NOTE

SURVEILLANCE BY AMAZON: THE WARRANT REQUIREMENT, TECH EXCEPTIONALISM, & RING SECURITY

Justine Morris[*]

INTRODUCTION

"Smart" video doorbell cameras have been available to consumers for several years. Options include Nest (now owned by Google), Ring (formerly DoorBot,

[*] B.A. 2017, New York University; J.D. Candidate 2021, Boston University School of Law. My endless thanks go to everyone who provided guidance and feedback on this note, especially Professor Tracey Maclin, whose thoughtful critiques were indispensable. I would also like to thank the journalists whose information requests shed light on these partnerships, without which we would be unable to discuss the appropriate level of oversight for this technology. Finally, my effusive thanks to the editors at JOSTL for their time, energy, and edits.

and now owned by Amazon), and innumerable other, smaller manufacturers. Ring has come under particular scrutiny for its secretive partnerships with police departments, thanks to reporters at CNET, Motherboard, and The Intercept, among others.

Following the first reports, privacy groups began to raise concerns about Ring and the partnerships.[1] Ring has since made some changes to address these concerns, but the partnerships remain in place.[2] While this note will look at police-Ring partnerships through a Fourth Amendment lens, the Fourth Amendment is an imperfect tool for regulating the surveillance techniques of law enforcement, primarily because litigation must be retroactive and is often slow. The Fourth Amendment is nonetheless a useful measuring stick by which we can examine police departments' adoption and use of new technology.

Part I details the Amazon products at issue: The Ring cameras and the Neighbors application. Part II turns to the ways in which law enforcement can obtain Ring footage—the Stored Communications Act, the Neighbors app, and "geofences" on the law enforcement portal to Neighbors. Part III examines the historical foundations of the warrant requirement. Part IV details the relevant exceptions to the warrant requirement and the cases that established exceptions to the exceptions. Finally, Part V applies this interpretation of the exception-to-the-exception cases to argue that the collection of Ring footage should be subjected to strong Fourth Amendment protections because of how law enforcement interacts with the cameras and the footage they collect, and what that footage contains.

I. RING DOORBELLS AND THE NEIGHBORS APP

To understand how the Fourth Amendment is violated in this circumstance, I must begin by explaining what the cameras have the potential to capture, as well as the attendant privacy concerns.[3] I will then briefly explain the functionalities of the Neighbors Application.

---

[1] Press Release, Fight for the Future, et al., Open Letter Calling on Elected Officials to Stop Amazon's Doorbell Surveillance Partnerships With Police (Oct. 7, 2019), https://www.fightforthefuture.org/news/2019-10-07-open-letter-calling-on-elected-officials-to-stop/ [https://perma.cc/V3NK-MARD]; *see* Sarah Perez, *Over 30 Civil Rights Groups Demand an End to Amazon Ring's Police Partnerships*, TECHCRUNCH (Oct. 8, 2019), https://techcrunch.com/2019/10/08/over-30-civil-rights-groups-demand-an-end-to-amazon-rings-police-partnerships/ [https://perma.cc/F2RW-6KAX].

[2] Michael Finch II, *California Police, Amazon Ring Partnerships Raise Concerns*, GOVERNMENT TECHNOLOGY (Oct. 13, 2020 2:20 PM), https://www.govtech.com/public-safety/California-Police-Amazon-Ring-Partnerships-Raise-Concerns.html [https://perma.cc/RV64-6FCD].

[3] One of the difficulties of the Fourth Amendment in the modern context is that there are two questions embedded: the what was taken, and the how it was taken. In this subset of cases, the focus has been on the how and the potential for what could be taken *See* Kyllo v. United States, 533 U.S. 27, 35-38 (2001); *see also* DAVID GRAY, THE FOURTH AMENDMENT IN AGE OF SURVEILLANCE 82-83 (2017).

A. Ring Security Doorbell Cameras: What They Do & Privacy Implications

In February 2018, Amazon acquired Ring,[4] a start-up selling smart doorbells. Generally, smart doorbells are enabled with video and sound recording devices that are triggered by motion. Owners of smart doorbells are then alerted through an app on their phone that the motion sensor at their door was triggered.

Amazon promptly began marketing Ring doorbells as a way to prevent package thieves and help homeowners let cleaners and other domestic aides into the home.[5] Since its acquisition, Ring has become a key component of Amazon's smart home and Internet of Things line-up. The most well-known device in this lineup is Echo, more commonly called Alexa, a virtual assistant.[6] Over 2019 and 2020, the Ring product line expanded to include not just the doorbell camera but interior cameras, exterior and interior lights, as well as a "smart" front gate.[7]

The Ring video doorbell itself comes in a variety of models.[8] All capture the entryway of the home, and can be triggered by motion up to thirty feet from the

[4] Brad Stone, *Here's Why Amazon Bought a Doorbell Company*, BLOOMBERG (Mar. 5, 2018), https://www.bloomberg.com/news/articles/2018-03-05/here-s-why-amazon-bought-a-doorbell-company [https://perma.cc/MR6J-6YJ3].

[5] Interview by Emily Chang with Alex Barinka, IPO and Deals Reporter, Bloomberg, in Bloomberg.com (Feb. 27, 2018). Frankly, the anxiety of package thieves can be attributed in no small part to Amazon. In December 2018, searches for "porch pirate" had quintupled up from the previous year's search, whereas total online retail had grown only 15%. Fareeha Ali, *U.S. Commerce Sales Grow 15.0% in 2018*, DIGITAL COMMERCE 360 (March 13, 2019), https://www.digitalcommerce360.com/article/us-ecommerce-sales/ [https://perma.cc/2QPT-WM8G].

[6] *See* Britta O'Boyle, *What is Alexa and What Can Amazon Echo Do?*, POCKET-LINT (Jun. 14, 2019), https://www.pocket-lint.com/smart-home/news/amazon/138846-what-is-alexa-how-does-it-work-and-what-can-amazons-alexa-do [https://perma.cc/7AHL-Z3GX]. Alexa has to listen constantly for its own name and has problems of waking up when it should not, as well as sending those non-activating conversations back to Amazon, where actual people listen in for quality control. Makena Kelly & Nick Statt, *Amazon confirms it holds on to Alexa data even if you delete audio files*, THE VERGE (Jul. 3, 2019), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy [https://perma.cc/NC5B-N649]; *see also* Elizabeth Weise, *6 Ways to Keep Alexa from Eavesdropping*, USA TODAY (May 25, 2018), https://www.usatoday.com/story/tech/talking-tech/2018/05/25/6-ways-keep-alexa-eavesdropping-you/645504002/ [https://perma.cc/G6CM-TX5S].

[7] Ring, *CES 2020: Ring Unveils New Devices and Gives a Sneak Preview of What's to Come this Year*, RING (Jan. 6, 2020), https://blog.ring.com/2020/01/06/ces-2020-ring-unveils-new-devices-and-gives-sneak-preview-of-what-is-to-come-this-year/ [https://perma.cc/WB4V-26U2].

[8] *Smart Doorbell Camera*, RING, https://shop.ring.com/pages/doorbell-cameras?medium=tsa&gclid=EAIaIQobChMIn7nKuqrM5QIVvoVaBR2GXAVWEAAYAiAAEgLUyfD_BwE&gclsrc=aw.ds [https://perma.cc/K3Z5-JXLC]; *see* Tyler Lacoma, *Ring Video Doorbell Buying Guide: Which is Best for You?*, DIGITAL TRENDS (Oct. 29, 2018), https://www.digitaltrends.com/home/ring-video-doorbell-buying-guide/ [https://perma.cc/8SXA-8NYX]. At least one doorbell model, the peephole camera, allows

camera's position.[9] Depending on the density of a neighborhood, this might include a passerby on a sidewalk or cars on the street.[10] After installing Ring, a homeowner can limit the "motion zones," which trigger the camera—and push alerts—only when motion occurs in specified areas, such as the front walkway or part of the yard.[11] How frequently users actually set up those limits is unknown.[12]

Another technical limit on Ring footage is the user's ability to store footage, which depends on how much additional money the user has paid to Ring. If the user has paid for at least the Basic Ring Protect Plan,[13] then they can access the footage within the Amazon cloud for up to sixty days.[14] To have access to footage beyond that, the user has to download it to their own computers.[15] If the owner of the camera does not have a Ring Protect Plan, then they can purportedly only view footage live.[16] It is unclear whether Ring stores the footage and

for particular areas to be blocked out via "privacy zones." How much this actually protects privacy is unclear, given all the context one could see of the area around the privacy zone. *Understanding Privacy Zones*, RING, https://support.ring.com/hc/en-us/articles/360027979331-Understanding-Privacy-Zones [https://perma.cc/P9F9-PYWP].

[9] *Motion Detection in Powered Ring Devices*, RING: SUPPORT CENTER, https://support.ring.com/hc/en-us/articles/360022461232-Motion-Detection-in-Powered-Ring-Devices [https://perma.cc/7E2Y-QFJ4]

[10] *See* Louise Matsakis, *The Ringification of Suburban Life*, WIRED (Sep. 26, 2019), https://www.wired.com/story/ring-surveillance-suburbs/ [https://perma.cc/65HZ-QW9K].

[11] *Utilizing Motion Zones with Your Powered Ring Devices*, RING: SUPPORT CENTER, https://support.ring.com/hc/en-us/articles/360021842611-Utilizing-Motion-Zones-With-Your-Powered-Ring-Devices [https://perma.cc/VY2C-GCEC].

[12] *See Understanding and Optimizing Motion Detection with Motion Frequency*, RING: SUPPORT CENTER, https://support.ring.com/hc/en-us/articles/115003477106-Understanding-and-Optimizing-Motion-Detection-with-Motion-Frequency [https://perma.cc/Y55A-C5SF] (It is in the user's interest to limit these zones, because a larger motion zone means more notifications to the user's smart phone).

[13] *Protect Plans*, RING, https://shop.ring.com/pages/protect-plans [https://perma.cc/9JYU-CD4W] (The Basic Plan costs three dollars a month, or thirty dollars annually. The Plus Plan costs ten dollars a month, or one hundred dollars annually. Basic and Plus both store video history for sixty days, allow video sharing, and the camera takes "snapshots" throughout the day—still images taken between motion-capture events. With the Plus Plan, the user receives 24/7 professional monitoring, an extended warranty on all Ring devices, and a ten percent discount on select products at Ring.com. All users, even those who have not paid for an additional plan, receive motion-activated notifications, real-time video feeds, and two-way talk. Two-way talk is the most-touted feature—it's what is used in those seductive videos of homeowners scaring off would-be burglars); *see* Inside Edition, *Homeowners Scare Off Would-Be Burglars Through Security Cameras*, YOUTUBE (Nov. 6, 2018), https://www.youtube.com/watch?v=-AcV1Qf8GsU [https://perma.cc/6F3P-KC2R].

[14] *Protect Plans*, *supra* note 13.

[15] *Id.*

[16] *Id.* If an individual does not have a Protect Plan, it is unclear if they can receive a footage request, and if they do, whether their Ring has captured footage they can share, or if they can

simply does not provide the user access to it without them buying a Protect Plan. If that is the case, then law enforcement may have access to footage even where a user does not. Furthermore, there are no available numbers on what percentage of Ring owners have a Protect Plan.

