

PUBLICATION-READY ARTICLE MANUSCRIPT

The Infrastructural Structuring of the Environment

BFIId, Consumer LiDAR, Pegasus, Rouvroy and Onoptic Thresholds in the Compulsory Inclusion of Homovictimus

Hakki Tan

ORCID: <https://orcid.org/0009-0008-8582-3132>

"My paradigm is not a paradigm of the Truth; it is a paradigm of Reality."

Prepared for peer review - May 2026

Abstract

This article examines three contemporary technical cases - **BFId**, a WiFi-based identity inference attack using Beamforming Feedback Information; **consumer LiDAR-based non-line-of-sight imaging**; and **Pegasus**, the commercial spyware associated with NSO Group - through Hakkı Tan's concepts of the **Reality Paradigm**, **Onopticon** and **Homovictimus**. The article does not claim that these technologies are completed forms of the Onopticon. Its more precise claim is that they disclose different **onoptic thresholds**: technical conditions through which subjects, objects, devices and environments become perceptible, referenceable, exploitable, processable or attachable to institutional decision systems before any explicit act of recognition, control or exclusion occurs.

The article refuses to reduce these cases to the familiar vocabularies of the Panopticon, societies of control, surveillance capitalism or algorithmic governmentality. Those frameworks remain indispensable as neighbouring concepts, yet they do not exhaust the problem addressed here. The central issue is not simply who watches, who modulates, who extracts value from behavioural data or how algorithmic profiles preempt conduct. The prior question is: **through what infrastructural conditions is the subject made processable in the first place?**

BFId demonstrates the infrastructural production of recognisability; consumer LiDAR demonstrates the infrastructural production of perceptibility; Pegasus demonstrates the infrastructural production of device-internal operational accessibility. Rouvroy's algorithmic governmentality explains how behaviours may be governed once datafication and profiling are already underway; Tan's infrastructural imposition names the prior material condition through which bodies, objects and devices become datafiable - that is, capable of being transformed into data - referenceable and processable in the first place.

The article uses the Reality Paradigm diagnostically. It does not prescribe technical, legal or policy remedies, but identifies the reality-condition disclosed by these technologies: the conversion of environments and devices from neutral media into infrastructural fields that precondition perception, recognition, access, agency and contestability.

Keywords: Reality Paradigm; Onopticon; Homovictimus; infrastructural imposition; environmental structuring; BFId; WiFi sensing; Beamforming Feedback Information; consumer LiDAR; non-line-of-sight imaging; Pegasus; zero-click exploit; Rouvroy; algorithmic governmentality; compulsory inclusion; opacity.

Contents

Key Terms and First-Use Clarifications	4
1. Introduction	5
2. Scope and Methodological Boundary	5
3. Not Panopticon, Not Control Society, Not Surveillance Capitalism	6
4. Rouvroy and Tan.....	7
5. Theoretical Framework.....	9
6. BFId	9
7. Consumer LiDAR	10
8. Pegasus	11
9. Onoptic Thresholds.....	11
10. Environmental and Device-Internal Structuring	12
11. Homovictimus	13
12. Compulsory Agency.....	13
13. Unequal Distribution	14
14. Onopticon Criteria	15
15. Six Onoptic Operations	15
16. Opacity	16
17. Methodological Positioning.....	16
18. Discussion	17
19. Conclusion	17
References	18

