Selected Papers of #AoIR2020:
The 21st Annual Conference of the
Association of Internet Researchers
Virtual Event / 27-31 October 2020

MATERIAL ENTANGLEMENTS OF COMMUNITY SURVEILLANCE NETWORKS & INFRASTRUCTURAL POWER

Lauren Bridges
Annenberg School for Communication, University of Pennsylvania

Introduction

Since Amazon acquired Ring Inc. in February 2018 for an estimated $1 billion, they have secured over 1,400 partnerships with law enforcement agencies who have access to consenting Ring users' feeds and publicly available content uploaded to Neighbors—the social media crime-reporting app. Neighbors is marketed by Ring as "your community coming together to keep you safe and informed" (*Neighbors by Ring - Apps on Google Play*, n.d.) and is a free for anyone to use and participate in, regardless of whether you own a Ring product or not. Although Neighbors is an "opt-in" application and users choose to upload content, Ring can disclose any content captured on a Ring device to law enforcement that complies with a warrant or is considered a "reasonable government request" (Cericola, 2020).

While there is anecdotal evidence of reduced petty crime and solving local policing cases, privacy advocates are concerned about the potential for abuse of civil liberties in discriminatory community surveillance networks, like Neighbors, that are predicated on a false sense of increased security (Stanley, 2019) and are prone to the "policing of race in residential space" (Kurwa, 2019). These kinds of neighborly surveillance practices encourage "solutions" that far outstrip the infraction and escalate minor incidents into (potentially fatal) encounters with law enforcement (Gilliard, 2020). Examples gleaned from local posts, reviewed for this paper, included someone stealing a pot plant from a neighbor's stoop, to which commenters replied calling the person a "low life", "useless scum", a "POS", and "pathetic". Similar moments of collective rage erupted over two kids dumping a mattress at the edge of someone's property, a young teen charging her phone on someone's front porch, and two youths making out on someone's bench, which had neighbors invoke racialized and classed condemnations and encouraged the poster "call the cops".

Ring have also filed patents to incorporate the use of facial recognition technology in the cameras that could be applied to live feeds and recorded content. If automated, facial

Suggested Citation (APA): Bridges, L. (2020, October) *Material Entanglements of Community Surveillance Networks & Infrastructural Power.* Paper presented at AoIR 2020: The 21th Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR. Retrieved from http://spir.aoir.org.

recognition on community surveillance feeds could alert law enforcement to a crime as it occurs and identify the perpetrator in real-time. Although facial recognition is not currently part of Ring's offerings, Amazon's facial recognition program, Rekognition, and other competing vendors such as Clearview AI are already being widely used by law enforcement agencies, including ICE, who once they have access to community-uploaded clips through the Neighbors app, could apply the facial recognition technology to the feeds retroactively.

Over-surveilled and Under-represented

Much important work has already been done to expose the "racializing assemblages" (Weheliye, 2014) of community-police surveillance networks and the fallibility of facial recognition technology (Benjamin, 2019; Browne, 2010, 2015; Buolamwini & Gebru, 2018). This work highlights the paradox of the white-washed machine vision, which at once enacts the hyper-surveillance of Black and Brown bodies in order to control, constrain, and codify according to the surveillant police-state, while simultaneously underrepresenting people of color in training data sets. It presents the demand for transparency in service of the control society, while serving opacity when demands are made of its services.

Joy Buolamwini calls this the "coded gaze" of artificial intelligence (AI), Ruha Benjamin (2019) says it is part of the "New Jim Code", while Simone Browne (2015) explains this as a process of digital epidermalization drawing from Fanon to explain the digital imposition of race on the body. Luke Stark (2019) has likened facial recognition to the plutonium of AI, where the "racializing effects are so potentially toxic to our lives as social beings that its widespread use doesn't outweigh the risks." There are endless examples of "data violence" (Hoffmann, 2018), which expose the racialized and gendered biases that proliferate algorithmic logics. A review of comments on the Neighbors app will quickly confirm such moments of data violence where unknowing subjects are gendered, classed, and racialized by their condemning neighbors. However, this paper seeks to move the focus away from individual actions of bigotry towards the infrastructural backbone, made up of discourses and fixtures, which not only makes these interactions possible, but actively produces systems of inequality. This paper asks, what are these community surveillance infrastructures *producing*? Who do they *serve*? And how are they materially and discursively *constructed*?

