



REVISITING AGAMBEN'S HOMO SACER IN THE AGE OF SURVEILLANCE AND DIGITAL CONTROL

Manas M S

Research Scholar, Department of Philosophy, University of Kerala

Abstract

Giorgio Agamben's *Homo Sacer: Sovereign Power and Bare Life* (1998) remains one of the most influential contributions to biopolitical theory since Michel Foucault. Written prior to the mass diffusion of networked digital technologies, Agamben's vocabulary of bare life, sovereign exception, and the camp nevertheless offers a productive framework for interpreting contemporary regimes of digital surveillance and algorithmic governance. This article revisits Agamben's central concepts and asks what happens to the sacred figure of homo sacer when the body is replaced by the data double. It argues that digital surveillance produces a new, datafied form of bare life; that biopolitics today is increasingly exercised through infrastructures of data collection and algorithmic sorting; that the state of exception has migrated from the juridical order into technical and corporate systems; and that digital identity has become a decisive threshold of inclusion and exclusion. The article closes by considering the limits of an Agambenian reading and the need to supplement it with attention to differential power and practices of resistance.

Keywords; Bare life, State of exception, Digital identity, Biopolitics.

Introduction

Surveillance is no longer an exceptional technique reserved for suspected criminals or wartime enemies; it is a routine condition of contemporary life, woven into smartphones, workplaces, welfare systems, and city streets (Lyon, 2014). At the same time, political theory has long possessed a vocabulary for describing how modern power constitutes and controls life itself. Agamben's *Homo Sacer* argues that Western politics has always been secretly organized around the production of "bare life," a form of existence that is included in the political order only through its exclusion from full legal and social personhood. This article asks what becomes of that argument once the primary technology of governance is not the camp or the law but the database, the sensor, and the algorithm.

The aim here is not to claim that Agamben anticipated digital surveillance, but to test the portability of his conceptual apparatus. Three questions organize the discussion. First, does the datafied subject constitute a new form of bare life, exposed to power without the mediating protections of law or context? Second, how does biopolitics operate when population management is conducted through data analytics rather than through disciplinary institutions alone? Third, what role does digital identity play in determining who is included in, and who is excluded from, the circuits of contemporary citizenship? The article proceeds by first outlining Agamben's core concepts, then applying them in turn to surveillance, biopolitical data governance, the generalized state of exception, and digital identity, before turning to a critical assessment of the framework's limitations.

Agamben's Conceptual Apparatus

Agamben's argument begins with a distinction inherited from Aristotle between *zoe*, the bare biological fact of life common to all living things, and *bios*, the qualified, politically meaningful form of life proper to a community (Agamben, 1998). Western politics, Agamben contends, is founded on a hidden inclusion of *zoe* within the sphere of *bios*, and the name he gives to the resulting figure is *homo sacer*, drawn from an obscure figure of archaic Roman law: a person who could be killed without the killing counting as homicide, yet who could not be offered as a religious sacrifice. This figure is banned rather than simply excluded; it is cast out of the ordinary legal order while remaining within reach of sovereign power, included precisely through its exclusion (Agamben, 1998).

This logic of the ban is, for Agamben, structurally identical to the logic of sovereignty itself, which he reads through Carl Schmitt's definition of the sovereign as the one who decides on the exception. The sovereign stands both inside and outside the legal order: inside, because the constitution grants the power to suspend the law; outside, because in exercising that



Cover Page



power the sovereign is no longer bound by the law being suspended (Agamben, 1998, 2005). The space produced by this suspension is the state of exception, a zone in which law is technically absent yet its coercive force remains fully operative. Agamben (2005) later argued that the exception, historically conceived as temporary and extraordinary, has become a permanent paradigm of government, most visible in the proliferation of emergency powers, indefinite detention, and administrative measures that bypass ordinary judicial process.

The camp is the paradigmatic spatial realization of this logic: a materialized state of exception in which persons are reduced to bare life and placed beyond the protection of ordinary law, subject instead to the direct and unmediated power of an administrative authority (Agamben, 1998). Agamben's biopolitical vocabulary is explicitly built on Foucault's account of the shift from sovereign power, which takes life or lets live, to biopower, which is concerned with fostering, calculating, and administering the life of populations through statistics, public health, and demography (Foucault, 1978). Where Foucault emphasizes productive, dispersed forms of power exercised through discipline and normalization, Agamben insists on the persistence of sovereign violence at the very heart of biopolitical modernity: the camp, not the panopticon, is his central image (Agamben, 1998).

