Selected Papers of #AoIR2025:
The 26th Annual Conference of the
Association of Internet Researchers
Niterói, Brazil / 15 – 18 Oct 2025

"A NETWORK OF COLLABORATIVE INTELLIGENCE": THE PLATFORMIZATION OF COMMUNITY ALGORITHMIC SURVEILLANCE

Meg Kitamura
University of Amsterdam

Gabriel Pereira
University of Amsterdam

Introduction

Garret Langley made a fortune by selling his vehicle subscription startup called Clutch. Later, in 2017, when Langley's car was stolen, he saw an opportunity: could he apply the lessons from his previous ventures in web-based services to public safety? That's how, according to him, Flock Safety emerged: the company offers a platform for surveillance-as-a-service, most notably installing Automated License Plate Recognition cameras to "empower your law enforcement agency to solve crime fast" (Flock, n.d.). Over the years, Flock made a name for itself by selling not just to police agencies, but notably directly to Homeowners Associations (known as gated communities), now responsible for around 40% of the company's revenue (Steirn, 2023).

This paper examines a crucial yet under examined layer through which platform logics are being embedded: community surveillance. We explore how two different startups (Flock and Gabriel) are *directly involving communities* in the infrastructuring of algorithmic surveillance. Such communities are made into direct collaborators, generating data to be used by communities themselves as well as other police actors. Ultimately, as we argue, community embeddedness shifts control over algorithmic surveillance from the state toward private platform logics.

Platformizing algorithmic surveillance

Internet researchers have investigated social media platforms' shift towards architectures of standardized programmability, modularity, and integration (Plantin et al., 2018; van Dijck et al., 2018)—see e.g. Anne Helmond's (2015) study on the development of Facebook's API. The shift went beyond social media, with platforms being defined by Poell et al. as "data infrastructures that facilitate, aggregate, monetize, and govern interactions between end-users and content and service providers" (2022,

Suggested Citation (APA): Kitamura, M., & Pereira, G. (2025, October). *"A Network Of Collaborative Intelligence": The Platformization Of Community Algorithmic Surveillance*. Paper presented at AoIR2025: The 26th Annual Conference of the Association of Internet Researchers. Niterói, BR: AoIR. Retrieved from http://spir.aoir.org.

p. 5). The process of platformization penetrated and reshaped many realms, including surveillance (Gates, 2019; Murakami Wood & Monahan, 2019), e.g. through surveillance-as-a-service (see e.g. West, 2019).

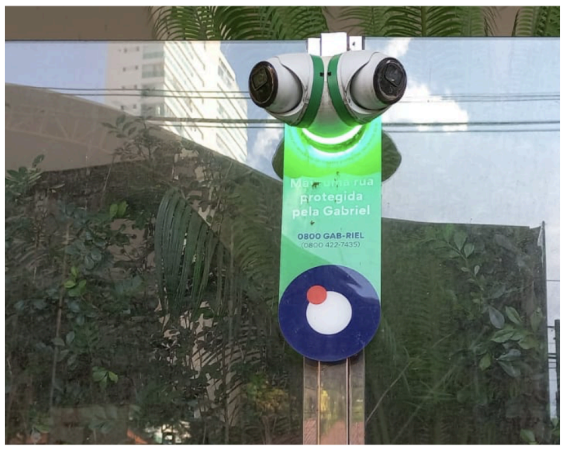
The platformization of surveillance has been studied across two different levels: First, scholars have discussed how the work of police and law enforcement has become reliant on “manifold data sets and databanks” that are “designed to improve police work on numerous levels by facilitating knowledge creation” (Egbert, 2019, p.84). Work in this field evidenced how companies sell data infrastructures to cities or states, e.g. Palantir (Galis & Karlsson, 2024; Iliadis & Acker, 2022). Second, work has shown how citizens and companies have included platform surveillance in their everyday practices, for example through workplace surveillance (Andrejevic, 2024; Levy, 2023) or Ring doorbell cameras (Bridges, 2021). Our work here proposes a new layer, by centering on the role played by community self-organization.

