Surveillance & Society

Dialogue

The Ontological Shift in Surveillance: Revisiting the "Surveillant Assemblage" in the Age of Facial Recognition

Marie Eneman

University of Gothenburg, Sweden
marie.eneman@gu.se

Jan Ljungberg

University of Gothenburg, Sweden
jan.ljungberg@ait.gu.se

Diana Miranda

University of Stirling, UK
diana.miranda@stir.ac.uk

Lachlan Urquhart

University of Edinburgh, UK
lachlan.urquhart@ed.ac.uk

William Webster

University of Stirling, UK
william.webster@stir.ac.uk

Introduction

It has been twenty-five years since Haggerty and Ericson's (2000) influential work on the "surveillant assemblage" was published. Building on Deleuze and Guattari (1987), their work challenged the dominance of earlier surveillance metaphors such as Orwell's "Big Brother" and Foucault's panopticon, arguing that these frameworks failed to capture the emergent, decentralised, and rhizomatic qualities of contemporary surveillance systems. Instead of hierarchical observation, Haggerty and Ericson (2000: 605) described a dynamic assemblage as a "convergence of once discrete surveillance systems." This foregrounded the dispersal, hybridity, and institutional heterogeneity of modern forms of control. Yet, since then, the surveillance landscape has evolved significantly, including through the adoption of facial recognition technologies in law enforcement, powered by advanced artificial intelligence (AI) processing (Eneman et al. 2022; Fussey and Murray 2025; Urquhart and Miranda 2021). Police forces in England and Wales have already deployed live facial recognition (LFR), while Sweden prepares to authorise police use from January 2026. Globally, LFR is spreading across the US, Latin America, Asia, and Africa, yet evidence from the UK and US shows that it can lead to false matches, wrongful interventions, and human rights violations (Dauvergne 2022; Fussey and Murray 2025)

Eneman, Marie, Jan Ljungberg, Diana Miranda, Lachlan Urquhart, and William Webster. 2025. The Ontological Shift in Surveillance: Revisiting the "Surveillant Assemblage" in the Age of Facial Recognition. *Surveillance & Society* 23 (4): 505-510.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

Contemporary surveillance systems operate through distributed infrastructures, probabilistic logic, and real-time biometric processing (Amoore et al. 2024). We argue that the concept of the surveillant assemblage has entered a new phase characterised by both *heightened complexity* and a fundamental *ontological shift* in how surveillance operates through approximation. Earlier surveillance regimes primarily functioned through representation, constructing *data doubles* as identifiable proxies of individuals across institutional domains. In contrast, contemporary AI-driven systems, such as LFR, increasingly operate through approximation, whereby algorithmically constructed models assess probabilistic resemblance rather than identity (Amoore 2020). This shift is not merely technical but deeply epistemological and political. The approximations generated by these systems are grounded in algorithmic architectures that are frequently opaque, even to those who design or deploy them (Eneman and Ljungberg 2025; Pasquale 2016). As a result, surveillance practices no longer simply aim to recognise subjects, but to infer their statistical proximity to risk categories embedded in machine learning infrastructures (Amoore 2020). This extends Lyon's (2003) early recognition that surveillance increasingly functions by sorting individuals into risk-based categories rather than identifying them as unique persons. Social sorting demonstrated how people were treated as data profiles representing broader social or behavioural types. Following Bowker and Star (1999), such classification is not merely technical but infrastructural and political, embedding assumptions about whose risks matter and whose identities are made actionable. This shift marks a precursor to today's logic of approximation, where governance operates through statistical resemblance. In addition to Amoore's (2020) concept of biometric approximation, Pasquale's (2016) critique of opaque black-box algorithms and Kitchin et al.'s (2025) critical studies of algorithms have enriched our understanding of how contemporary surveillance operates by approximation rather than representation.

The surveillant assemblage remains a valuable lens for understanding today's surveillance landscape, now characterized more by biometric approximation. Yet while Ghantous (in this issue) underscores how assemblages operate through colonial violence and frictions, we argue that the concept's analytical core, its representational logic, requires critical rethinking under algorithmic governance. It is pertinent to ask: does the era of algorithmic governance require not merely theoretical refinement but also a more profound rethinking of surveillance's ontological and epistemological foundations to account for the generative, performative, predictive, and ontologically destabilizing logic behind algorithmic governance? To critically examine the surveillant assemblage, we revisit two elements considering their relevance in relation to contemporary LFR in policing: *data doubles* and *rhizomatic surveillance*.