Digital Surveillance and the Production of Bare Life

Applying this vocabulary to digital surveillance requires attention to what is actually stripped away when a person becomes an object of data collection. Surveillance capitalism, as theorized by Zuboff (2019), operates through the continuous extraction of behavioral data, transformed into predictive products and sold in markets for future behavior. The subject of this extraction rarely consents in any meaningful sense and typically has little ability to contest how their data is used once it has left their control (Zuboff, 2019). In this respect, the datafied subject resembles bare life: a form of existence rendered legible and actionable to power while being stripped of the context, narrative, and legal standing that would normally accompany a full political or legal subject.

Where bare life is the body reduced to its biological substrate, exposed to sovereign violence without recourse, the "data double" is the person reduced to a set of measurable attributes, exposed to algorithmic judgment with limited possibility of appeal (Haggerty & Ericson, 2000). Haggerty and Ericson's account of the surveillant assemblage describes how bodies are abstracted into flows of data that are reassembled elsewhere, for purposes the original subject neither anticipated nor authorized. This abstraction is not incidental; it is the mechanism by which surveillance systems achieve their reach, since a body encumbered by context and narrative is harder to sort, compare, and act upon at scale than a body reduced to a profile.

The parallel with Agamben should not be overstated: unlike the inhabitant of the camp, the surveilled internet user is rarely in physical danger, and formal legal protections, however unevenly enforced, still nominally apply. Yet the structural logic of inclusion through exclusion recurs: the data subject is included in commercial and governmental systems precisely by being stripped of the qualities that would make them a fully recognized interlocutor within those systems, and this stripping occurs largely outside effective legal or political oversight (Andrejevic, 2007; Bauman & Lyon, 2013). Bauman and Lyon (2013) describe this condition as liquid surveillance, in which monitoring is no longer confined to fixed institutions but flows continuously across social, commercial, and state domains, dissolving the boundaries that once separated exceptional surveillance from ordinary life.

Biopolitics and the Digital Management of Populations

If bare life describes the condition of the individual data subject, biopolitics describes the scale at which digital systems govern. Contemporary data analytics extend Foucauldian biopower by allowing populations to be managed not merely through statistics and public health campaigns but through continuous, real-time behavioral tracking, risk scoring, and predictive modeling (Andrejevic, 2007). Predictive policing systems, for instance, allocate police attention according to statistically modeled risk rather than individualized suspicion, reproducing and amplifying existing patterns of racialized enforcement under the guise of neutral calculation (Browne, 2015). Browne's (2015) analysis of surveillance and Blackness



Cover Page



demonstrates that the capacity to be reduced to a suspect data profile, and thereby to bare life in Agamben's sense, has never been evenly distributed; historical practices of racial control anticipate and inform many of the sorting logics embedded in contemporary risk-scoring systems.

The COVID-19 pandemic offered a particularly vivid instance of digital biopolitics, as governments around the world deployed contact-tracing applications, location data, and health passports to manage population-level risk. These measures were frequently justified by explicit appeal to emergency and exception: ordinary rules regarding data minimization and purpose limitation were suspended in the name of public health, with the implicit promise that such suspension was temporary. Agamben (2005) had already argued that emergency measures, once introduced, tend to outlast the crises that justified them and to become part of the ordinary technique of government; the normalization of pandemic-era tracking infrastructures in several jurisdictions lends some support to this claim, even where specific applications were later scaled back.

Credit scoring, insurance underwriting, and social benefit eligibility systems extend this logic further, converting individuals into calculable risk profiles whose life chances are shaped by algorithmic classification rather than direct human judgment (Cheney-Lippold, 2017). Cheney-Lippold (2017) argues that such systems construct inferred categories of identity, such as inferred gender or inferred creditworthiness, that circulate independently of the subject's own self-understanding and yet directly determine their access to resources and opportunities. This is biopolitics in a strict sense: the management of populations through the calculated distribution of life chances, conducted at a level of abstraction that individual subjects can neither fully observe nor contest.