Key Terms and First-Use Clarifications

Term	Clarification
Reality Paradigm	Hakkı Tan's diagnostic framework for analysing how reality is not merely represented, interpreted or observed, but infrastructurally imposed as the field within which subjects appear, act, access institutions and contest decisions.
Onopticon	Not a digital Panopticon or a general metaphor for surveillance. It names the imposed technical and environmental conditions through which subjects, objects and devices become perceptible, referenceable, processable and attachable to decision before explicit control occurs.
Homovictimus	The subject of compulsory inclusion: an actor whose actions, devices and environments are made processable while they are still held responsible as if agency remained intact.
Infrastructural imposition	The compulsory structuring of environments, devices and institutional gateways in ways that make subjects datafiable, referenceable, accessible or governable before they can meaningfully consent, refuse or contest.
Environmental structuring	The organisation of physical, digital or institutional surroundings so that certain forms of perception, recognition, access, movement or decision become technically possible in advance.
Onoptic threshold	An intermediate stage in which a subject, object, device or environment has already been made perceptible, referenceable, exploitable, processable or attachable to decision systems.
Processability	The condition of being technically available for classification, analysis, recognition, extraction, prediction or institutional action.
Datafiable / datafiability	"Datafiable" means capable of being transformed into data. "Datafiability" refers to the prior capacity of a body, object, action or device to become data before actual data-processing begins.
Opacity	A boundary concept naming what is eroded when a subject, object, device or environment becomes fully processable.
Algorithmic governmentality	Antoinette Rouvroy's concept for data-driven, predictive and pre-emptive governance through algorithmic processing. In this article, it is treated as a neighbouring but downstream framework.
BFIId	A WiFi-based identity inference attack that uses Beamforming Feedback Information to infer identity within a closed reference set. It does not identify all unknown persons universally.
Beamforming Feedback Information (BFI)	Technical feedback sent by WiFi client devices to access points to optimise signal transmission. BFIId shows that this feedback can also reveal body-related radio-frequency patterns.
Closed-set classification	A machine-learning setting in which the system chooses among identities already present in a known reference set.
Open-set identification	A harder setting in which the system must recognise known persons while also correctly rejecting unknown persons.
Non-line-of-sight (NLOS) imaging	Imaging or reconstructing objects that are not directly visible to the sensor, usually by analysing indirect reflections or scattered signals.
Zero-click exploit	An exploit that compromises a device without requiring the user to click a link, open a file or perform any visible action.

Term	Clarification
Endpoint compromise	The takeover or infiltration of the user's device itself. Once the endpoint is compromised, encrypted communications may be accessed before encryption or after decryption.

1. Introduction

Contemporary sensing and intrusion technologies push debates on surveillance beyond cameras, platforms and data profiles. WiFi-based identity inference, consumer-level LiDAR imaging beyond the line of sight and spyware such as Pegasus represent different technical intensities of a broader transformation. BFId shows that the human body may become a referenceable radio-frequency pattern within a WiFi environment. Consumer LiDAR shows that hidden or non-line-of-sight objects may become perceptible through consumer-grade sensors. Pegasus shows that a personal phone can become an infrastructure of extraction, sensing, location, communication capture and operational access.

This article reads these cases through Hakkı Tan's Reality Paradigm. Tan's theoretical claim is not merely that human beings are watched, measured, classified or governed. The deeper problem is that power can impose the field of reality within which the human being appears, acts, objects, accesses institutions and remains socially viable. In Tan's formulation, the Onopticon is not the next stage of the Panopticon, but belongs to another ontological register: it names the imposed reality in which the subject can appear at all (Tan 2026a).

Research question. To what extent do BFId, consumer LiDAR and Pegasus empirically disclose the infrastructural conditions through which human beings, objects, devices and environments become perceptible, referenceable, exploitable or attachable to institutional processing before explicit participation, consent or awareness?

The answer is deliberately limited. BFId is not an open-set universal identity system. Consumer LiDAR does not identify persons by itself. Pegasus does not, in every case, automatically produce political foreclosure. Yet each case discloses a threshold. BFId is a **referential onoptic threshold**. Consumer LiDAR is a **perceptual and consumerised onoptic threshold**. Pegasus is a **device-internal and operational onoptic threshold**.

For this reason, the central concept of the article is not surveillance but **environmental structuring**. The central problem is not control as such but **infrastructural imposition**. Control, surveillance, extraction, profiling and decision are downstream formations. This article addresses the prior technical and environmental conditions that make them possible.

2. Scope and Methodological Boundary

This article does not use the Reality Paradigm as a programme of technical repair, legal reform or policy design. Its purpose is not to ask what should be encrypted, banned, regulated, audited

or redesigned. Such questions are legitimate, but they belong to a different inquiry. The present argument is diagnostic: it asks what kind of reality-condition these technologies reveal.

This boundary matters. If every diagnosis is immediately converted into a reform proposal, the deeper ontological claim disappears. The Reality Paradigm does not begin from the question "what should be done?" but from the question "what is being imposed as the field in which action, recognition, refusal and contestation become possible or impossible?"

This article therefore names thresholds rather than solutions: perceptibility, recognisability, device-internal access, consumerisation, operational attachment and onoptic closure. Its task is diagnostic rather than prescriptive. It identifies the infrastructural conditions through which subjects, objects and devices become processable before explicit recognition, decision or exclusion occurs.

3. Not Panopticon, Not Control Society, Not Surveillance Capitalism: Onopticon as Infrastructural Imposition

The theoretical claim of this article is not that BFIId, consumer LiDAR and Pegasus are merely new surveillance technologies. If these cases are reduced to the Panopticon, societies of control or surveillance capitalism, the specific contribution of the Reality Paradigm is lost. The article does not ask primarily: who watches? who controls? who profits from data? It asks a prior question:

Under what infrastructural conditions is the subject made perceptible, recognisable, processable and attachable to decision?