Data Doubles

Haggerty and Ericson (2000) described a process where bodies are abstracted from their territorial contexts, deconstructed into data flows, and recomposed as virtual "data doubles," i.e., fragments drawn from disparate databases and institutional records. These virtual representations enable forms of indirect control and risk management but are largely retrospective and passive in character. In contrast, LFR in policing illustrates how data doubles are no longer merely informational composites, as they have become active, real-time entities that trigger immediate intervention. The data double ceases to function solely as a representation. Instead, it becomes a technical agent of governance, initiating alerts, structuring responses, and as noted by Miranda (2024), even shaping power structures for rendering bodies visible or actionable.

Haggerty and Ericson (2000) captured a critical perspective on how individuals are rendered visible through informational assemblages. Their focus was largely on fragmented, institutional flows of data that rendered subjects knowable at a distance. What was once considered a digital representation has now become an integral component of an individual's very existence, shaping the interventionist nature of contemporary biometric systems. According to Kitchin (2017) and Amoore (2020). data does not merely describe *who* we are but actively constitutes *what* we are. As Suchman (1994) early reminded us, categories themselves have politics: classificatory practices do not neutrally label but enact realities by shaping what actions and

responses become possible. In LFR, these categories are materialised through probabilistic thresholds that trigger intervention.

The data double was originally framed as a tool of governance in the hands of institutions, but more recent work highlights how these digital constructs actively shape subjectivity and social reality. Amoore (2020) argues that algorithmic systems are not merely descriptive but ethicopolitical, enacting subject positions through probabilistic logics of risk and approximation. Kitchin (2017) and Kitchin et al. (2025) similarly contend that algorithmic systems do not represent the world objectively, but construct it operationally, generating actionable inferences that shape governance and control. This shift is not only technical but ontological: the boundary between the individual and their data becomes increasingly blurred. Nissenbaum's (2009) concept of contextual integrity underscores how informational flows can undermine autonomy when abstracted from their social and ethical contexts, while Coeckelbergh (2024) emphasises that AI technologies reshape how moral and political personhood is constituted in the digital age. Together, these perspectives point to a profound transformation in how identity, agency, and accountability are enacted through data.

Whereas Haggerty and Ericson (2000) focused on how the body is abstracted from its territorial context and rendered as information for the purposes of surveillance, Amoore (2020) emphasises how this information becomes operationalised within the individual's identity and social agency. In this light, the data double is not merely an object of institutional control, but an ethical and existential concern, raising profound questions about autonomy, dignity, and rights. Miranda (2024) invites us to think about how contemporary biometric systems may be contributing to a reshaping of subjectivity, where the datafied body no longer merely represents the individual, but increasingly becomes a site through which power is exercised and governance enacted. As surveillant assemblages grow in complexity, the normative frameworks governing and regulating their operation often become increasingly opaque (Black and Murray 2019). The integration of AI further amplifies this challenge, introducing new demands for effective and adaptive regulatory responses (Murray 2021). This opacity raises critical questions around accountability, particularly in cases where individuals are subject to harm due to false positives or biased approximations. As stated by Abbey and Akbari (in this issue): "we [must] recognise that different bodies have complex, uneven experiences of living under surveillance... [in particular] specific racialised, classed, gendered, sexualised, and disabled bodies."

The data double remains foundational but its analytical utility needs refinement to respond to AI surveillance like LFR. Its retrospective and representational orientation needs to be supplemented by a more dynamic, relational, and ethically attuned account of how data doubles now operate through approximation, probabilistic judgement, and automated governance (Amoore 2020; Pasquale 2016). Given this development, the data double should no longer be seen merely as a static representation of the individual within institutional spaces, but as a dynamic, operative construct that participates in decision-making processes and actively mediates access, suspicion, and response. It raises urgent questions concerning agency, autonomy, and accountability in our contemporary society where surveillance identifies, targets, anticipates and acts, often opaquely and without recourse (Coeckelbergh 2024; Kitchin 2017).