Many people still like smart doorbells and continue to purchase them. Even in the face of at least one technology publication withdrawing their recommendation,[17] sales have continued to climb.[18] People like them because they think that crime is rising[19] and they say it helps them feel safer in their homes and in their neighborhood.[20] At the very least, people always know when someone is on their front porch.

---

review it. *See* Letter from Brian Huseman, Vice President of Pub. Policy, Amazon, to Senator Ed Markey, Cong. Senate Rep. Mass. (Sept. 26, 2019) [hereinafter "First letter from Amazon to Sen. Markey"], https://www.markey.senate.gov/imo/media/doc/Response%20Letter_Ring_Senator%20Markey%209.26.19.pdf [https://perma.cc/U5JC-36VV].

[17] *See* After several hacks were made public, Wirecutter withdrew its recommendation of Ring products. Wirecutter (@wirecutter), TWITTER (Dec. 19, 2019, 10:34 AM), https://twitter.com/wirecutter/status/1207730874860609536 [https://perma.cc/W6GY-ZN4N] (After several hacks were made public, Wirecutter withdrew its recommendation of Ring products); *see also* Will Oremus, *Wirecutter No Longer Recommend Ring Doorbells, and It's About Time*, ONEZERO (Dec. 19, 2019), https://onezero.medium.com/wirecutter-no-longer-recommends-ring-doorbells-and-its-about-time-952d93062ea2 [https://perma.cc/C39T-PVJT].

[18] Ring has not released any sales numbers but does frequently allude to "millions" of customers. Jumpshot, a data analytics firm, estimates there were 400,000 sales in December 2019 alone, up 180 percent from the previous December. Rani Molla, *Amazon Ring Sales Nearly Tripled in December Despite Hacks*, VOX (Jan. 21, 2020), https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data [https://perma.cc/QL3K-9DRE].

[19] *See, e.g.*, John Gramlich, *5 Facts About Crime in the U.S.*, PEW RESEARCH CENTER (Oct. 17, 2019), https://www.pewresearch.org/fact-tank/2019/10/17/facts-about-crime-in-the-u-s/ [https://perma.cc/C3WV-NUZZ] (noting crime rates have fallen and "public perception about crime in the U.S. often doesn't align with the data"); Gary Lafree, Opinion, *American Attitudes are Disconnected From Reality on Crime Trends*, THE HILL (Jan. 31, 2018), https://thehill.com/opinion/criminal-justice/371287-american-attitudes-are-disconnected-from-reality-on-crime-trends [https://perma.cc/VKG3-GV4R].

[20] *See* Caroline Haskins, *How Ring Transmits Fear to American Suburbs*, MOTHERBOARD (Dec. 6, 2019), https://www.vice.com/en_us/article/ywaa57/how-ring-transmits-fear-to-american-suburbs [https://perma.cc/LX8E-EK8A]. While Ring claims in no uncertain terms that it makes neighborhoods safer, the evidence suggesting that is circumstantial at best. *See Mother Shaken After Seeing Would-be Burglar Scared Off by Her Ring Doorbell Camera*, NBC2 (Nov. 26, 2019, 6:11 PM), https://nbc-2.com/nbc-2-wbbh/2019/11/26/mother-shaken-after-seeing-would-be-burglar-scared-off-by-her-ring-doorbell-camera/ [https://perma.cc/H92C-MK8K] ("The insurgence of Ring doorbells and other home security systems…continue helping homeowners feel at ease"). *But see* Mark Harris, *Video Doorbell Firm Ring Says its Devices Slash Crime—But the Evidence Looks Flimsy*, MIT TECHNOLOGY REVIEW (Oct. 19, 2018), https://www.technologyreview.com/s/612307/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/ [https://perma.cc/B4UU-HWHV].

However, even if Ring is only triggered by something in its immediate vicinity, the footage that it captures encompasses a far wider scope.[21] Though this is a natural consequence of any video surveillance system, the amount and often intimate nature of video footage collected alarms privacy advocates.[22] There is already at least one case where an individual was indicted partially on the basis of Ring footage.[23]

Even when the cameras are not being used for prosecution, regular people, not just privacy advocates, feel more than a little creeped out by the rising prevalence of doorbell cameras:

> "I've been worried about this," one UPS employee wrote on Reddit. "Those Ring cameras are everywhere now and going up to houses with packages already delivered I'm afraid they'll think I'm stealing them." On a U.S. Postal Service forum, a mail carrier asked: "Anyone else feel kind of creeped out that people are recording and watching you, up close, deliver mail to their house or is it just me?"[24]

For the owners, too, Ring reinforces a sense of paranoia.[25] In one clip, a user captured someone walking up the porch, and lingering for a short time: the homeowner shared the clip, tagging it "suspicious male" and warning their

---

[21] *See The Ring Doorbell Buyer's Guide*, RING: SUPPORT CENTER (last visited Oct. 2, 2020), https://support.ring.com/hc/en-us/articles/360035250032-The-Ring-Doorbell-Buyers-Guide [https://perma.cc/72BG-P4GN].

[22] *See, e.g.*, Matthew Guariglia, *Amazon's Ring Is a Perfect Storm of Privacy Threats*, ELECTRONIC FRONTIER FOUNDATION (Aug. 8, 2019), https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats [https://perma.cc/JSQ6-58P2]; Catherine Thorbecke, *Senator Blasts Amazon's Ring Doorbell as an 'Open Door for Privacy and Civil Liberty Violations'*, ABC NEWS (Nov. 20, 2019, 2:06 PM), https://abcnews.go.com/Business/senator-blasts-amazons-ring-doorbell-open-door-privacy/story?id=67162384 [https://perma.cc/6CMH-7TWU].

[23] *See* Lauren Smiley, *A Brutal Murder, A Wearable Witness, and an Unlikely Suspect*, WIRED (Sept. 26, 2019, 6:00 AM), https://www.wired.com/story/telltale-heart-fitbit-murder/ [https://perma.cc/SP99-VP6W] ("Footage from a Ring security camera kitty-corner from [the victim's] home, however, had captured images of a car in [the victim's] driveway like the [one the defendant] drove. The camera recorded only snippets of footage when triggered by movement, but the images showed the car parked at 3:12 pm, still there at 3:33, and then gone by the time the next image was taken at 3:35. The video never showed the driver.").

[24] John Herrman, *Who's Watching Your Porch?,* THE NEW YORK TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-security.html [https://perma.cc/N5XT-44G8].

[25] William Antonelli, *Neighborhood Security Apps Are Making Us Wildly Paranoid*, THE OUTLINE (Feb. 22, 2019, 10:00 AM), https://theoutline.com/post/7108/surveillance-startups-thrive-on-a-whole-new-level-of-paranoia?zd=1&zi=olveon5c [https://perma.cc/WL5F-4BEU] ("[I]t's impossible to feel protected when these apps are always shouting about how much potential danger we're in. Spending so much time focused on that danger just leads to anger, depression, burnout. In our quest for safety, we've found ways to become more paranoid.").

neighbors to be on the lookout.[26] In an unusual turn, the malingerer saw the post, and commented mortified; he had in fact, lived at that house many years prior and was simply taking a walk down memory lane.[27] After events like these, at least one police department has explicitly asked residents to send footage to them instead of posting it in order to prevent this sort of hysteria.[28]

Sometimes the doorbells capture objectively good acts, but even those interactions can still be invasive. For instance, one homeowner left snacks out for delivery drivers, and captured one of them doing a happy dance at finding the snacks.[29] The driver did not know he had been recorded until it went viral.[30] One video, titled "Neighbor Saves Woman from Freezing Temperatures," published by Ring TV,[31] features a woman shivering in a t-shirt, snow on the ground.[32] She tells the homeowner she lives across the street and is locked out of her home before asking the homeowner to call her husband.[33] But the Ring owner neither opens the door nor calls the husband—instead, the owner calls the police, leaving the woman on the stoop until officers arrive some minutes later.[34]

B. The Neighbors App: Just a Digital Neighborhood Watch?

The Neighbors application was launched as a stand-alone app by Ring in May of 2018.[35] It had previously been integrated into the Ring app, which was

---

[26] Spencer Buell, *Ring's Neighborhood Watch is Bringing out the Worst in Boston*, BOSTON MAGAZINE (Jan. 27, 2020, 1:32 PM), https://www.bostonmagazine.com/news/2020/01/27/ring-cameras-neighbors-app/ [https://perma.cc/T9Y7-4CXF].

[27] *Id.*

[28] *See* Christina Hall, *How Doorbell Cams are Creating Dilemmas for Police, Neighborhoods*, DETROIT FREE PRESS (Aug. 23, 2018, 6:00 AM), https://www.freep.com/story/news/local/michigan/2018/08/23/doorbell-camera-videos-ring-police/1000358002/ [https://perma.cc/64L5-HLUH].

[29] Sarah Kaufman, *'Happy Dance' Delivery Driver Shares Why Snacks Make Such a Big Difference*, TODAY (Dec. 20, 2019), https://www.today.com/food/happy-dance-delivery-driver-shares-why-snacks-make-such-big-t170409 [https://perma.cc/Z3NE-VJ6K].

[30] *Id.*

[31] Ring TV is the in-house publishing arm of Ring, where Ring collects and curates best of videos, largely as a form of marketing, and the clips frequently end up as part of the local news. Herrman, *supra* note 24.

[32] Mason Mauro, *Woman Escapes Arctic Threat Through Neighbor's Doorbell*, WOWT (Feb. 1, 2019), https://www.wowt.com/content/news/Woman-escapes-arctic-threat-through-neighbors-doorbell-505192331.html [https://perma.cc/9ESY-Q6LG].

[33] *Id.*

[34] *Id.*

[35] *See* 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/ [https://perma.cc/RKW7-BTFU].

available only to individuals who had the Ring doorbell camera,[36] and users could not opt-out of Neighbors app.[37]

Now, anyone can sign up for the app, but footage can only be posted on Neighbors from a Ring camera, and all of the footage is watermarked as being from a Ring camera.[38] Posting on the app is done anonymously—all user names appear as "neighbor" followed by a random, short string of numbers.[39] Despite these gestures at anonymity and security, a user can share any footage they wish—suspicious activity, drug use, animals in their yard, or good deeds.[40] As Caroline Haskins noted:

> Ring sells a very particular message: while you shouldn't trust your neighbors, you *should* trust Amazon to help police it. The Neighbors app is free. But the more unsafe the app makes you feel the more inclined you would feel to dole out money for a Ring home security system. Neighbors functions as a fear and peer pressure-driven advertisement for a fancy, Amazon-owned camera system. But in practice, Neighbors reinforces the racist biases of its users, and actively puts people of color at risk in communities where the app is being used.[41]

Much of that could be said about any of the other neighborhood watch apps, such as Nextdoor and Citizen.[42] Neighbors, however, is different because of the

---

[36] See *Id.*

[37] *Ring App – Neighbors – How do i disable?*, REDDIT (last visited Oct. 04, 2020), https://www.reddit.com/r/ringdoorbell/comments/7fp3m6/ring_app_neighbors_how_do_i_disable/ [https://perma.cc/7JKW-9YK3]. However, as Neighbors is now a stand-alone app, Ring owners can probably opt out of Neighbors. *See* Rachel Cericola, *Ring Neighbors Is The Best and Worst Neighborhood Watch App*, N.Y. TIMES (Feb. 14, 2020), https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/ [https://perma.cc/HA3R-KFGV]. This is in-line with newly added ability to preemptively opt out of police requests entirely. *See infra* note 60.