In the Panopticon, power operates through the possibility of being seen. The subject internalises the possibility of observation and disciplines behaviour. Visibility, self-regulation and disciplinary subject formation are central. In the cases analysed here, however, the subject need not know that sensing, reference or device-internal operation is occurring. BFIId may render the body referenceable through radio-frequency disturbance. Consumer LiDAR may render hidden space perceptible. Pegasus may render the device operationally accessible without visible user action. The decisive operation is not psychological interiorisation, but the infrastructural structuring of the environment or device before the subject can respond.

Deleuze's societies of control remain essential for understanding modulation, access codes and dividualisation. Yet the cases examined here do not only show the subject becoming a dividual data fragment. They disclose the prior condition under which dividualisation becomes possible. BFIId first produces the body as a radio-frequency pattern. Consumer LiDAR first produces hidden space as perceptible. Pegasus first converts the device into an operational field. Control can later attach itself to these conditions, but it does not explain their infrastructural production.

Zuboff's surveillance capitalism illuminates the extraction of behavioural surplus, prediction and commercial behavioural modification. Yet BFIId, consumer LiDAR and Pegasus are not primarily important here because they monetise data. Their onoptic significance lies earlier: they disclose how persons, objects or devices become transformable into data-bearing, process-

able realities before market extraction, bureaucratic decision or policing is attached. In this sense, the Reality Paradigm asks not first "who owns the data?" but "which environment makes the human being convertible into data in the first place?"

Framework	Central question	Logic of operation	Limit for this article
Panopticon	Who sees whom?	The possibility of visibility induces self-discipline.	In BfId, LiDAR and Pegasus, the subject need not know that processing has occurred.
Societies of control	How is the individual modulated as individual data?	Continuous access, codes, modulation and flows.	This article examines the condition before modulation: the infrastructural production of processability.
Surveillance capitalism	How is behavioural data extracted and monetised?	Extraction, prediction, behavioural modification and profit.	This article is not centred on profit but on perceptibility, recognisability and compulsory processability.
Onopticon	Under what imposed reality can the subject appear?	Environmental structuring, infrastructural imposition and pre-decisional processability.	This is the central analytic frame.

This is the article's core theoretical contribution: contemporary sensing and intrusion technologies should not be placed under the single rubric of surveillance. They should be differentiated as **thresholds of infrastructural imposition**.

4. Rouvroy and Tan: Algorithmic Governmentality versus Infrastructural Imposition

Antoinette Rouvroy's concept of **algorithmic governmentality** is one of the closest neighbouring frameworks to this article, but it should not be confused with the Reality Paradigm. Rouvroy and Berns define algorithmic governmentality as a form of normative and political rationality based on the automated collection, aggregation and analysis of big data. Its aim is to model, anticipate and pre-emptively affect possible behaviours (Rouvroy and Berns 2013).

This framework shifts attention away from classical discipline, conscious obedience and legal normativity towards pre-emptive, data-driven modulation. Rouvroy and Berns also stress that algorithmic governmentality operates through infra-individual data and supra-individual patterns, thereby bypassing the reflexive subject rather than addressing it as a legal or moral agent.

The present article accepts the relevance of Rouvroy's analysis, but places it at a different level. Rouvroy explains what happens **once datafication and algorithmic processing are already underway**. Tan's notion of infrastructural imposition asks a prior question: **through what material, technical and environmental conditions can something become datafiable, referenceable or processable in the first place?**

The distinction is decisive. Rouvroy's object is primarily algorithmic: data correlations, statistical inference, probabilistic modelling, pre-emption and the evacuation of reflexive subjectivity. Tan's object is infrastructural: radio-frequency environments, LiDAR sensing surfaces, device-internal exploit chains, institutional gateways and the material conditions through which the subject is made processable before algorithmic governmentality can operate.

Rouvroy's tragic figure is the subject evacuated into data fragments, infra-individual traces and supra-individual profiles. Tan's Homovictimus is different. Homovictimus does not disappear into data. Homovictimus continues to act, speak, walk, work, communicate and testify. The tragedy is not the disappearance of the subject, but the compulsory conversion of the subject's ongoing actions into another field of processing. In Rouvroy, the subject is bypassed by algorithmic governmentality. In Tan, the subject is compulsorily included in infrastructures that make such bypassing possible.

