring"—which is to say, all of the people who walked up to a Ring doorbell, perhaps to greet a neighbor or deliver the mail, and were not aware that their facial measurements would be taken.

Personality Rights

The right of publicity gives a person the right to control how their "name, likeness, or other recognizable aspects" are used in advertising and other commercial settings. 90 Rights of publicity protect people from their likenesses being sold or used for commercial purposes without their consent. Although the strength of protections varies by state, it is possible that individuals could push against Nextdoor's bizarre practice of sending letters promoting Nextdoor from a Nextdoor user to their neighbors without the user's knowledge or consent. 91 Neighbors' marketing strategy of using app users' footage of "crimes" may also violate the personality rights of the subjects of such footage. Often, Amazon asks owners for permission to use their footage so that they can also collect testimonials about the product. But as the previously mentioned suit against Ring alleges, there is no indication that Amazon makes any effort to communicate with the subjects of Ring footage before obtaining their biometric data—or before using their image to promote surveillance products. Neighbors now blurs subjects' faces in crime-related posts on its social media and website, but many posts and advertisements unrelated to crime do not obscure subjects' faces.

Consumer Privacy Laws

Other state laws address consumer privacy through their general applicability to personal consumer data instead of specifically limiting right of actions to biometric information. Laws such as California's Consumer Communications Privacy Act or state Unfair Commerce or Unfair and Deceitful Acts and Practices laws ("UCL" or "UDAP" laws) have already been used to bring lawsuits against these companies, including Ring, for not keeping consumer data secure, for data

⁸⁹ Caroline Haskins, "Revealed: The Secret Scripts Amazon Gives to Cops to Promote Ring Surveillance Cameras," Vice, August 6, 2019, https://www.vice.com/en/article/wjwea4/revealed-the-secret-scripts-amazon-give-to-cops-to-promote-ring-surveillance-

cameras.

90 "Publicity," Cornell Law School Legal Information Institute, https://www.law.cornell.edu/wex/publicity.

90 "Publicity," Cornell Law School Legal Information Institute, https://www.law.cornell.edu/wex/publicity.

90 "Publicity," Cornell Law School Legal Information Institute, https://www.law.cornell.edu/wex/publicity.

90 "Publicity," Cornell Law School Legal Information Institute, https://www.law.cornell.edu/wex/publicity. ⁹¹ Boris, "Warning: Social Media Site Sends Letters to Your Neighbors Signed by You," WPDH, June 10, 2021, https://wpdh.com/warning-social-media-site-sends-letters-to-your-neighbors-signed-by-you/.

breaches, and for selling data to third parties. 92 Nextdoor may also be liable, as it also uses third-party trackers.

Legal Liability for App Content

Neighborhood surveillance apps routinely publish content that accuses individuals of criminality—posts that can be defamatory when they are false and injure individuals' livelihoods or lead to harassment or shunning. But are apps ever legally responsible for these patterns of discrimination and defamation? Under Section 230 of the Communications Decency Act, a company becomes liable as a publisher only when it produces content. ⁹³ Insofar as Nextdoor or Neighbors by Ring simply host and moderate users' posts, the companies are not liable for that content under Section 230, except for certain extreme content. But Citizen generates some of its content. Indeed, it sometimes generates extraordinarily dangerous, defamatory content: its own posts purposefully started a manhunt for an innocent individual. And Citizen recently began hiring employees to record and post videos while posing as ordinary users. Therefore, it is likely that, at a minimum, Citizen could be sued by those it defames.

Conclusion

For far too long, the Neighborhood Surveillance Apps that watch our homes, communities, and neighbors have gone unnoticed by lawmakers. Even as these apps put our communities at risk and put every aspect of our lives under the microscope, their own marketing claims and practices have escaped scrutiny. That needs to change. Before we allow these apps to continue to endanger our communities, we need a real reckoning, confronting the cost of how these systems fail, and combatting the racism and bigotry they enable. Until we act, every new app download will undermine the very thing it's supposed to protect: community safety.

⁻

 ⁹² Spencer Soper and Ben Brody, "Amazon Probed by U.S. Antitrust Officials Over Marketplace," Bloomberg, September 11, 2019, xhttps://www.bloomberg.com/news/articles/2019-09-11/amazon-antitrust-probe-ftc-investigators-interview-merchants.
 ⁹³ Theodore F. Claypoole, "The Churl Nextdoor," National Law Review, April 29, 2021, https://www.natlawreview.com/article/churl-nextdoor.

SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT, INC.

40 RECTOR STREET
9TH FLOOR
NEW YORK, NY 10006
www.STOPSpying.org