[38] *See* Cericola, *supra* note 37.

[39] "Nick," *Introducing the Neighbors App: The New Neighborhood Watch*, RING (May 8, 2018), https://blog.ring.com/2018/05/08/introducing-the-neighbors-app-the-new-neighborhood-watch/ [https://perma.cc/7FQR-XAGM]. Anonymous here only means that names, or even a more typical username, is not attached to the post. See *infra* note 57.

[40] Jay Peters, *Amazon's Ring Now Lets You Snitch on Your Neighbors Good Deeds, Too*, THE VERGE (Feb. 11, 2020, 8:00 AM), https://www.theverge.com/2020/2/11/21128727/amazon-ring-neighbors-app-neighborly-moments [https://perma.cc/Y7B4-NHU8].

[41] Caroline Haskins, *Amazon's Home Security Company is Turning Everyone Into Cops*, MOTHERBOARD (Feb. 7, 2019), https://www.vice.com/en_us/article/qvyvzd/amazons-home-security-compcany-is-turning-everyone-into-cops [https://perma.cc/RX49-V93E].

[42] *See* Makena Kelly, *Inside NextDoor's 'Karen Problem'*, THE VERGE (Jun. 8, 2020), https://www.theverge.com/21283993/nextdoor-app-racism-community-moderation-guidance-protests [https://perma.cc/XD62-SPW3] (examining the issues of race on Nextdoor, another neighborhood watch app); *see also* Sarah Lustbader, *Spotlight: Neighborhood Crime Apps Stoke Fears, Reinforce Racist Stereotypes, and Don't Prevent Crime*, THE APPEAL (Jun. 4, 2019), https://theappeal.org/spotlight-neighborhood-crime-apps-stoke-fears-reinforce-

many ways that law enforcement agencies can extract footage from Neighbors via the law enforcement portal.[43]

II. PATHWAYS FOR LAW ENFORCEMENT TO OBTAIN RING FOOTAGE

First, Ring partnerships with local law enforcement are not accidental, but instead long cultivated and desired by Ring. Since at least 2016, the CEO of Ring, Jamie Siminoff, has intended Ring as an investigatory tool for law enforcement.[44] The relationships between Ring and law enforcement started to formalize in March 2018, about a month after Amazon acquired Ring.[45] Since then, Ring has developed partnerships with over 1300 agencies, each of which has their own Neighbors profile and portal.[46]

racist-stereotypes-and-dont-prevent-crime/ [https://perma.cc/H89S-ZZ2N]; Campbell Robertson and John Schwartz, *Shooting Focuses Attention on a Program That Seeks to Avoid Guns*, N. Y. TIMES (Mar. 22, 2012), https://www.nytimes.com/2012/03/23/us/trayvon-martin-death-spotlights-neighborhood-watch-groups.html [https://perma.cc/M7F4-UHHF] (demonstrating an example to unconvinced readers about the real dangers of neighborhood watch groups and specifically considering the death of Trayvon Martin); s*ee generally* Rani Molla, *The Rise of Fear-Based Social Media like Nextdoor, Citizen, and Now Amazon's Neighbors*, VOX (May 7, 2019), https://www.vox.com/recode/2019/5/7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors [https://perma.cc/226Q-8YU7].

[43] *See infra* Part II.B, II.C; *see also* First letter from Amazon to Sen. Markey, *supra* note 16 (contract appended, noting that in partnership they get access to the portal); *see also* Elise Schmelzer, Two Colorado Police Departments Already Partner with a Popular Doorbell Camera Company — and More Are Considering, Denver Post (Sept. 24, 2019, 12:34 PM), https://www.denverpost.com/2019/09/22/ring-colorado-police-camera-surveillance/ [https://perma.cc/A3JQ-XVJF]. Notably, after the protests for George Floyd, Nextdoor has made it more difficult for police to obtain reports from the app. Kim Lyons, Nextdoor Eliminates Its Forward to Police Program, THE VERGE (June 20, 2020 5:38 PM), https://www.theverge.com/2020/6/20/21297876/nextdoor-forward-police-racism-messages [https://perma.cc/3VYR-AXEU].

[44] Sam Biddle, *Amazon's Home Surveillance Chief Declared War on "Dirtbag Criminals" as Company Got Closer to Police*, THE INTERCEPT (Feb. 14, 2019, 1:25 PM), https://theintercept.com/2019/02/14/amazon-ring-police-surveillance/ [https://perma.cc/77XQ-2YYB].

[45] Alfred Ng, *Ring Let Police View Map of Video Doorbell Installations for Over a Year*, CNET (Dec. 3, 2019, 5:00 AM), https://www.cnet.com/news/ring-gave-police-a-street-level-view-of-where-video-doorbells-were-for-over-a-year/ [https://perma.cc/D8FD-P8SP]. The Greenfield Police Department, in a suburb of Milwaukee, established the first partnership on March 22, 2018. Map of Neighbors Law Enforcement, GOOGLE MAPS, https://www.google.com/maps/d/viewer?mid=1eY-VDPh5itXq5acDT9b0BVeQwmESBa4cB&ll=38.2528703536363%2C-95.76605790204496&z=5 [https://perma.cc/2K6L-MYME].

[46] *Id.* Ring has been weekly updating this map, visually demonstrating where all the police departments are nationally that have adopted this tech. The map was originally posted in August 2019, and now includes the number of requests an agency sent for the most recent quarter. Jamie Siminoff, *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map*, RING (Aug. 28, 2019),

After partnering with Ring, police departments obtain access to a special portal designed for law enforcement and receive materials and other incentives, which the departments can distribute to encourage households within their jurisdictions to install Ring and join Neighbors.[47] In some cases, households can enter to win a free Ring by signing up for Neighbors and entering their local law enforcement's unique sign up code.[48] In Rancho Palos Verdes, California, law enforcement negotiated a subsidy with Ring, and the city committed to provide 2,000 $50 incentives for residents, in addition to the subsidy.[49]

There are two additional ways law enforcement can obtain Ring footage: by obtaining a warrant under the Stored Communications Act (SCA),[50] or by posting or commenting on the Neighbors application. For the purposes of this note, the former does not need further exploration because, as "content" the footage would require a warrant and therefore likely comports with the Fourth Amendment.[51] While the latter also probably accords with the Fourth Amendment, it is worth exploring in more detail in order to provide more context to the

https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/#comment-54636 [https://perma.cc/LDM3-3DT7]. Most of these partnerships were developed in secrecy. *See, e.g.*, Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, MOTHERBOARD (July 25, 2019, 11:54 AM), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement [https://perma.cc/CAG4-LB9X]. Unfortunately, it is all too common for police departments to adopt and buy surveillance technology without the citizenry knowing. See CYRUS FARIVAR, HABEAS DATA: PRIVACY VS. THE RISE OF SURVEILLANCE TECH 170-197 (2018) (discussing the secretive adoption of stingrays by law enforcement).

[47] Caroline Haskins, *Amazon is Coaching Cops on How to Obtain Surveillance Footage Without a Warrant*, MOTHERBOARD (Aug. 5, 2019, 1:08 PM), https://www.vice.com/en_us/article/43kga3/amazon-is-coaching-cops-on-how-to-obtain-surveillance-footage-without-a-warrant [https://perma.cc/H7L7-9D3N]; Louise Mataskis, *Cops Are Offering Ring Doorbells in Exchange for Info*, WIRED (Aug. 2, 2019), https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/ [https://perma.cc/7H4G-LVMF].

[48] Caroline Haskins, *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*, MOTHERBOARD (Aug. 2, 2019), https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money [https://perma.cc/N3P2-TM2G]; *see* Mataskis, *supra* note 47.

[49] Herrman, *supra* note 24.

[50] 18 U.S.C. §§ 2701 *et seq.* (2019); Andrew Sellars, *Data Generated by New Technologies and The Law, 2019 Edition,* MCLE: WHEN NEW TECHNOLOGIES BECOME EVIDENCE, July 2019 at 1.

[51] 18 U.S.C. § 2702(a)(3). It should be noted, however, that if law enforcement used the SCA to obtain "non-content" records from the Ring an individual homeowner might be able to mount a successful challenge under *Carpenter*. *See Carpenter*, 138 S. Ct. at 2220-2221 (holding that a law enforcement agent must have a warrant, and not just a subpoena pursuant to the SCA, in order to obtain non-content records that qualify as "real-time CSLI or 'tower dumps'").

relationship between Ring and law enforcement before discussing the details of the law enforcement portal.

A. Via Neighbors

A police department can either comment on the footage or post independently—much like on Facebook—and directly ask a user to share their footage.[52] While Ring does not directly assist officers in obtaining footage in this case, it does assist passively. For instance, the promotional materials that Ring sends to police departments suggest particular phraseologies police officers should use in their footage requests from homeowners.[53] These requests allow law enforcement agencies to bypass warrant processes by requesting information directly from homeowners. In emails between Ring and police departments, Ring also encourages police departments to regularly post on Neighbors because it increases the "opt-in rate"—i.e. how often homeowners turn their footage over to police voluntarily.[54]

According to Amazon and Ring, locations of users who share footage are anonymous within the app.[55] However, this appears to be largely untrue—at least one police chief was simply sending officers to the doors of those who had digitally declined to share.[56] Further, third-party researchers have been able to

[52] It is not clear whether a police department must have partnered with Ring to view the app, but I believe that is the case, based on the language in the contract. *See* First Letter from Amazon to Sen. Markey, *supra* note 16.

[53] Haskins, *supra* note 47; *see* Biddle, *supra* note 44.

[54] Haskins, supra note 47.

[55] *See* Cericola, *supra* note 37. It appears that after the revelations from Gizmodo, discussed *infra* note 57, Ring has removed the representations about the anonymity and security of posting. *See Neighbors by Ring*, RING.COM (last visited October 30, 2020) https://shop.ring.com/pages/neighbors [https://perma.cc/4QD4-W2F9]. In relevant part, the site reads as follows:

> Ring will continue to innovate on behalf of our customers to help make neighborhoods safer. We will do so with our customers, their privacy and the security of their information at the top of our priority list. We know that our customers place a huge amount of trust in us, and we have every intention of continuing to earn that trust.
>
> Users have full control of who views their Ring footage. Only the content that a user chooses to make publicly available on Neighbors (by posting it to the App) can be viewed via the Neighbors App or by local law enforcement. Users can choose to share text updates, photos and videos taken on any device, including but not limited to Ring's home security devices. Only content that a Neighbors user chooses to share on the Neighbors App is publicly accessible through the Neighbors App or by your local law enforcement. Ring does not view or share a user's videos that are not posted to the App without the user's express permission or a valid and binding legal demand properly served on us.
>
> We do not display personal information like names in the Neighbors App, and we do not share personal information with other users of the App.

[56] Alfred Ng, *Amazon's Helping Police Build a Surveillance Network with Ring Doorbells*, CNET (June 25, 2019, 7:55 AM), https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/ [https://perma.cc/JU4A-9AGV].

use the Neighbors app itself to identify poster locations down to inches.[57] Ring had also previously shared a "heat map" with partnered police departments, which showed the general location and density of Ring Cameras.[58]

Both this method and the warrant via the Stored Communications Act are not unusual methods of investigation. The SCA was enacted in 1986, and the public interaction on Neighbors is barely distinguishable from an old-fashioned tip-line. However, with the law enforcement portal, police departments have yet one more way to access the footage that is unique among neighborhood watch apps, even as the Fourth Amendment concerns it raises are not.