The State of Exception in the Networked Society

Agamben's (2005) claim that the exception has become the rule finds a striking analogue in the legal and technical architecture of digital surveillance since the early 2000s. The expansion of signals intelligence programs following the September 11 attacks, most visibly documented through the 2013 disclosures associated with Edward Snowden, revealed surveillance infrastructures built on emergency legal authorities that were subsequently normalized into standing institutional practice (Lyon, 2014). What began as an extraordinary security measure became, in effect, a permanent condition of population-wide data collection, with legal oversight mechanisms frequently described by critics as secret, retrospective, or largely symbolic.

Bigo's (2006) concept of the ban-opticon extends Agamben's vocabulary directly into the security field, describing how contemporary security professionals govern through the categorization of populations into those who are free to circulate and those who are banned, monitored, or contained, often on the basis of risk profiles generated by data systems rather than individualized due process. This is a state of exception exercised not through martial law but through administrative databases, watchlists, and biometric registries that determine who may cross a border, board a flight, or access a service, typically without the formal judicial process that would apply to comparable restrictions imposed through ordinary law (Bigo, 2006; Amoore, 2006).

The condition of refugees and migrants offers perhaps the closest contemporary echo of Agamben's camp. Biometric registration systems such as the European Union's EURODAC database reduce asylum seekers to fingerprint records circulated among state authorities, a process that Agamben's framework would describe as the production of bare life through inclusion in a system of registration that simultaneously excludes the registered person from full legal personhood and mobility rights (Ajana, 2013). Ajana (2013) argues that biometric governance of this kind renders the migrant body legible to the state precisely by stripping away its narrative and legal context, leaving only a set of measurable, comparable traits.

A further, less territorial extension of the state of exception can be found in the governance regimes of digital platforms themselves. Content moderation systems, automated account suspension, and opaque appeals processes constitute a private, quasi-sovereign power that decides, often without meaningful due process, who may remain within a given digital public



Cover Page



sphere and who is banned from it (Zuboff, 2019). This is sovereignty exercised not by the state but by the platform, and exception exercised not through martial law but through terms of service enforced by automated systems that are rarely subject to external legal review.

Digital Identity: New Thresholds of Inclusion and Exclusion

Agamben's account of inclusion through exclusion is especially illuminating when applied to systems of digital identity. National biometric identification programs, of which India's Aadhaar system is among the largest, condition access to welfare benefits, banking, and government services on successful biometric enrollment and authentication (Ajana, 2013). Where enrollment fails, whether due to technical error, biometric degradation from manual labor, or infrastructural gaps in connectivity, individuals can find themselves excluded from services to which they are formally entitled, producing what several scholars have described as a form of digital statelessness: inclusion in the legal category of citizen accompanied by practical exclusion from the systems through which citizenship is exercised (Ajana, 2013).

Algorithmic bordering technologies extend this logic to international mobility. Amoore's (2006) analysis of biometric borders describes how travelers are increasingly sorted into categories of low and high risk on the basis of data profiles compiled before they ever reach a physical border checkpoint, a process Amoore terms the biometric border, in which the site of exclusion is displaced from the territorial boundary into distributed data systems. This sorting reproduces Agamben's logic of the ban: individuals are included within global mobility infrastructures as data subjects while remaining permanently exposed to exclusion on the basis of classifications they cannot see or contest.

Social credit and reputation systems, whether formally state-administered or emergent from commercial platforms, generalize this dynamic still further, making access to opportunities contingent on an ongoing, continuously updated digital identity score (Cheney-Lippold, 2017). De-platforming, the removal of an individual from a major digital communication service, functions as a symbolic analogue to banishment: the individual is not physically confined but is expelled from a space of public appearance that has become, for many purposes, functionally equivalent to political visibility itself. In each of these cases, digital identity operates as the threshold that determines whether a person is treated as a full participant in social, economic, and political life or reduced to a status closer to Agamben's bare life: recognized by systems of power, yet stripped of the protections and standing that would normally accompany that recognition.

Critical Reassessment: Limits of the Agamben's Thought

Notwithstanding its evident productivity, an Agambenian reading of digital surveillance carries important limitations that must be acknowledged. First, critics have long noted that Agamben's framework tends toward a totalizing and undifferentiated account of power, in which the camp threatens to become a metaphor for the whole of modernity, obscuring the significant differences between, for example, involuntary biometric registration of stateless refugees and the comparatively lower-stakes data collection experienced by an affluent social media user (Mbembe, 2019). Mbembe's (2019) concept of necropolitics, developed partly in dialogue with and partly as a corrective to Agamben, insists on the specifically racialized and colonial genealogies of the power to expose certain populations to death or degradation, a specificity that a purely formal account of bare life risks flattening.