As data doubles are increasingly embedded in algorithmic systems that act in predictive and performative ways, the metaphor risks obscuring more than it reveals. Several scholars argue (Amoore et al. 2024; Kitchin 2017; Kitchin et al. 2025; Suchman 1994) that such systems must be understood not merely as technical artefacts, but as socio-technical constructs with cultural, political, and ethical dimensions. Against this development, revisiting the data double becomes essential, not to discard the concept, but to better refine it with the logics of approximation, automation, and operational agency that define contemporary surveillance. Together, these perspectives point to a profound transformation in how identity, agency, and accountability are enacted through data.

Rhizomatic Surveillance

The notion of rhizomatic surveillance is used to describe how surveillance expands laterally and unpredictably across institutional and technological contexts. Surveillance, even then, did not originate from a single point of control but proliferated through diffuse and decentralised connections, forming an assemblage whose constituent parts and boundaries were already difficult to map, define, regulate, or dismantle. The rhizome metaphor articulates the core features of the surveillance assemblage: "its phenomenal growth through expanding uses, and its levelling effect on hierarchies" (Haggerty and Ericson 2000: 614). It was precisely this decentralised, unstructured nature that made the surveillant assemblage so compelling and elusive. However, assemblage theory ranges from the perspective of an assemblage as a boundless collection of heterogeneous objects in interaction, to the notion of something that has (clearer) boundaries and is arranged to fulfil a particular purpose or desire. Thus, the rhizome is in itself not an assemblage, but rather a space within which assemblages may emerge.

Today the digitalization of society with notions of platformization and datafication further strengthens the rhizomatic nature of the surveillant assemblage. Platformization describes the expanded reach that major platforms achieve through generativity and convergence (Nieborg and Poell 2018), while datafication constitutes what Zuboff (2019) calls surveillance capitalism, where surveillance has become the core of the digital platform's business model. This means that an extensive digital infrastructure with global reach handles large volumes of data points related to every citizen, in real time algorithmically metrified into approximations and predictions of human behaviour. This surveillant infrastructure is messy and ill-defined with ever shifting relationships between public and private infrastructures and institutions (e.g., police, banks, social media, retail stores, and even individuals with smartphones). Despite its distribution and fragmentation, this digital infrastructure increases the power of central control for certain actors (i.e., the platform corporations). In such platformised environments, classificatory schemes themselves travel as part of the infrastructure (Bowker and Star 1999), quietly coordinating and constraining possibilities for action at scale. LFR systems, particularly when used in policing, can be introduced with limited transparency or democratic oversight and are also increasingly entangled in commercial logics (Ball and Webster 2018). Rather than drifting assemblages, these systems materialise as socio-technical-commercial assemblages embedded in infrastructures of assemblage, i.e., centralised, proprietary architectures often governed by private actors. These actors not only design and develop but also maintain and govern access, enacting assemblages of governance that displace accountability and authority from public oversight into opaque techno-commercial domains. The result is not a loose constellation but a structured ordering with profound ethical and political consequences.

While the technological infrastructure of facial recognition may still rely on several, interlinked systems with cameras, biometric databases, and mobile platforms, its application is increasingly guided by centralised, goal-oriented mandates often based on the desire of enhanced effectiveness and public safety (Fussey, Davies, and Innes 2021). In this sense, the rhizomatic logic of surveillance has been partially *reterritorialized*—i.e., channelled into operational frameworks, institutional and supranational hierarchies, and legal structures. So this metaphor must also be renegotiated in light of the institutional and supranational consolidation, as well as legal oversight with implications for accountability and legitimacy surrounding LFR. The assemblage remains distributed in form but is increasingly governed and regulated in function, raising questions about whether the rhizome metaphor still captures the dynamics of contemporary algorithmic policing? As questioned by Hier (in this issue): "is it time to tear down the walls (or dig up the rhizomes and shoots?) of the assemblage as one of the leading metaphors in surveillance studies?" Yet others, drawing more directly on Deleuze and Guattari (1987), may argue that assemblages can equally encompass hierarchical power, suggesting the concept retains analytical value even under AI-driven reterritorialisation.