B. Via the Law Enforcement Portal

The law enforcement portal ("the portal") works like this: If police are investigating a crime independent of footage already posted, they can drag and create a box on a map—a "geofence"[59]—and the portal will then push a request for relevant footage to every Ring user[60] within that box. According to Ring, the minimum area for a request is .0025 square miles and the maximum is .5 square mile, and the max time is 12 hours.[61] There are no known technical limits on the number of requests a department could send over any time period. The "video request" is sent via email, and it prompts users to either "review and share" or "share without reviewing."[62] The email also allows the user the option to stop

[57] Dell Cameron & Dhruv Mehrota, *Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network*, GIZMODO (Dec. 9, 2019, 3:32 PM), https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279 [https://perma.cc/4A7F-VWDR].

[58] Colin Lecher, *Ring Reportedly Outed Camera Owners to Police with a Heat Map*, THE VERGE (Dec. 3, 2019, 3:05 PM), https://www.theverge.com/2019/12/3/20993814/ring-user-location-heat-map-police-privacy-tool-camera-owners [https://perma.cc/PB8W-3CCS].

[59] Ng, *supra* note 56.

[60] Ring now offers users the option to opt-out before they receive a request via the Ring app. Jason Cipriani, *Ring doorbell and police surveillance: There's a new way to opt out of video requests*, CNET (Feb. 4, 2020, 3:00 AM), https://www.cnet.com/how-to/ring-doorbell-and-police-surveillance-theres-a-new-way-to-opt-out-of-video-requests/ [https://perma.cc/3BQX-HUHA]; see Lauren Goode & Louise Matsakis, *Amazon Doubles Down on Ring Partnerships with Law Enforcement*, WIRED (Jan. 7, 2020, 8:02 PM), https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/ [https://perma.cc/7HJN-YDN5].

[61] Letter from Brian Huseman, Vice President of Pub. Policy, Amazon.com, Inc., to Senator Ed Markey, Cong. Senate Rep. Mass., (Nov. 1, 2019) [hereinafter "Second Letter from Amazon to Sen. Markey"], https://www.markey.senate.gov/imo/media/doc/Response%20Letter_Ring_Senator%20Markey%2011.01.2019.pdf [https://perma.cc/B9TZ-23AM].

[62] *See Requests for Video Recordings from Law Enforcement*, RING, https://support.ring.com/hc/en-us/articles/360023205151-Requests-for-Video-Recordings-from-Law-Enforcement [https://perma.cc/7T7A-4BCQ]; *see also* Second Letter from Amazon to Sen. Markey, *supra* note 61.

receiving future emails.[63] As it stands now, Ring users cannot opt-out of Neighbors entirely—by having a Ring camera they are automatically enrolled in the app, and there is no way to remove or hide the link to Neighbors in the Ring app.[64]

Thus, with very little effort, limited only by internal policies, law enforcement could receive massive amounts of footage. Furthermore, attempting to replicate the results without the portal would require substantially more work from an officer. The officer would first have to travel to the neighborhood he sought footage from and physically go door-to-door, checking for cameras and requesting footage. Of course, people might not be home, so the officer might have to come back later. Even if the police are granted access to the footage, the resident would have to transfer data to the officer by some process that would likely be more cumbersome than digitally requesting footage on Neighbors.

Neither scenario involving the Neighbors portal—nor their analog equivalents—requires a warrant because both would be understood by a court to fall under the "consent" exception to the Fourth Amendment's warrant requirement.[65] That is, obtaining video footage on Neighbors is not a violation of the Fourth Amendment because police officers have been given explicit, non-coerced consent to access and view the footage by someone who legally owns it.[66] This is an accurate conclusion where an individual voluntarily posts their footage to the app.[67] If the admissibility of Ring footage obtained via a video request was challenged on Fourth Amendment grounds, the state would almost certainly argue the officers are functionally going door-to-door and requesting footage, thereby falling within the consent exception, making this just a modern extension of that time-honored investigation technique.[68]

I disagree; the geofence is so different from that traditional technique that the warrant clause must be enforced when officers use that portal. As will be discussed in Part IV, the Supreme Court has already begun negating the traditional exceptions in some circumstances, which this geofence function falls neatly into.[69] However, the exceptions to the warrant requirement cannot be understood without first understanding the warrant requirement itself.

---

[63] *See* RING, *supra* note 62. The opt-out link at the bottom of an emailed video request is required to be CAN-SPAM compliant. *See* 15 U.S.C. § 7704 (2018).

[64] *See* Cericola, *supra* note 37.

[65] *See* discussion *infra* Part V.A.

[66] *See* discussion *infra* Part V.

[67] See Haskins, *supra* note 47. While one could draw a distinction that the police department is collecting footage, hard evidence, to be stored indefinitely (as far as we know) and not just the words of someone who saw something. This gets scarier when you consider the implementation of facial recognition. *See infra* note 161, and accompanying text.

[68] *See* discussion *infra* Section V.A.

[69] *See* discussion *infra* Part IV.

III. HISTORICAL FOUNDATIONS OF THE WARRANT REQUIREMENT

At its most fundamental level, the text of the Fourth Amendment forces us to ask two questions: was the law enforcement activity at issue a search and seizure, and was it reasonable? The importance of the second question has waxed and waned overtime, but it has nonetheless remained essential for understanding when police have overstepped their Constitutional boundaries. The plain text of the Fourth Amendment does not require warrants—it states only that the people have a right to be secure against unreasonable searches and seizures.[70] In a separate clause, the Fourth Amendment details that "no Warrants shall issue but upon probable cause,"[71] thus restricting law enforcement's access to warrants.[72] "The relationship between these two clauses of the Fourth Amendment" is a core issue in debates over the Court's warrant requirement doctrine:[73] one could read the clauses separately, and interpret the Fourth Amendment solely through what constitutes a "reasonable" law enforcement activity.[74] Another approach is to read the Fourth Amendment as demanding a warrant for all search and seizure activity—without a warrant, the activity is presumptively unreasonable and the government must prove that the activity was reasonable.[75]

The warrant requirement was first endorsed by the Supreme Court in 1925,[76] but an ambitious scholar could trace it as far back as the 1886 decision in *Boyd v. United States*.[77] In recent years, it has been resurgent: "the past decade of the Roberts Court has produced a series of Fourth Amendment decisions, ranging across a variety of subsidiary doctrinal areas, where the warrant requirement has made a comeback."[78] Most warrant requirement cases follow a similar pattern: aggressive police tactics pose a threat to the citizenry and the Court is concerned

---

[70] U.S. Const. amend. IV.

[71] *Id.*

[72] GRAY, *supra* note 3, at 190.

[73] Benjamin J. Priester, *A Warrant Requirement Resurgence? The Fourth Amendment in the Roberts Court*, 93 ST. JOHN'S L. REV. 89, 90-91 (2019).

[74] *E.g.*, Payton v. New York, 445 U.S. 573, 611 (1980) (White, J., dissenting); United States v. Rabinowitz, 339 U.S. 56, 60 (1950); *see* Priester, *supra* note 73, at 94-95.

[75] *E.g.*, Riley v. California, 573 U.S. 373, 398 (2014) (emphasizing the importance of categorical rules, such as the warrant requirement, in securing liberties); Berger v. New York, 388 U.S. 41, 53, 63-64 (1967); Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 201 (1993) ("The Constitutional lodestar for understanding the Fourth Amendment is not an ad hoc reasonableness standard; rather, the central meaning of the Fourth Amendment is distrust of police power and discretion"). *See* Priester, *supra* note 73, at 91.

[76] GRAY, *supra* note 3, at 203 (citing Agnello v. United States, 269 U.S. 20, 32 (1925)).

[77] Boyd v. United States, 116 U.S. 616, 641 (1886). For a thorough explanation of tracing the warrant requirement back to *Boyd*, *see* GRAY, *supra* note 3, at 205 n.169 (noting that *Boyd*'s place as essential to establishing the warrant requirement was reiterated by Chief Justice Roberts in his majority opinion in *Riley v. California*, 573 U.S. 373 (2014)).

[78] Priester, *supra* note 73, at 89. *E.g.,* GRAY, *supra* note 3, at 207 (noting the Court applied the warrant requirement in *Kyllo v. United States*, 533 U.S. 27, 40 (2001)).

by the dangers of granting officers unfettered discretion to that tactic, so the Court re-emphasizes the flexibility of the "unreasonableness" language in the Amendment, and finds a warrant requirement as a mechanism that allows oversight by granting judges concrete enforceability powers.[79] While "unreasonableness" is flexible, it is not a "free floating balloon," but tethered to "what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted."[80]

Colonialists were seeking to prevent two primary methods of intrusion: general warrants and writs of assistance.[81] In the American colonies, the Crown's agents needed only to say that a crime had occurred—or even that they had a mere suspicion—to obtain a general warrant.[82] No further details were required: neither the details of who had committed the crime nor where the evidence was.[83] "[General warrants] gave executive agents unfettered license to search whatever they pleased, for illegitimate reasons, for insufficient reasons, or no reason at all."[84] These general warrants stood in contrast to particular warrants, which required something very similar to probable cause presented to a neutral judge.[85]

Writs of assistance were an even more heinous sub-species of general warrants: they allowed the Crown's agents to enter any home and seize anything prohibited.[86] The holder of a warrant was also immune from any liability for destruction he caused while acting pursuant to the warrant.[87] These writs were famously described at the time by James Otis as an "instrument of arbitrary power, the most destructive of English liberty, and the fundamental principle of the constitution, that ever was found in an English law book."[88] Otis was particularly concerned about the searches of homes on nothing more than "bare suspicion without oath,"[89] emphasizing that the absence of judicial oversight was

[79] GRAY, *supra* note 3, at 204-05, 11 ("[T]he Court describes the warrant requirement as prospective remedy grounded in the reasonableness clause"); *see* Priester, *supra* note 73, at 93.

[80] GRAY, *supra* note 3, at 210 (citing to *Carroll v. United States*, 267 US 132, 149 (1925)).

[81] *See* Maclin, *supra* note 75 (arguing that the focus of the Amendment is the "rights of the people" and therefore the relevant perspective is of the people, not of individual Framers).

[82] LEONARD W. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 224 (Ivan R. Dee 2000) (1988); BRUCE A. NEWMAN, AGAINST THAT "POWERFUL ENGINE OF DESPOTISM" 2 (2007).

[83] *Id.* at 224-25.

[84] GRAY, *supra* note 3, at 162.

[85] NEWMAN, *supra* note 82, at 2.

[86] *Id.*

[87] See Thomas Y. Davies, *Can You Handle the Truth? The Framers Preserved Common-Law Criminal Arrest and Search Rules in "Due Process of Law"—"Fourth Amendment Reasonableness" is Only a Modern, Destructive, Judicial Myth*, 43 TEX. TECH. L. REV. 51, 86 n.164 (2010).

[88] JAMES OTIS, AGAINST WRITS OF ASSISTANCE (Feb. 24, 1761).