Methodology: Two platforms

This paper builds upon the close analysis of Flock and Gabriel, two distinct startup platforms that market algorithmic surveillance platforms—systems for automated data surveillance, including license plate recognition and other smart cameras (Pereira & Raetzsch, 2022). Flock, founded in 2017, operates exclusively in the USA—where it is present in over 4000 cities and expanding quickly. Gabriel was founded in 2020, operates exclusively in Brazil, and has also seen great expansion—in 2021, it received ca. 11 million US Dollars investment by the SoftBank Group (Martins, 2021). We have chosen to analyze these companies due to their similar approach in developing platform surveillance solutions as well as their rapid growth.

We deployed a mixed-methods approach to study these companies and their data infrastructures. First, we conducted extensive analysis of the startups’ publicly-available material, including their websites, policies, and other documents made available to communities. Second, we conducted fieldwork to investigate the materiality of their data infrastructures (Parks, 2015)—e.g. mapping cameras, the APIs used for transparency, but also attending policing/traffic conferences. Finally, within the realm of a larger project, we interviewed over 30 people working in algorithmic surveillance—including company representatives, regulators, journalists, and activists in this field. For this paper we used situational analysis (Clarke, 2003) to collaboratively analyze the data on community participation in platform surveillance.

Figs. 1 and 2 — On the left, a Flock license plate recognition camera installed in an intersection in Tukwila (Washington, USA). The camera is powered by a solar panel next to it. On the right, Flock's motto in a trade show indicates its community-oriented mission (“together”).



Figs. 3 and 4 — On the left, a Gabriel smart camera pole installed on the curb of a residential building in São Paulo (Brazil). On the right, a close-up of Gabriel smart cameras installed on a building's wall, with ostensive branding of the platform (“One more street protected by Gabriel”) and contact information.

Community empowerment through platform self-organization

Whereas other surveillance platforms are exclusively sold directly to police departments, the two startups rely on direct contact with communities to establish their platform for algorithmic surveillance in neighborhoods. This shift towards self-organization fits with “seeing cities like a platform”, as analyzed by Törnberg & Uitermark (2025, p. 44), as it “means that the government itself does not dictate what happens but instead facilitates urbanites to participate and take initiative.” These platforms thrive under such promise of bottom-up and community-driven security.

The companies adopt a Business to Consumer (B2C) positioning, including intensive campaigns of recruitment. The service is presented as a way to empower communities for their own safety—e.g., Gabriel proposes that “the safety of your neighborhood also depends on you” (Gabriel, n.d.). Both companies carefully position “privacy” and “transparency” as values. Flock, for example, touts its “Transparency Portals”, which offer a curated overview of the data infrastructure and its data sharing with other actors.

Platform integration, including with law enforcement

The data infrastructure of Flock and Gabriel's surveillance is intrinsically tied to platform logics and its architectures of integration. When privately-run platforms become a *mediator* of surveillance they act as *data infrastructures* that facilitate and govern the flow of data. The data generated by the algorithmic surveillance in communities travels upwards to differing layers of law enforcement but also laterally across neighborhoods/police departments. Gabriel (n.d.) terms this “a network of collaborative intelligence”, whereby community members protect their homes while also “helping to build the Protection Area in [their] region.” The key offering of the companies, therefore, is the *integration* of data sources from communities through the platform's infrastructure—marking a difference from legacy systems of neighborhood CCTV cameras (see Firmino & Duarte, 2016).

These platforms make collaboration between communities *and* with the police an implicit—but unavoidable—aspect of their data infrastructure. This is evident in how they explain the use-value of their technology to consumers. Flock, for example, guarantees improved neighborhood safety by “capturing actionable evidence police can use to investigate crimes in the area” (Flock. n.d.) while Gabriel promises sending automated alerts to police when a crime is detected. Bottom-up community surveillance is thus directly integrated through data infrastructures with the surveillance state. These companies are different, for example, from Ring doorbell cameras, which operate at the *individual-level* but *may* become integrated through Amazon's app (Bridges, 2020; 2021).

Ultimately, the communities’ adoption of platform surveillance fuels the capabilities of law enforcement to expand its *access*—but not full control over—algorithmic surveillance data. Moreover, despite the startups' B2C positioning indicating the security needs of the community are prioritized, there is a vast power imbalance: communities themselves are only *subscribers to a service*, and also do not fully govern/control how the platform is used.