From Representation to Approximation: Facial Recognition and the Ontological Shift in Surveillance

The deployment of biometric technologies such as LFR constitutes a profound shift in surveillance, marking a transition from representative identification to algorithmic approximation (Amoore 2020; Amoore et al. 2024; Fussey and Murray 2025). These systems do not verify identities in any absolute sense but instead generate biometric approximations, i.e., probabilistic inferences derived from similarity thresholds computed by opaque algorithmic models. A match does not confirm who someone *is*, but rather how closely their facial data resembles a reference image stored in a database. This represents a notable difference from the *data double*, which implied a relatively stable correspondence between the subject and its digital proxy. In contrast, contemporary algorithmic surveillance regimes no longer seek to recognise individuals as coherent identities, but instead operate through probabilistic thresholds, treating resemblance as actionable risk. Identity, suspicion, and intervention thus become collapsed into automated inference.

The shift from representation to approximation also entails a fundamental transformation in how knowledge is produced and operationalized within surveillance systems (Amoore 2020; Fussey, Davies, and Innes 2021). Decisions are no longer grounded in certainty but in probability, reshaping what is accepted as valid knowledge within policing and legal contexts. Most significantly, epistemic authority is displaced from human judgement to algorithmic systems, whose internal logics of resemblance and risk often remain opaque and unaccountable (Murray 2021). In this epistemic transformation, surveillance no longer relies on observing and categorising known identities, but on calculating likeness and projecting risk. This marks not only a shift in surveillance's technological form but also a deeper ontological and epistemological realignment from recognition to speculation, from evidence to approximation, from subject to statistical proxy (Amoore et al. 2024).

In the original notion of surveillant assemblage, the subject was fragmented into discrete data flows, reassembled as a digital double, and subjected to monitoring. Today, biometric approximation supersedes full representation. Control no longer hinges on the accumulation of total data, but on statistical proximity to a risk model. The result is automated suspicion, interventions triggered not by confirmed identity, but by algorithmic similarity (Fussey and Murray 2025). When LFR flags an individual, this may prompt police intervention, stopping, questioning, or detention based not on who the person is, but on the likelihood of who they might be. Who determines what degrees of resemblance warrant intervention? This shift is both epistemologically opaque and ontologically destabilising: surveillance no longer observes discrete individuals, but tracks statistical patterns, thereby raising urgent normative concerns. The normalisation of error margins, the erosion of singular personhood, and the diminishing of accountability (Amoore 2020; Amoore et al. 2024) threaten foundational principles such as civil liberties and legal certainty. As argued by Lageson (in this issue): "machine learning models are designed to identify patterns, not to ensure fairness or accuracy."

By shifting the analytic focus from representation to approximation, and from data doubles to biometric resemblance, we contribute to critical debates on the surveillant assemblage. Has the shift from representation to approximation rendered its foundational assumptions, particularly its representational logic, obsolete? Does the era of algorithmic governance require not merely theoretical refinement but also a more radical rethinking of surveillance's ontological and epistemological foundations? Surveillance today no longer simply visualises and classifies; it infers, predicts, and intervenes based on statistical resemblance. This development calls not only for conceptual refinement, but for a deeper political reckoning with how surveillance, agency, and governance are being rearticulated in the algorithmic age, challenging the very grounds of democratic oversight and accountability (Black and Murray 2019; Murray 2021).

The line of argument here raises a series of questions for further reflection, including:

- Does the surveillant assemblage still provide a sufficient lens for understanding contemporary surveillance systems such as LFR, or has it reached its analytical limits?

- What has become of the *rhizomatic* nature of the surveillant assemblage when a decentralised surveillance infrastructure is re-anchored in centralised, opaque, and commercially governed algorithmic systems?

- How do we theorise democratic oversight when algorithmic governance operates through prediction and opacity, beyond established mechanisms of political accountability?

- What happens to legal certainty when the subject is reduced to a biometric approximation rather than recognised as a rights-bearing individual?

- Are our institutions prepared to regulate a predictive, probabilistic ontology of governance?

References

Abbey, Matthew, and Azadeh Akbari. 2025. A Critique of Surveillant Assemblage: Bodies, Desire, and the Limits of the Data Double. *Surveillance & Society* 23 (4): 511–517.