[89] *Id.*

one of the prime evils inherent in the writs.[90] The Fourth Amendment was intended to reverse colonial precedents and restrain discretionary search and seizure powers,[91] establishing protections for the home, as well as persons, papers, and effects.[92]

Time and again, the colonial memory of the dangers of broad grants of power has been a motivating concern for the Court in its Fourth Amendment jurisprudence. For instance, in *Berger v. New York*, the Court struck down a statute which gave police officers significant discretion to install wiretaps.[93] In so doing, the Court noted that the warrant requirement is not a formality "but a fundamental rule that has been recognized as basic to the privacy of every home in America."[94] The Court has also consistently held that the Fourth Amendment "should receive a liberal construction, so as to prevent stealthy encroachment upon or 'gradual depreciation' of the rights secured by them, by imperceptible practice of courts or by well intentioned, but mistakenly overzealous, officers."[95]

IV. CARPENTER IS NEITHER AN EXCEPTION TO AN EXCEPTION, NOR ALL THAT EXCEPTIONAL.

These concerns and expectations undergird the logic of expectations of privacy in *Katz v. United States*,[96] upon which nearly all modern Fourth Amendment jurisprudence rests.[97] After *Katz*, courts determine the scope of an individual's Fourth Amendment rights by examining whether that individual had a subjective expectation of privacy, and if so, whether society accepts that expectation of privacy as objectively reasonable.[98] While many of the exceptions to the warrant requirement pre-date *Katz*, over time, the Court has formulated them in *Katz*'s terms.

---

[90] Maclin, *supra* note 81, at 224.

[91] LEVY, *supra* note 82, at 224; *see* Brinegar v. United States, 338 U.S. 160, 182 (1949) (Jackson, J., dissenting) (officers engaged in crime investigation "will push the limit" of reasonableness without judicial restraint); *see also* Maclin, *supra* note 81, at 228.

[92] U.S. CONST. amend. IV. Professor Ohm has noted that banning general warrants and writs of assistance was not the end, but rather the means of creating distance between an individual and their government: "Or, put another way . . . 'it was a quirk of physics that this lined up with privacy pretty well.'" FARIVAR, *supra* note 46, at 168.

[93] 388 U.S. 41, 64 (1967).

[94] *Id.* at 63.

[95] GRAY, *supra* note 3, at 210 (quoting Gouled v. United States, 255 U.S. 293, 304 (1921)).

[96] 389 U.S. 347, 357 (1967).

[97] See generally, Martin McKown, *Fifty Years of Katz: A Look Back—and Forward—at the Influence of Justice Harlan's Concurring Opinion on the Reasonable Expectation of Privacy*, 85 GEO. WASH. L. REV. ARGUENDO 140, 140 (2017).

[98] *See* Katz, 389 U.S. at 361 (Harlan, J. concurring); *see also* McKown, *supra* note 97, As Professors Gray and Citron noted, if the Court had declined to extend Fourth Amendment protections to Katz, it would have "unsettled broadly held expectations and raise[d] the specter of a surveillance state." David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 85 (2013) [hereinafter Gray & Citron, Quantitative Privacy].

The exceptions to the warrant requirement under the Fourth Amendment are numerous and complex,[99] but there are four exceptions to the warrant requirement a prosecutor might invoke to establish that Ring footage collected without a warrant should not be suppressed: plain view, publicly visible movements, third party doctrine, and consent.[100] Despite the seemingly disparate nature of the exceptions, they are all united, at least in part, by the fact that something negates the individual's privacy interest under *Katz*.[101] And yet, for all of these exceptions to the warrant requirement (consent exception notwithstanding), the Court's jurisprudence over the last twenty years has been treated as establishing that there are sometimes exceptions to the exceptions, with the exception to the third-party doctrine in *Carpenter* having most visibly received this treatment.[102] In reality, instead of mechanically applying the exceptions, the Court is focusing on the technology at issue, thus recognizing these practices as not just different in degree, but different in kind.[103] Understood this way, the Court's decision in *Carpenter* not to extend the third-party doctrine is not an anomaly,[104] but rather the final brushstroke in the creation of an entirely new approach—one which begins with an examination of the technology itself.[105]

This approach was made explicit in *Riley v. California*, which raised questions about the limits of the search incident to arrest exception.[106] After an officer has facilitated a lawful arrest, the officer is permitted to conduct a warrantless search of the arrestee's person and the area within the arrestee's immediate control,[107] including inspecting and opening containers found on the person or in the area within the arrestee's immediate control.[108] According to the Court, these searches are necessary to secure evidence and protect the officer from weapons or ambush.[109] Additionally, the arrestee has a low expectation of privacy—they are, after all, now in the state's custody.[110]

---

[99] *See* GRAY, *supra* note 3, at 79-99.

[100] *Id.*

[101] *See Katz*, 389 U.S. at 360-361.

[102] See Laura K. Donohue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing A Test Consistent with Precedent and Original Meaning*, SUP. CT. REV. 347, 351-52 (2018).

[103] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 399 (2019); *see* Riley v. California, 573 U.S. 373, 393 (2014); FARIVAR, *supra* note 46, at 206 (noting the crux of petitioner's argument was "digital is different").

[104] *See* Donohue, *supra* note 102.

[105] GRAY, *supra* note 3, at 124-28; *see e.g.*, Gray & Citron, *Quantitative Privacy*, *supra* note 98.

[106] Riley v. California, 573 U.S. 374, 378 (2014).

[107] *See* Chimel v. California, 395 U.S. 752, 762-63 (1969).

[108] *See* Robinson v. United States, 414 U.S. 218, 236 (1973).

[109] *See* Arizona v. Gant, 556 U.S. 332, 338-39 (2009).

[110] Even if the arrestee argued a significant privacy interest, society would be unwilling to accept that expectation of privacy because of the need to protect officers and to preserve evidence for prosecution. *See* Lynne Peeples, *Brutality and Racial Bias: What the Data Say*, 583

And yet, despite the government making precisely the same arguments in *Riley v. California*,[111] the Court refused to allow a warrantless search of a cell phone.[112] The Court, with almost shocking clarity, rejected the expectation of privacy rationale:

> *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.[113]

The government had urged the Court to compare the cellphone with its numerous physical world predecessors, the Court not only refused but "responded with sarcastic exaggeration,"[114] noting that the argument was, "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[115]

Instead, the Court took up the petitioner's argument[116] that this broad search was more analogous to the general warrants and writs of assistance of the past.[117] The Court reasoned that the search of a cell phone is both qualitatively and quantitatively different from past searches because a cell phone can store so much information and connect to a variety of accounts, which might include medical, political, and religious information.[118] No such sensitive information was retrieved in this case; instead, the Court was concerned that the potential was

Nature 22, 22 (2020); Zack Beauchamp, *What the Police Really Believe*, Vox (July 7, 2020, 8:10 AM), https://www.vox.com/policy-and-politics/2020/7/7/21293259/police-racism-violence-ideology-george-floyd [https://perma.cc/WFN7-W3CA]; Myron Moskowitz, *A Rule in Search of a Reason: An Empirical Reexamination of* Chimel *and* Belton, 2002 WISC. L. REV. 657, 672 (2002).

[111] 573 U.S. at 374, 388 (2014). For a thorough recitation of the facts that led to arrest of David Riley, see Farivar, supra note 46, at 198-200. The tactics used by the police officers in that incident to escalate the situation are generally understood to be hallmarks of racist policing. See, e.g., Darwin Bond Graham, *Black People in California Are Stopped Far More Often by the Police*, THE GUARDIAN (Jan. 3, 2020, 1:00 AM), https://www.theguardian.com/us-news/2020/jan/02/california-police-black-stops-force [https://perma.cc/9B8J-7JZN].

[112] *Riley*, 573 U.S. at 401 (2014).

[113] *Id.* at 386.

[114] Ohm, *supra* note 103, at 400.

[115] *Id.* at 393. This was one of the key arguments the petitioners made that the Court adopted. FARIVAR, *supra* note 46, at 206 ("[A]n analogy [they] came up with was that saying 'a phone is just another container… [which is] like saying that a ride on a 747 is no different than a bicycle.'").

[116] "Physical items at the scene can pose a safety threat and have destruction possibilities that aren't present with a digital evidence. What is more, once you get into the digital world, you have the framers' concern of general warrant and the—the writs of assistance." FARIVAR, *supra* note 46, at 207.

[117] *See Riley*, 573 U.S. at 403.

[118] Priester, *supra* note 73, at 113 (citing *Riley*, 573 U.S. at 393-97).

there.[119] In holding that accessing the cell phone was a search, "the Court recognized that doctrinal principles grounded in the practical realities of the common law, and even the analog modern period, cannot be transposed by rote to digital data in the internet age."[120]

Similarly, the doctrines of the other relevant warrant requirement exceptions have not been "transposed by rote."[121] The following sections examine these exceptions and the logic underpinning them, the cases marked as exceptions to the exceptions, and the ways these exceptions might apply to Ring cameras. Where helpful, I will consider how lower courts have applied the identified ideas to pole cameras. Like Ring, pole cameras are often aimed at homes over a long period of time and create a digital archive of footage.[122]

A. The plain view exception, and Kyllo's "exception" to it

In the broadest terms, if law enforcement can see evidence of a crime an individual has no reasonable expectation of privacy in that evidence.[123] So long as the officer has the right to be where they are, what they observe is not considered a search.[124] However, officers are limited to what they can observe without manipulation; for instance, the Court has held that lifting up a stereo in order to determine by its serial number if it was stolen did not fit within the plain view exception and was a search.[125] Thus, where an individual has displayed something such that any member of the public can clearly view it, then they cannot

[119] At oral arguments, Justice Sotomayor raised this consideration to which the attorney for the government responded by noting there were around 250 contacts, about 59 photos, and 42 videos, each of which was less than a minute long. FARIVAR, *supra* note 46, at 207-08. It's worth noting too, that the arrest happened in 2009, and the phone was a competitor of the first generation of iPhone. *Id.* at 199.

[120] Priester, *supra* note 73, at 113.

[121] Priester, *supra* note 73, at 98.

[122] *See* United States v. Houston, 813 F.3d 282, 285 (6th Cir. 2016) ("The footage was recorded over the course of ten weeks by a camera installed on top of a public utility pole approximately 200 yards away."); *see also* United States v. Moore-Bush, 963 F.3d 29, 33 (1st Cir. 2020) ("The pole camera operated 24/7. Officers could access the video feed either live or via recordings.").

[123] This was first articulated in Coolidge v. New Hampshire, 403 U.S. 443 (1971), but the test has undergone slight changes since. *See, e.g.*, Horton v. California, 496 U.S. 128 (1990); Texas v. Brown 460 U.S. 730 (1983).

[124] To seize the item, the test acquires two additional prongs: did the officer have a right to physically access the item, and was the item obviously contraband. Horton v. California, 496 U.S. 128, 142 (1990). This confusing legal definition of a search was criticized by Justice Scalia in his majority opinion in *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001).

[125] Arizona v. Hicks, 480 U.S. 321, 327 (1987).

reasonably expect it to remain private from anyone—including officers. It would be absurd (and impossible to administer) to hold otherwise.[126]

In *Kyllo v. United States*, the Court confronted the question of what limits should be placed on the power of technology to shrink the realm of guaranteed privacy, a question it had repeatedly sidestepped.[127] It held that while the officer could stand in the street and look at Kyllo's home,[128] the addition of a thermal imaging device turned the officer's observations into an unreasonable search.[129] Much of the Court's reasoning turned on the sanctity of the home.[130] It noted that warrantless searches of the home are presumptively unreasonable, with only a few, narrowly tailored, exceptions.[131] In a move paralleled in *Riley*,[132] the Court did not distinguish between surveillance of the home that picks up intimate details and that which does not, instead noting that because law enforcement could not know in advance which they would be obtaining, all details must be intimate.[133] Instead, where the government has "obtain[ed] by sense-enhancing technology *any* information regarding the interior of the home that could not otherwise have been obtained without a physical 'intrusion into a constitutionally protected area'" a search has occurred, thus requiring a warrant.[134]

[126] *See* California v. Greenwood, 486 U.S. 35, 41 (1988) (noting "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public").