Second, Agamben's model has been criticized for underspecifying the empirical mechanisms through which contemporary surveillance actually operates. Haggerty and Ericson (2000) argue for a more granular, rhizomatic model of the surveillant assemblage precisely because power in networked societies is dispersed across commercial, governmental, and technical actors in ways that resist reduction to a single sovereign decision on the exception. Digital surveillance is rarely the act of a unified sovereign; it is more often the emergent product of interoperating databases, commercial incentives, and technical infrastructures whose effects even their designers may not fully anticipate.

Third, an exclusive focus on bare life risks understating the agency and resistance of surveilled subjects. Scholars of surveillance have documented a range of counter-conducts, including encryption practices, deliberate data obfuscation, collective privacy activism, and legal challenges to biometric and data-retention regimes, through which individuals and



Cover Page



communities contest their reduction to data doubles (Lyon, 2014). These practices suggest that the datafied subject, unlike Agamben's homo sacer, retains meaningful, if constrained, capacities for contestation, a possibility that a strictly juridical reading of sovereign exception can underplay.

These critiques do not so much refute the Agambenian framework as indicate the terms on which it should be used: as a diagnostic vocabulary for identifying structural tendencies toward the production of exposed, rightless data subjects, rather than as a complete empirical account of how digital power actually operates in every instance. Combined with Foucauldian governmentality, intersectional analyses of differential exposure, and empirically grounded studies of specific technical systems, Agamben's concepts retain considerable interpretive value.

Conclusion

Read through the framework of Homo Sacer, digital surveillance appears not as a wholly new phenomenon but as a technologically mediated intensification of a much older logic: the production of forms of life that are included in systems of power precisely through their exclusion from the protections normally attached to full legal and political personhood. The datafied subject, stripped of context and rendered legible to commercial and state actors alike, occupies a position structurally analogous to bare life. Biopolitical governance today proceeds increasingly through algorithmic risk scoring and population-level data analytics rather than through discipline and statistics alone. The state of exception, rather than remaining an extraordinary suspension of law, has migrated into the standing architecture of security databases, biometric registries, and platform governance. And digital identity has become a decisive threshold determining who is included in, and who is excluded from, the circuits of contemporary social and political life.

At the same time, the Agambenian framework must be handled with care. Its tendency toward totalizing abstraction needs to be supplemented with attention to the uneven, racialized, and historically specific distribution of exposure to digital harm, and with empirical attention to the dispersed, multi-actor character of actually existing surveillance systems. Read critically rather than applied mechanically, however, Agamben's vocabulary of bare life, sovereignty, and the exception continues to offer a valuable set of tools for interrogating the political stakes of a world increasingly organized around data.

References

1. Agamben, G. (1998). *Homo Sacer: Sovereign power and bare life* (D. Heller-Roazen, Trans.). Stanford University Press.
2. Agamben, G. (2005). *State of exception* (K. Attell, Trans.). University of Chicago Press.
3. Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. Palgrave Macmillan.
4. Amoore, L. (2006). Biometric borders: *Governing mobilities in the war on terror*. *Political Geography*, 25(3), 336–351.
5. Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. University Press of Kansas.
6. Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Polity Press.
7. Bigo, D. (2006). *Security, exception, ban and surveillance*. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 46–68). Willan Publishing.
8. Browne, S. (2015). *Dark matters: On the surveillance of Blackness*. Duke University Press.
9. Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York University Press.
10. Foucault, M. (1978). *The history of sexuality, Volume 1: An introduction* (R. Hurley, Trans.). Pantheon Books.
11. Haggerty, K. D., & Ericson, R. V. (2000). *The surveillant assemblage*. *The British Journal of Sociology*, 51(4), 605–622.
12. Lyon, D. (2014). *Surveillance, Snowden, and big data: Capacities, consequences, critique*. *Big Data & Society*, 1(2), 1–13.
13. Mbembe, A. (2019). *Necropolitics* (S. Corcoran, Trans.). Duke University Press.
14. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.