Understanding Ring as Infrastructural Power

Legal scholar, Frank Pasquale (2019), has proposed a periodization schema for AI research, where the first wave of research focused on the need to diversify data inputs to achieve more accurate outputs, while the second wave is concerned with structural forces, issues of governance, and power inequities endogenous to societies of control. In line with second wave concerns and wary of the dangers of "predatory inclusion" (Taylor, 2019), this paper argues for an critical infrastructural approach that attends to the "complex material formations that operate at multiple *scales",* recognizes

the “interconnections of media infrastructures with other systems”, addresses “*difference and uneven conditions*” which shape infrastructures, as well as the “*labor, maintenance, and repair*” required to sustain them (Parks & Starosielski, 2015).

As protests against systemic racism and police violence erupted around the United States, spurred by the murder of George Floyd and Breonna Taylor and exacerbated by the disparate effects of the global pandemic on communities of color, Amazon has *doubled* its net profit year over year to $5.2 billion since 2019 (Faulkner, 2020) and Jeff Bezos has added $87 billion to his personal fortune since January 2020 (Toh, 2020). Ring cannot be viewed in isolation of its entangled corporate owner, which relies on an ever-expanding infrastructural network, including surveillance of their highly prized package delivery service. Ring is more than individual community members installing sensors and cameras that extend beyond their properties into public spaces; it is the blurring of boundaries between police work and civilian surveillance, the reliance on obscured digital infrastructures that hide their labor and material supply chains, and expansion of Amazon’s vast infrastructural power.

Laleh Khalili (2018: 915) defines infrastructural power as an assemblage of “practices, discourses, physical fixtures, laws and procedures” with the aim of (re)producing capitalist relations. This infrastructural power relies on private tech partnerships with law enforcement, community buy-in that more surveillance will improve safety, free labor from Neighbors uploading content, discourses of fear and paranoia, a vast network of physical fixtures such as sensors and cameras willingly installed by civilians, and laws that allow warrants and other “reasonable government requests” to access recordings. If the House judicial committee hearings on antitrust give us any insight into how this market power is built and wielded, Amazon CEO Jeff Bezos said it best in an internal company email about the pending acquisition of Ring: “to be clear, my view here is that we’re buying the market position – not technology. And that market position and momentum is very valuable.”

In addition to posts on Ring’s social media app Neighbors, I reviewed over 100 product reviews on review websites Better Business Bureau (BBB), SiteJabber, Trustpilot, and Amazon’s marketplace. Both SiteJabber and Trustpilot, the two sites with star ratings, rated Ring 1.4 and 1.6 out of 5 stars respectively, while Amazon’s reviews ranged from 4.2 to 4.6 for different Ring products. The complaints shared a number of common themes including issues with connectivity, instances of hacking, and feelings of “bait and switch” where users could not access their recordings without signing up for expensive on-going subscriptions called “protection plans”, all of which provide ample evidence on how Amazon’s infrastructural power negatively affects customers.

Looking vertically into Ring’s supply-chain you’ll find familiar OEM’s like Foxconn, a Taiwanese manufacturer, who are infamous for the exploitative and abusive labor practices (Condliffe, 2018). These oppressive labor regimes are reproduced throughout the Amazon supply-chain seen in their staunch opposition to labor unions and crackdown on whistle-blowers (Palmer, 2020), the dangerous conditions in warehouses and fulfilment centers (Heater, 2020), and their restrictive non-compete clauses, which many have argued rob workers the right to practice

their trade where they want (Jaret & Vaheesan, 2019; Novet, 2020; Vaheesan, 2018).

This paper aims to highlight the complex human and non-human entanglements that constitute community surveillance networks in order to move towards an infrastructural understanding of Ring products so that we may more effectively evaluate the social and material costs of such systems. This analysis reveals how each node in the supply-chain network is entangled with histories of settler-colonialism, racialization and gendered inequities. Bolstered by developments in cloud computing, concealing the human and nonhuman supply-chains, these systems are never detached from material inputs; rather, they are embedded in vast infrastructural systems and complex transnational supply chains powered by logics of extraction, circulation and accumulation of capital. Further research is crucially needed to understand the *political* ramifications of such private infrastructures that are taking on increasingly central roles in public governance, policing, and community networks.

References

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity.