[127] *Id.* at 34 (referencing the decision in *California v. Ciraolo*, 476 U.S. 207 (1986), where the technology of flight was allowed to expand plain view doctrine); *see* Silverman v. United States, 365 U.S. 505, 508-09 (1961) (refusing to center analysis on the "spike mic" and focusing instead on the narrow trespass violation); *see also* United States v. Knotts, 460 U.S. 276, 284 (1983) ("if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable").

[128] In his dissent, Justice Stevens notes that any member of the public might have seen with their own eyes snow melting at a different rate and fails to see how the use of the thermal imaging camera changes the Constitutional calculus. *Kyllo*, 533 U.S. at 43 (Stevens, J., dissenting). The majority responds to this by saying that just because "equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Id.* at 35 n.2.

[129] "Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images." *Id.* at 29-30.

[130] *Kyllo*, 533 U.S. at 31 (citing *Silverman*, 365 U.S. at 511) (noting that the right to retreat into the home stands at "the very core" of the Fourth Amendment).

[131] *Kyllo*, 533 U.S. at 31 (citing *Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990); Payton v. New York, 445 U.S. 573, 586 (1980)).

[132] *See Riley*, 573 U.S. at 403 ("With all [modern cell phones] contain and all they *may* reveal, they hold for many Americans 'the privacies of life'"); *supra* note 119.

[133] *Kyllo*, 533 U.S. at 38-39.

[134] *Id.* at 34 (quoting Silverman, 365 U.S. at 512) (emphasis added); *see* Priester, *supra* note 73, at 101 ("once technological enhancement further expands the information available to the

As an initial matter, where a Ring camera is pointed towards the street, the footage will likely be of events that occurred in plain view.[135] Generally, the camera just records what a human could see.[136] However, at least one lower court has found that "a pole camera is not a mere video camera and most certainly allowed law enforcement to enhance their senses" because it recorded "twenty-four hours a day, sent the recording to a distant location, and allowed the officer to view it at any time and to replay moments in time."[137] Ring doorbells, as they currently work, do not produce recordings of all hours of everyday,[138] but, like pole cameras, they do create an otherwise perfect digital record, at least as far as a home is concerned.[139] Anytime someone leaves a Ring-equipped home, the camera is necessarily triggered and, if the motion zone is set to the street, it might record each and every time someone drives by, even including the movements of a neighbor across the street.[140] All this to say that Ring cameras record the details of the home, thus implicating *Kyllo*'s strong

police, the constitutional calculus changes"). Sense-enhancing technology has been extended beyond heat-vision: in her concurring opinion in *Florida v. Jardines*, Justice Kagan posited that a drug-sniffing dog is so specialized as to be sense-enhancing. Florida v. Jardines, 569 U.S. 1, 13-15 (2013).

[135] *See Ring Video Doorbells*, RING, https://shop.ring.com/pages/doorbell-cameras [https://perma.cc/LB2K-P6Z5**]**.

[136] *See* Bruce Brown, *Ring Adds Color Night Vision to Wired Security Devices and HDR to Wireless Ones*, DIGITAL TRENDS (Feb. 14, 2019), https://www.digitaltrends.com/home/ring-wired-security-products-color-night-vision [https://perma.cc/3XJB-Q6MD].

[137] State v. Jones, 903 N.W.2d 101, 112 (S.D. 2017) ("[T]his type of surveillance does not grow weary, or blink, or have family, friends, or other duties to draw its attention."); *see* Commonwealth v. Mora, 485 Mass. 360, 367 (2020); United States v. Moore-Bush, 381 F. Supp. 3d 139, 149 (D. Mass 2019) ("While the law does not 'require law enforcement officers to shield their eyes when *passing by* a home on public thoroughfares,' . . . it does forbid the intrusive, constant surveillance here." (emphasis added) (citing California v. Ciraolo*,* 476 U.S. 207, 213 (1986))).

[138] *See Protect Plans*, *supra* note 13. Depending on the Ring Protect Plan, the homeowner only has access to live streamed footage and the moments that get recorded. However, the highest level of protect plan offers 24/7 monitoring, so whether Amazon has records of that footage is unknown. *Id.*

[139] *See Jones*, 903 N.W.2d at 112 ("Much like the tracking of public movements through GPS monitoring, long-term video surveillance of the home will generate 'a wealth of detail [about the home occupant's] familial, political, professional, religious, and sexual associations.'" (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring))).

[140] *See Nationwide Search Underway for Suspect After Body of Titusville Woman Found in Trunk of Car, Police Say*, FOX 35 ORLANDO (Feb. 25, 2020), https://www.fox35orlando.com/news/nationwide-search-underway-for-suspect-after-body-of-titusville-woman-found-in-trunk-of-car-police-say [https://perma.cc/449B-RA3E] (suspect's car was last seen on Ring footage).

protections for the home.[141] Reliance on the plain view exception for warrantlessly obtaining Ring recordings is further negated by the fact that the law enforcement portal is not in general public use.[142]

B. The publicly visible movement exception, and Jones's "exception" to it

As the Court was developing the plain view doctrine, it also extended it to cases where officers tail someone suspected of a crime, which came to be known as the exception for publicly visible movements. Under this exception, officers are not required to obtain a warrant to follow someone because any ordinary citizen could theoretically do the same.[143] This investigative technique first met technology in the "beeper cases," *United States v. Knotts*[144] and *United States v. Karo*.[145] In both cases, law enforcement, acting without a warrant, installed a GPS-tracking beeper within a container that was then transported via car, and the beeper's final location was used to support a search warrant for those premises.[146] In *Knotts*, the use of the beeper was found constitutionally permissible because the container's movement could have been tracked by visually monitoring it,[147] whereas the beeper in *Karo* was not because the container with the beeper entered the home of the suspect, and tracking a suspect into a dwelling, absent an exigent circumstance, was not permissible.[148] And yet, in *United States*

[141] *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) (holding that all details of the home are intimate details).

[142] *See How Public Safety Agencies Use Neighbors*, RING.COM, https://support.ring.com/hc/en-us/articles/360031595491-How-Public-Safety-Agencies-Use-Neighbors [https://perma.cc/AZH3-9HGX] (The information on this page originally appeared under the title "How Your Local Law Enforcement Agency Uses Neighbors[.]"). This factor of the *Kyllo* test has been under scrutiny nearly since its inception, so the actual weight it should be afforded is unclear. *See* Florida v. Jardines, 569 U.S. 1, 11 (2013); *see also Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting) ("[T]he threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."); *see also* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1394 (2002).

[143] United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). The Court cited to precedent which outlined the lesser expectation of privacy in a motor vehicle. *See* Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion); *see also* Rakas v. Illinois, 439 U.S. 128, 153-154, 154 n.2 (1978) (Powell, J., concurring); South Dakota v. Opperman, 428 U.S. 364, 368 (1976)).

[144] 460 U.S. 276, 282 (1983). For the circumstances leading to the arrest, see FARIVAR, *supra* note 46, at 88-89.

[145] 468 U.S. 705 (1984).

[146] *Id.* at 709-10; *Knotts*, 460 U.S. at 279.

[147] *Knotts*, 460 U.S. at 281-82. The Court specifically declined to distinguish between the level of efficiency of a law enforcement officer when forced to manually tail versus being aided by the beeper. *See Knotts*, 460 U.S. at 284.

[148] *See Karo*, 468 U.S. at 717.

v. Jones, the Court held that the GPS tracking at issue required a warrant,[149] even though the car remained publicly observable.[150]

While the Court in *Jones* unanimously held that the warrantless GPS tracking was impermissible, the majority opinion focused on reestablishing trespass as a means of violating the Fourth Amendment.[151] However, in her concurrence, Justice Sotomayor suggested that GPS surveillance might support a greater privacy right because of its ability to generate a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[152] This rationale was later adopted by the Court in *Carpenter v. United States*, when it examined the constitutionality of the warrantless collection of data that (imprecisely) detailed the individuals movements over the course of four months.[153] In *Jones*, the tracker was active for twenty-eight days, yet the information it captured resulted in over 2,000 pages of data.[154] Furthermore, all of this was done with no human involvement and minimal cost.[155] In his concurrence, Justice Alito noted this distinction:

[149] *See* United States v. Jones, 565 U.S. 400, 410 (2012).

[150] *See id.* at 403; *see also Karo*, 468 U.S. at 715.

[151] *Jones*, 565 U.S. at 404-11.

[152] *Id.* at 415-16. This is sometimes referred to as a mosaic theory—that out of all these discrete pieces, law enforcement could build a whole picture—a "mosaic." *E.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012). Scholars have pointed out that a mosaic theory of privacy raises more questions than it answers, particularly because it implicates "traditional" surveillance techniques. GRAY, *supra* note 3, at 109-16; *see generally* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 382 (2013). An additional problem is that it is difficult to justify why one piece of information does not violate privacy, but the aggregate might: "it is impossible to add zero to zero and get anything other than zero." GRAY, *supra* note 3, at 83 (citing Kerr, *supra*).

[153] 138 S. Ct. 2206, 2217 (2018); Ohm, *supra* note 103, at 371-72 ("*Jones* played a central role in the Court's reasoning [in *Carpenter*] . . . Robert's adopted the shadow majority in the prior case as though it had been the grounds on which it had been decided . . . As Justice Kennedy pointed out in his dissent, in so doing, the Court treated the concurrences as though they were holding").

[154] *Jones*, 565 U.S. at 403. "What distinguished *Jones* from *Knotts* in the *Katz* analysis was both the quantity of location tracking data gathered by the electronically enhanced surveillance—not simply for twenty-eight days, but twenty-four hours per day to accumulate over two thousand pages of location data points—and the qualitative nature of the technology involved—using automated hardware and software to generate surveillance data with no human involvement and at minimal cost." Priester, *supra* note 73, at 117-18.

[155] FARIVAR, supra note 46, at 157. In arguing *Jones*, the lawyer for the government attempted to analogize to *Knotts* because the police had lost the car and had to send out a helicopter, which Chief Justice Roberts quickly distinguished on cost grounds:

"But that's a good example of the change in technology," Roberts retorted. "That's a lot of work to follow the car. They've got to listen to the beeper. When they lose it they have got to call in the helicopter. Here they just back in the station and they—they push a button whenever

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken . . . Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap . . . [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.[156]

In a similar line of questions at oral arguments, Justice Sotomayor asked the government to explain the difference between GPS surveillance and a general warrant, before noting that indiscriminate surveillance is the foundation of the Fourth Amendment.[157]

In a potential challenge to the warrantless collection of Ring footage, the government would doubtless argue that the defendant's movements were publicly visible, and, depending on the case, that tracking occurred over a short period of time, in contrast to the weeks and months of tracking at issue in *Jones* and *Carpenter*.[158] However, in a case prosecuting either the owner of the Ring doorbell or the homeowner across the street, tracking all the comings and goings from a house still generates a comprehensive record.[159] Furthermore, once obtained, the footage could be digitally catalogued, kept indefinitely,[160] and used with third-party facial recognition software, such as Clearview AI.[161] While the record of

---

they want to find out where the car is. They look at data from a month and find out everywhere it's been in the past month. That—that seems to me dramatically different." *Id.*

[156] *Jones*, 565 U.S. at 429-30 (Alito, J., concurring).