Conclusion

The paper contributes to critical data studies with an empirical exploration of community participation in the platformization of algorithmic surveillance. The startups analyzed, Flock and Gabriel, rely on the active participation of self-organized communities, rather than the direct intervention of the state. The companies adopt a B2C positioning and promise community empowerment in order to expand their surveillance network. The private platforms build and operate the expansion of algorithmic surveillance infrastructures, taking this role from the state. The consequences of this shift raise crucial questions around how platform logics are reshaping surveillance practices and, thus, renewing power imbalances.

References

Andrejevic, M. (2024). Automated monitoring in the workplace: the devolution of recognition. International Journal of Communication, 18, 3205-3211. https://ijoc.org/index.php/ijoc/article/view/23368/4669

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.

Bridges, L. (2021). Infrastructural obfuscation: Unpacking the carceral logics of the ring surveillant assemblage. Information, Communication & Society, 24(6), 830–849. https://doi.org/10.1080/1369118x.2021.1909097

Clarke, A. E. (2003). Situational analyses: Grounded Theory Mapping after the postmodern turn. Symbolic Interaction, 26(4), 553–576. https://doi.org/10.1525/si.2003.26.4.553

Egbert, S. (2019). Predictive policing and the platformization of police work. Surveillance & Society, 17(1/2), 83–88. https://doi.org/10.24908/ss.v17i1/2.12920

Firmino, R., & Duarte, F. (2015). Private video monitoring of public spaces: The construction of New Invisible Territories. Urban Studies, 53(4), 741–754. https://doi.org/10.1177/0042098014567064

Flock Safety. (n.d.). Safety for every situation. https://www.flocksafety.com/

Gabriel. (n.d.). https://gabriel.com.br/

Galis, V., & Karlsson, B. (2024). A world of Palantir – ontological politics in the Danish police's pol-intel. Information, Communication & Society, 27(13), 2438–2456. https://doi.org/10.1080/1369118x.2024.2410255

Gates, K. (2019). Policing as digital platform. Surveillance & Society, 17(1/2), 63–68. https://doi.org/10.24908/ss.v17i1/2.12940

Helmond, A. (2015). The platformization of the web: Making web data platform ready. Social Media + Society, 1(2). https://doi.org/10.1177/2056305115603080

Iliadis, A., & Acker, A. (2022). The seer and the seen: Surveying Palantir's surveillance platform. The Information Society, 38(5), 334–363. https://doi.org/10.1080/01972243.2022.2100851

Kevy, K. (2023). Data Driven: Truckers, technology, and the new workplace surveillance. Princeton University Press.

Martins, A. (2021). Gabriel, startup de segurança, capta R$ 66 milhões em rodada com Softbank. Exame. https://exame.com/pme/gabriel-startup-de-seguranca-capta-r-66-milhoes-em-rodada-com-softbank/

Murakami Wood, D., & Monahan, T. (2019a). Editorial: Platform surveillance. Surveillance & Society, 17(1/2), 1–6. https://doi.org/10.24908/ss.v17i1/2.13237

Parks, L. (2015). "Stuff you can kick": Toward a theory of media infrastructures. Between Humanities and the Digital, 355–374. https://doi.org/10.7551/mitpress/9465.003.0031

Pereira, G., & Raetzsch, C. (2022). From banal surveillance to function creep: Automated License Plate Recognition (ALPR) in Denmark. Surveillance & Society, 20(3), 265–280. https://doi.org/10.24908/ss.v20i3.15000

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2016). Infrastructure Studies Meet Platform Studies in the age of google and facebook. New Media & Society, 20(1), 293–310. https://doi.org/10.1177/1461444816661553

Rudnicka-Lavoie, D., Poell, T., & Duffy, B. E. (2022). Platforms and cultural production. Canadian Journal of Communication, 47(4), 800–803. https://doi.org/10.3138/cjc.2022-0042

Steirn, J. (2023). Report: Flock Safety Business Breakdown & Founding Story. Contrary Research. https://research.contrary.com/company/flock-safety

Törnberg, P., & Uitermark, J. (2025). Seeing like a platform: An inquiry into the condition of Digital Modernity. Taylor & Francis Group.

van Dijck, J., Poell, T., & de Waal, M. (2018). The Platform Society. Oxford Scholarship Online. https://doi.org/10.1093/oso/9780190889760.001.0001

West, E. (2019). Amazon: Surveillance as a Service. Surveillance & Society, 17(1/2), 27–33. https://doi.org/10.24908/ss.v17i1/2.13008