Browne, S. (2010). Digital Epidermalization: Race, Identity and Biometrics. *Critical Sociology*, *36*(1), 131–150. https://doi.org/10.1177/0896920509347144

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Machine Learning Research*, *81*, 1–15. https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/

Cericola, R. (2020, February 14). Ring Neighbors Is the Best and Worst Neighborhood Watch App. *New York Times*. https://thewirecutter.com/blog/ring-neighbors-app-review/

Chun, W. H. K. (2009). Introduction: Race and/as Technology; or, How to Do Things to Race. *Camera Obscura: Feminism, Culture, and Media Studies*, *24*(1), 7–35. https://doi.org/10.1215/02705346-2008-013

Condliffe, J. (2018, June 11). Foxconn Is Under Scrutiny for Worker Conditions. It's Not the First Time. *The New York Times*. https://www.nytimes.com/2018/06/11/business/dealbook/foxconn-worker-conditions.html

Faulkner, C. (2020, July 30). *Amazon doubled its profit during a pandemic*. The Verge. https://www.theverge.com/2020/7/30/21348368/amazon-q2-2020-earnings-covid-19-coronavirus-jeff-bezos

Gilliard, C. (2020, January 9). Caught in the Spotlight. *Urban Omnibus*. https://urbanomnibus.net/2020/01/caught-in-the-spotlight/

Heater, B. (2020, May 22). An eighth Amazon warehouse employee has died from COVID-19. *TechCrunch*. https://social.techcrunch.com/2020/05/22/an-eighth-amazon-warehouse-employee-has-died-from-covid-19/

Hoffmann, A. L. (2018, April 30). *Data Violence and How Bad Engineering Choices Can Damage Society*. Medium. https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4

Jaret, A., & Vaheesan, S. (2019, December 19). Non-Compete Clauses Are Suffocating American Workers. *Time*. https://time.com/5753078/non-compete-clauses-american-workers/

Justice, A. E. for C. (2020, February 19). Amazon Employees Share Our Views on Company Business. *Medium*. https://medium.com/@amazonemployeesclimatejustice/amazon-employees-share-our-views-on-company-business-f5abcdea849

Kurwa, R. (2019). Building the Digitally Gated Community: The Case of Nextdoor. *Surveillance & Society*, *17*(1/2), 111–117. https://doi.org/10.24908/ss.v17i1/2.12927

Neighbors by Ring—Apps on Google Play. (n.d.). Retrieved March 2, 2020, from https://play.google.com/store/apps/details?id=com.ring.neighborhoods&hl=en_US

Novet, J. (2020, June 11). *Amazon is suing a cloud employee who left for Google, rekindling the debate over non-compete agreements*. CNBC. https://www.cnbc.com/2020/06/11/aws-case-against-worker-who-joined-google-reignites-non-compete-debate.html

Palmer, A. (2020, May 4). *Amazon engineer quits after he "snapped" when the company fired workers who called for coronavirus protections*. CNBC. https://www.cnbc.com/2020/05/04/amazon-engineer-resigns-over-companys-treatment-of-workers.html

Parks, L., & Starosielski, N. (Eds.). (2015). *Signal traffic: Critical studies of media infrastructures*. University of Illinois Press.

Pasquale, F. (2019, November 25). The Second Wave of Algorithmic Accountability. *Law and Political Economy*. https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/

Stanley, J. (2019, September 10). *Should You Buy a Ring Doorbell Camera?* American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/should-you-buy-ring-doorbell-camera

Stark, L. (2019, April). *Facial recognition is the plutonium of AI*. XRDS, an ACM Publication. https://xrds.acm.org/article.cfm?aid=3313129

Taylor, K.-Y. (2019). Predatory Inclusion. *N+1*, *Fall*(35). https://nplusonemag.com/issue-35/essays/predatory-inclusion/

Toh, M. (2020, August 27). *Jeff Bezos is now worth a whopping $200 billion*. CNN. https://www.cnn.com/2020/08/27/tech/jeff-bezos-net-worth-200-billion-intl-hnk/index.html

Vaheesan, S. (2018, July 19). How Contemporary Antitrust Robs Workers of Power. *LPE Project*. https://lpeproject.org/blog/how-contemporary-antitrust-robs-workers-of-power/

Weheliye, A. G. (2014). *Habeas viscus: Racializing assemblages, biopolitics, and black feminist theories of the human*. Duke University Press.

Wolfe, E., & Ries, B. (n.d.). *A hacker accessed a family's Ring security camera and told their 8-year-old daughter he was Santa Claus*. CNN. Retrieved March 2, 2020, from https://www.cnn.com/2019/12/12/tech/ring-security-camera-hacker-harassed-girl-trnd/index.html

Suggested Citation (APA): Bridges, L. (2020, October 27-31). *Material Entanglements of Community Surveillance Networks and Infrastructural Power*. Paper presented at AoIR 2020: The 21st Annual Conference of the Association of Internet Researchers. AoIR. Retrieved from http://spir.aoir.org.