[157] "What motivated the Fourth Amendment historically was the disapproval, the outrage, that our Founding Fathers experienced with general warrants that permitted police indiscriminately to investigate just on the basis of suspicion, not probable cause and to invade every possession that the individual had in search of a crime. How is this different?" FARIVAR, *supra* note 46, at 158.

[158] *Carpenter*, 138 S. Ct. at 2212; *Jones*, 565 U.S. at 403.

[159] *See, e.g.*, United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *16-34 (E.D. Wash. Dec. 15, 2014); State v. Jones, 903 N.W.2d 101, 112 (S.D. 2017); People v. Tafoya, 2019 Colo. App. LEXIS 1799, at *13 (Co. Ct. of App. Nov. 27, 2019).

[160] *See* Aaron Holmes, *Amazon says police can keep videos from Ring doorbells forever and share them with anyone*, BUS. INSIDER (Nov. 20, 2019, 9:50 AM), https://www.businessinsider.com/police-keep-amazon-ring-doorbell-videos-forever-2019-11?op=1 [https://perma.cc/VDZ8-FK9P].

[161] According to the founder of Clearview, one of the challenges for the accuracy of the software is that the photos in the database are at eye level, whereas "much of the material that the police upload is from surveillance cameras mounted on the ceilings or high on walls. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-

an individual suspect's movement might not be as detailed as it was in *Jones* or *Carpenter*, the law enforcement portal has a similar effect of significantly reducing the amount of work involved in collecting footage.[162]

C. The third-party doctrine and Carpenter's "exception" to it

The third-party doctrine has its origins in *Hoffa v. United States*.[163] Before prosecuting Jimmy Hoffa, the government hired an informant, who Hoffa allowed into his hotel room and conspired to commit crimes in front of.[164] Hoffa's attorneys argued that hiring the informant violated Hoffa's Fourth Amendment rights, but the Court held otherwise, saying that Hoffa relied on his own misplaced confidence, and that the Fourth Amendment emphatically does not protect misplaced confidence.[165]

Post-*Katz*, the "misplaced trust" idea was reaffirmed and extended in *Smith v. Maryland.*[166] Relying on *Hoffa* and *United States v. Miller*,[167] the Court held that an individual has no legitimate expectation of privacy in information that they voluntarily turn over to a third-party.[168] For many years, the third party doctrine was largely unchallengeable because it served as a complete negation of an individual's expectation of privacy, even as the doctrine expanded from "filling in the gaps" by looking for something specific, to "trawling for anything,

recognition.html [https://perma.cc/TQ96-XQG9]. Ring cameras, in contrast, are often mounted much lower, and thus would likely be more accurate. However, in this instance, accuracy is nearly as harmful as inaccuracy. *See, e.g.*, ACLU Letter, https://www.aclu.org/sites/default/files/field_document/02.16.2021_coalition_letter_requesting_federal_moratorium_on_facial_recognition.pdf [https://perma.cc/5Z4J-YE9B]; *see also* Kashmir Hill, *What Happens When Our Faces Are Tracked Everywhere We Go?*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html (noting the origins of Clearview in physiognomy, the discredited theory that a person's character might be judged based on their facial features).

[162] *See* Ng, *supra* note 56. As more people buy Ring doorbells, the location inferences might become more precise. *See* Cameron & Mehrota, *supra* note 57.

[163] 385 U.S. 293 (1966).

[164] *Id.* at 296.

[165] *Id.* at 300-02.

[166] 442 U.S. 735 (1979). The defendant argued that the pen register at issue—installed by the telephone company—was typically used to track long distance calls, not local calls, so he had a reasonable expectation of privacy in his local calls. The Court disagreed, noting that it was typical for operators to be a part of a phone call, and because of how billing works, the defendant was in fact on notice that all his calls might be tracked, therefore negating his reasonable expectation of privacy. *Id.* at 735-45.

[167] 425 U.S. 435 (1976). In *Miller*, the government had obtained Miller's banking records. The Court held that by voluntarily conveying his information to the bank, Miller had no expectation of privacy and therefore, the bank handing over the records was not a search. *Id.*

[168] *Smith*, 442 U.S. at 743-44.

anywhere, all the time."[169] Justice Sotomayor noted these shifts in *Jones*,[170] but a majority of the Court did not pick up the cause until *Carpenter v. United States*.[171]

In *Carpenter*, the government sought to identify the suspect in a string of robberies by obtaining approximately four months' worth of cell-site location information (CSLI) via a subpoena under the Stored Communications Act.[172] Instead, the Court held that the "progress of science . . . does not erode" privacy protections, [173] and thus "[a] person does not surrender all [privacy] rights by venturing into the public sphere."[174] In the same vein, at the start of the majority opinion, Chief Justice Roberts embraced a strong privacy right: "First, [] the [Fourth] Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' Second, and relatedly, [] a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[175]

The Court described CSLI as "detailed, encyclopedic, and effortlessly compiled."[176] This reaffirms many of the concerns raised in *Jones*, particularly that this surveillance requires police to expend few resources.[177] Furthermore, the Court explicitly rejected the idea that because an individual had shared the information with (or in front of) a third-party they had no privacy interest. Instead, the Court noted that where an individual "has a reduced expectation of privacy in information knowingly shared with another," privacy protections do not "fall[] out of the picture entirely" particularly because "in no meaningful sense does [a cell phone] user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[178] As Professor Ohm has suggested, in so holding, the Court adopted Justice Sotomayor's concurrence in *Jones*, where she noted that people reveal a great deal of information about themselves in the course of carrying out mundane tasks, making the third-party doctrine ill-suited to the digital age.[179]

If the defendant challenging the collection is someone other than homeowner, perhaps a neighbor across the street or someone walking by, the third-party

[169] FARIVAR, *supra* note 46, at 60; *see* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 987-988 (2016).

[170] *E.g.,* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

[171] 138 S. Ct. 2206 (2018).

[172] *Id.* at 2212 ("Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.")

[173] *Id.* at 2223.

[174] *Id.* at 2217.

[175] *Id.* at 2214 (internal citations omitted).

[176] *Carpenter*, 138 S. Ct at 2216.

[177] Ohm, *supra* note 103, at 367.

[178] *Carpenter*, 138 S. Ct. at 2219-20.

[179] Ohm, *supra* note 103, at 372 (citing United States v. Jones, 565 U.S. 400, 415 (2012)).

doctrine remains pertinent because the information was shared with the homeowner, and they become the relevant third-party. While the opinion in *Carpenter* leaves a carve out for "traditional techniques," including cameras, the technology at issue here is not the cameras but the law enforcement portal.[180] Additionally, Ring doorbells are networked: the footage is effortlessly compiled and accurately time-stamped.[181] Law enforcement does not need to go door to door looking for cameras and asking for footage—they do not even have to type out a request; instead, they may simply create a box and wait to receive footage.[182]

After an officer has requested and collected a homeowners' Ring footage, the government could argue that is not an unreasonable search and seizure under the foregoing exceptions. However, Ring and the law enforcement portal are more similar to the "exceptional" cases than they are to the founding cases. As in *Kyllo*, this could be sense-enhanced surveillance of the home.[183] As in *Jones* and *Carpenter*, law enforcement likely obtains comprehensive records, effortlessly compiled.[184] While all of these cases (and *Riley*) were considered exceptional cases at the time of decision, they are better understood as united by their shared feature: the warrantless police use of digital technology as the primary method of investigation.[185] In every case, the Court saw that the use of technology required it to reach a different conclusion than would be reached under traditional and well-established exceptions to the warrant requirement.[186] Collectively, these cases suggest that when law enforcement is relying on digital technology, the Court may reevaluate other exceptions to the warrant requirement.[187] Once the reader is looking for this kind of "tech exceptionalism"[188] and approaches the search and seizure question by centering the technology used, *Carpenter* becomes exceptional only for its explicitness.[189]

But there's one more exception law enforcement relies on when requesting footage that does not yet have an "exception to the exception." The following section argues that the consent exception can be similarly negated in the context of Amazon Ring's law enforcement portal.

---

[180] *Id.* at 2220.

[181] *See id.* at 2216.

[182] *See* Ng, *supra* note 56; *Requests for Video Recordings from Law Enforcement*, *supra* note 62.

[183] *See supra* note 137; *Kyllo*, 533 U.S. at 34.

[184] *Carpenter*, 138 S. Ct. at 2216.

[185] *Carpenter*, 138 S. Ct. at 2206; Riley v. California, 573 U.S. 374, 378 (2014); United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001).

[186] *See Carpenter*, 138 S. Ct. at 2206; *Riley,* 573 U.S. at 378; *Jones*, 565 U.S. 400; *Kyllo*, 533 U.S. at 27.

[187] *See Carpenter*, 138 S. Ct. at 2206; *Riley,* 573 U.S. at 378; *Jones*, 565 U.S. 400; *Kyllo*, 533 U.S. at 27.

[188] *See* Ohm, *supra* note 103, at 399-413.

[189] Gray & Citron, *Quantitative Privacy*, *supra* note 98, at 101-113.

V. APPLYING TECH EXCEPTIONALISM TO POLICE COLLECTION OF RING FOOTAGE.

In requesting footage or information of any kind, officers rely on the consent exception to the warrant requirement. This section argues that for similar reasons as discussed above, footage requests via the law enforcement portal should not fall under the consent exception, but instead require a warrant. I begin by explaining the logic underpinning the consent exception, before applying the principles discussed in Part IV to challenge the consent exception in cases of collection of Ring Footage.

A. The consent exception to the warrant requirement

The consent exception is facially intuitive but can become quite complicated.[190] At its most basic level, the consent exception simply means that if a police officer asks for permission to conduct a search and receives consent, then no search has taken place within the meaning of the Fourth Amendment.[191] The earliest case predates *Katz* by some forty-years. While the Court did not use the word "consent",[192] it held that Fourth Amendment rights could not be waived because of the "implied coercion" by law enforcement.[193] Consent as an exception to the warrant requirement was first suggested in 1946 in Davis v. United States,[194] with the "voluntariness" test being formalized in *Schneckloth v. Bustamonte*,[195] though the Court had implied it might exist in *dicta* in *Katz*.[196] One can understand this in terms of a privacy expectation under *Katz*: if an individual knows about the search and has acknowledged it, then that person does not have an expectation of privacy in the thing that was searched.[197] As with most of the other exceptions, the Court weighs other considerations, such as the normative idea that "the concept of agreement and consent should be given a weight and dignity of its own."[198]

However, the amount of weight that should be accorded to an individual's consent is complicated by power disparities between the police and the

[190] For a thorough examination of the consent exception, *see* Tracey Maclin, *The Good and Bad News About Consent Searches in the Supreme Court*, 39 MCGEORGE L. REV. 27 (2008).

[191] *Id.* at 27.

[192] *Id.* at 36-37 (discussing *Amos v. United States*, 255 U.S. 313 (1921)).