Amoore, Louise. 2020. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, NC: Duke University Press.

Amoore, Louise, Alexander Campolo, Benjamen Jacobsen, and Ludovico Rella. 2024. A World Model: On the Political Logics o Generative AI. *Political Geography* 113: https://doi.org/10.1016/j.polgeo.2024.103134.

Ball, Kirstie, and William Webster. 2018. *Surveillance and Democracy in Europe*. London: Routledge.

Black, Julia, and Andrew Murray. 2019. Regulating AI and Machine Learning: Setting the Regulatory Agenda. *European Journal of Law and Technology* 10 (3): 1–21.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out: Classification and Its Consequences.* Cambridge, MA: MIT Press.

Coeckelbergh, Mark. 2024. *Why AI Undermines Democracy and What to Do About It.* London: Polity Press.

Dauvergne, Pete. 2022. Facial Recognition Technology for Policing and Surveillance in the Global South: A Call for Bans. *Third World Quarterly* 43 (9): 2325–2335.

Deleuze, Gilles, and Félix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia*. Translated by Brian Massumi. Minneapolis, MN: University of Minnesota Press.

Eneman, Marie, and Jan Ljungberg. 2025. AI and Governance Dilemmas for Law Enforcement Agencies. In *Leading Digital Transformation: Management, Governance and Control*, edited by Einar Iveroth, Jan Lindvall, and Johan Magnusson, 259–271. London: Routledge.

Eneman, Marie, Jan Ljungberg, Elena Raviola, and Bertil Rolandsson. 2022. The Sensitive Nature of Facial Recognition: Tensions Between the Swedish Police and Regulatory Authorities. *Information Polity* 27 (2): 219–232.

Fussey, Pete, and Daragh Murray. 2025. *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence*. Oxford, UK: Oxford University Press.

Fussey, Pete, Bethan Davies, and Martin Innes. 2021. "Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing. *The British Journal of Criminology* 61 (2): 325–344.

Ghantous, Wassim. 2025. Rethinking the Surveillant Assemblage in Palestine: Racialization, Friction, Speed. *Surveillance & Society* 23 (4): 505–510.

Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *The British Journal of Sociology* 51 (4): 605–622.

Hier, Sean P. 2025. From Surveillant Assemblage to Surveillance Culture: Shifting Metaphors in Surveillance Studies. *Surveillance & Society* 23 (4): 524–528.

Kitchin, Rob. 2017. Thinking Critically About and Researching Algorithms. *Information, Communication & Society* 20 (1): 14–29.

Kitchin, Rob, João Davret, Cecilia Maria Kayanan, and Stephen Mutter. 2025. Data Mobilities: Rethinking the Movement and Circulation of Digital Data. *Mobilities* 20 (1): 1–19.

Lageson, Sarah. 2025. The Artificially Unintelligent Data Double. *Surveillance & Society* 23 (4): 491–497.

Lyon, David. 2003. *Surveillance as Social Sorting : Privacy, Risk, and Digital Discrimination*. London: Routledge.

Miranda, Diana. 2024. Carceral Surveillance: Data Flows Within and Beyond Prison Walls. *Incarceration* 5: https://doi.org/10.1177/26326663241237966.

Murray, Andrew. 2021. *Almost Human: Law and Human Agency in the Time of Artificial Intelligence.* The Hague, NL: T.M.C. Asser Press.
Nieborg, David, and Thomas Poell. 2018. The Platformization of Cultural Production: Theorizing the Contingent Cultural Commodity. *New Media & Society* 20 (11): 4275–4292.
Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CT: Stanford University Press.
Pasquale, Frank. 2016. *The Black Box Society*. Cambrdige, MA: Harvard University Press.
Suchman, Lucy. 1994. Do Categories Have Politics? The Language/Action Perspective Reconsidered. *Computer Supported Cooperative Work (CSCW*) 2 (3): 177–190.
Urquhart, Lachlan, and Diana Miranda. 2021. Policing Faces: The Present and Future of Intelligent Facial Surveillance. *Information & Communications Technology Law* 31 (2): 194–219.
Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. London: Profile Books.