[193] *See Amos*, 255 U.S. at 317.

[194] Maclin, *supra* note 190, at 37.

[195] 412 U.S. 218 (1973). The case discusses whether consent is in fact an exception to the warrant requirement, but simultaneously treats consent as an exception to the probable cause requirement for car searches. *Id.* at 219 ("It is … well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent"). *See* Maclin, *supra* note 190, at 48-63.

[196] Maclin, *supra* note 190, at 50, n.152.

[197] *See* Katz v. United States, 389 U.S. 347, 357 (1967).

[198] United States v. Drayton, 536 U.S. 194, 207 (2002).

policed.[199] Empirical studies have shown "the extent to which people feel free to refuse to comply is extremely limited under situationally induced pressures," such as those at play in interactions between law enforcement and citizens.[200] Furthermore, police officers have acknowledged that they seek consent because it may allow a broader search than they would be able to conduct under a warrant, i.e., officers seek consent in order to conduct wider searches than are supported by probable cause.[201] Officers are further incentivized to seek consent because courts treat consent with significant deference, and are thus unlikely to exclude evidence at a suppression hearing.[202]

When requesting footage, law enforcement seeks consent via comments on posts on the Neighbors app or via mass-email when using the geofence feature of the portal.[203] The question is whether either of these is so quantitatively and qualitatively different as to necessitate an exception to the consent exception of the warrant requirement.[204] Commenting and requesting footage is likely too similar to traditional investigative methods for consent to be negated[205]—little distinguishes it from a traditional tip line. As will be discussed in the following section, law enforcement use of the portal likely produces a different result.

B. Using tech exceptionalism to negate the consent exception

There are several features that distinguish the law enforcement portal from traditional instances where consent has been accepted as a permissible exception to the warrant requirement. Consent necessarily implies a right to say no, but there is no actual "no" button within the email: the only obvious option is to hand over the footage—with or without reviewing it.[206] It is unclear what, if any, repercussion saying "no" might carry. In the past, Ring shared with law enforcement the information of people who decline to share footage, such that law enforcement could visit in person to request again.[207] While Ring claims it no

[199] See Janice Nadler, No Need to Shout: Bus Sweeps and the Psychology of Coercion, SUP. CT. REV. 153, 155 (2002).

[200] *Id.*

[201] *See* Maclin, *supra* note 179, at 31; *see* George C. Thomas III, *Terrorism, Race, and a New Approach to Consent Searches*, 73 Miss. L.J. 525, 548-49 (2003).

[202] *See* Maclin, *supra* note 190, at 31. Of course, it is still possible to challenge consent searches on reasonableness grounds. *See, e.g.*, United States v. Drayton, 536 U.S. 194 (2002); *see also* Illinois v. Rodriguez, 497 U.S. 177 (1990).

[203] *See supra* Part II.B, II.C.

[204] *See* Priester, *supra* note 73.

[205] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220.

[206] *See A Helpful Guide to Video Requests*, RING, https://support.ring.com/hc/en-us/articles/360023205151-A-Helpful-Guide-to-Video-Requests- [https://perma.cc/A8CB-YK37]; *see also* Second Letter from Amazon to Sen. Markey, *supra* note 61, at 6-7. The individual could also choose to ignore the email, or unsubscribe from all emails. *Id.*

[207] Dell Cameron, *Ring Gave Police Stats About Users Who Said 'No' to Law Enforcement Requests*, GIZMODO (Aug. 30, 2019, 1:45 PM), https://gizmodo.com/ring-gave-police-stats-

longer does this, nothing more than their own internal policy stops them from doing so in the future. In addition, Ring is likely collecting this information because collecting email click and response rates is a standard industry practice.[208]

Further, the portal allows for law enforcement to submit a mass request to as many people as have cameras within the geofence.[209] As one police chief noted, "[Police] could digitally cover a block in a few seconds if people were monitoring the app closely[.] . . . Right now, people would have to be home for us to ask for video. Now they can [respond] from their office, while they're at work, while they're on vacation, anywhere they happen to be."[210] In addition to not having to hope that individuals are at home, police do not have to spend significant time or resources sending follow-up requests or even looking for cameras. The only limits on the amount of footage are those set by Ring or internal police policies.[211] The ease of obtaining mass amounts of footage in a short time means that, like the records in *Carpenter*, this is quantitatively different.[212]

This "mass-message" capability saves significant time and resources that officers typically spend sending follow-up requests, looking for cameras, or calling on individuals when they are not at home.[213] Further, the amount of footage shared with the police is only limited by internal police policies or by Ring itself.[214] As such, the ease by which a mass amount of footage may be obtained via the portal is, like the phone records in *Carpenter*, quantitatively distinct.

The portal is also qualitatively different from traditional police surveillance. Surveillance cameras have traditionally been confined to conspicuous placement in business districts, where an individual more clearly has a reduced expectation

about-users-who-said-no-to-law-e-1837713840 [https://perma.cc/C746-3GKD]. It should be noted Ring claims to no longer share this information with law enforcement.

[208] Sarah Scire, *"Big Tech Is Watching You. Who's Watching Big Tech?" The Markup is Finally Ready for Liftoff*, NIEMAN LAB (Feb. 25, 2020), https://www.niemanlab.org/2020/02/big-tech-is-watching-you-whos-watching-big-tech-the-markup-is-finally-ready-for-liftoff/ [https://perma.cc/J75E-Q9UZ].

[209] The number of people who will receive the request is dependent on density of both buildings and Ring doorbells. For a discussion of the density of cameras within major American cities, see Cameron & Mehrota, *supra* note 57. The law enforcement portal does have limits on how large the geofence can be and the window of time in which footage can be requested in one request, but, heretofore, there has been no reporting of other measures internal to the portal which prevent law enforcement from constantly requesting all footage, such as a limit of requests. *See* Second Letter from Amazon to Sen. Markey, *supra* note 61, at 2.

[210] Alfred Ng, *Amazon's Ring Wants Police to Keep These Surveillance Details From You*, CNET (Aug. 21, 2019 5:00 AM), https://www.cnet.com/news/amazon-ring-wants-police-to-keep-these-surveillance-details-from-you/ [https://perma.cc/3GWL-QHTF].

[211] *See* Maclin, *supra* note 75, at 202.

[212] Ng, *supra* note 210.

[213] *See id.*

[214] *See id.*

of privacy because they are in a public place.[215] However, networked surveillance of a residential neighborhood is different in kind, as it inevitably captures the "intimate details of the home,"[216] or the "whole of [one's] physical movements."[217] Given police officers' recent willingness to use whatever technology is at their disposal to track protestors exercising their First Amendment rights,[218] it is easy to imagine the extension of this logic to legitimate casual use of the law enforcement portal. In fact, at least one police department has used the portal to collect footage of protesters, although what details were obtained is unclear.[219] As discussed above, Fourth Amendment cases typically turn on the scope of what was actually accessed; but the Court's willingness to entertain hypotheticals in digital search cases brings salience to conceivable harm.[220]

Finally, it is unclear whose consent is or should be relevant here. In traditional consent cases it is generally obvious that the person consenting has authority over what is being searched, and in most cases, they are also the person the government will ultimately be prosecuting with the fruits of the search.[221] In the cases involving Ring footage, the person prosecuted is not the one consenting. Typically, in the search of a physical object, for instance, a court would then consider whether the person consenting had either actual or apparent authority over the thing being searched, under third-party consent.[222] However, that is an

[215] *But see* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 542 (citing *State v. Thomas*, N.E.2d 240, 246 (Ind. Ct. App. 1994) (holding prolonged, surreptitious business surveillance in violation of Fourth Amendment)).

[216] Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

[217] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 415, 430 (2015) (Sotomayor, J., concurring) (Alito, J., concurring)); *see* discussion *supra* Part IV.B & C.

[218] *See, e.g.*, Sam Biddle, *Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr*, THE INTERCEPT (July 9, 2020, 2:00 PM), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests [https://perma.cc/9CAM-T2V4]; Ken Klippenstein, *Federal Agencies Tapped Protesters' Phones in Portland*, THE NATION (Sept. 21, 2020), https://www.thenation.com/article/politics/homeland-security-portland [https://perma.cc/597E-7SW6].

[219] *See* Matthew Guariglia & Dave Maass, *LAPD Requested Ring Footage of Black Lives Matter Protests*, ELECTRONIC FRONTIER FOUNDATION (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests [https://perma.cc/QS9B-3RKG].

[220] *See supra* notes 119, 132, 133; *see also* FARIVAR *supra* note 46, at 198-199, 207, and accompanying text.

[221] *See* Maclin, supra note 190, at 44 (citing Thomas Y. Davies, Denying a Right by Disregarding Doctrine: How Illinois v. Rodriguez Demeans Consent, Trivializes Fourth Amendment Reasonableness, and Exaggerates the Excusability of Police Error, 59 TENN. L. REV. 1, 30 (1991)).

[222] Illinois v. Rodriguez, 497 U.S. 177 (1990).

ill-fitting match here, because in those cases, such as the search of a shared house, the ultimate target of prosecution also had some authority over it.[223] Here, a person walking by on the street, for example, has *no* authority—and would never be afforded the opportunity—to consent to the search. Framed this way, the relevant exception to the warrant requirement here is more like the third-party doctrine. Just as Carpenter could not opt out of having a cell phone, how could an individual opt-out of being recorded by a Ring camera?[224]

All of this taken together, the law enforcement portal raises the specter of a general warrant.[225] Beyond a veneer of consent, it is difficult to distinguish the mass-emails from a general warrant, and thus, using the portal to send these requests should require a warrant.

CONCLUSION

At bottom, where law enforcement use of digital technology is quantitatively and qualitatively different from traditional surveillance, the Court has affirmed the Fourth Amendment's protection against a surveillance state. In this instance, requiring judicial approval before law enforcement accesses the portal gives due weight to the danger of unlimited police discretion, even at the expense of some efficiency in law enforcement.[226]

The Fourth Amendment is a call to action that demands political branches commit to policies of restraint for law enforcement and, should they fail, allows courts to step in and act as a guardian of those rights.[227] While the political branches neglected this duty for some time, this political moment is finally forcing us to question and redefine what policing means.[228] The benefits of formal policy affirmatively limiting police surveillance are significant: instead of waiting for abuses and a subsequent court to determine if an abuse in fact occurred, they might be completely prevented.[229] Until then, beginning the reasonableness inquiry with the technology used reaffirms what the Court has already begun to

[223] *Id.*

[224] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[225] *See* discussion *supra* Part III (regarding searches incident to general warrants).

[226] *See* GRAY, *supra* note 3, at 215.

[227] *See id.* at 171.

[228] *See* Jason Kelley & Matthew Guariglia, *Amazon Ring Must End Its Dangerous Partnerships with Police*, ELECTRONIC FRONTIER FOUNDATION (June 10, 2020), https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police [https://perma.cc/4C6D-XUER]; John Eligon & Dionne Searcey, *Minneapolis Will Dismantle Its Police Force, Council Members Pledge*, N.Y. TIMES (June 7, 2020), https://www.nytimes.com/2020/06/07/us/minneapolis-police-abolish.html [https://perma.cc/RX9L-BQA5].

[229] Farivar, *supra* note 46, at 230-31.

articulate: our technological moment is not just different in degree, but different in kind, and our core rights are threatened by the dangers it poses.