The difference also concerns temporality. Rouvroy's algorithmic governmentality is oriented towards the future: uncertainty, probability, risk, pre-emption and the reduction of possible futures to manageable predictions. Tan's infrastructural imposition is oriented towards the present material condition: the RF field in which a body becomes referenceable, the LiDAR environment in which hiddenness becomes perceptible, the compromised device through which communication and testimony become operationally accessible.

Category	Rouvroy: Algorithmic Governmentality	Tan: Infrastructural Imposition
Primary object	Algorithms, big data, correlations, statistical inference.	Material-technical infrastructures: RF, LiDAR, device-internal exploit chains.
Data relation	Processing, prediction and pre-emption once data exists.	The material conditions through which something becomes datafiable.
Subject figure	Evacuated subject; infra-individual traces; supra-individual profiles.	Homovictimus: a continuing actor whose actions are compulsorily made processable.
Tragedy	The disappearance or bypassing of the reflexive subject.	The subject continues acting, but action is converted into another processing field.
Temporality	Future, uncertainty, probability, pre-emption.	Present infrastructural condition: space, device, sensor, access.
Opacity	Normative-political horizon; critique and emancipation.	Boundary concept; diagnostic marker of what is being eroded.
Normative stance	Critical and reform-oriented.	Diagnostic; does not propose reform.
Relation to On-opticon	Downstream algorithmic layer.	Prior infrastructural field that can make algorithmic governmentality possible.

The three cases clarify this distinction. BFI_d is not first an algorithmic governmentality case. It first shows that the WiFi environment can render the body referenceable as an RF pattern. Consumer LiDAR is not first a predictive governance case. It first shows that hiddenness can be technically weakened by consumer sensing. Pegasus is not first a profiling system. It first converts the device itself into an operational infrastructure.

Thus, Rouvroy helps explain how data-driven profiles, correlations and anticipatory interventions operate once datafication is underway. Tan explains the prior infrastructural imposition through which bodies, objects and devices become available to such processing. Algorithmic governmentality may be a downstream regime of the Onopticon, but it is not identical with it. The strongest formulation is therefore:

Rouvroy shows how algorithmic governmentality bypasses the subject; Tan shows how the subject is placed inside the infrastructural reality that makes such bypassing possible.

5. Theoretical Framework: Reality Paradigm, Onopticon and Homovictimus

Tan's Reality Paradigm is not a theory of truth. It does not ask primarily what is true, who tells the truth or how truth is distorted. It asks under what imposed conditions the human being encounters reality. In this framework, reality is not simply given, interpreted or represented. It is operationally imposed through infrastructures of recognition, access, eligibility, risk, identity, movement, labour, health, decision and appeal.

The Onopticon is therefore not a digitalised Panopticon. The question is not merely who watches, who modulates or who extracts; it is who imposes the reality in which the subject can appear. Homovictimus names the subject produced within this imposed field: a subject held responsible as an agent while deprived of the infrastructural conditions required for agency. Tan's related work on environmental structuring frames the Onopticon as a regime in which technical systems pre-process conditions of access, recognition, mobility, risk, service provision and institutional action (Tan 2026b).

The three cases analysed here remain below the biological threshold of cellular pre-regulation. They concern radio-frequency recognisability, non-line-of-sight perceptibility and device-internal operational accessibility.

6. BFId: Closed-Set, Reference-Based Identity Inference

BFId must be described technically before it can be used theoretically. It is not a universal system that names any person encountered for the first time. It is a closed-set, reference-based identity inference attack using Beamforming Feedback Information, or BFI. Beamforming in WiFi 5 requires clients to broadcast observations of channel characteristics. The BFId study introduces the first identity inference attack using BFI-based sensing and evaluates it on WiFi recordings of 197 individuals, reporting high accuracy across walking styles and perspectives (Todt, Morsbach and Strufe 2025).

This accuracy must not be read as general social omniscience. It indicates performance within a closed reference setting, not open-set identification of unknown persons. BFId does not demonstrate zero-shot recognition. It shows that a body can become technically distinguishable within an RF environment when sufficient BFI data and reference modelling are available.

The passive listening model is also not unlimited. An attacker must be positioned to capture relevant access point-client BFI traffic on the appropriate channel. This is not equivalent to saying that any person in any WiFi environment is automatically identifiable. The more precise claim is that, under suitable radio, access point and client-traffic conditions, a person's body may become a referenceable RF pattern without the person themselves carrying a device.

The onoptic significance of BFID lies in showing the **infrastructural production of recognisability**. The WiFi environment is no longer merely a communication medium. Under certain conditions, it becomes a pre-decisional surface that can render the body processable. KIT's public communication on the study also emphasises that BFI is transmitted in unencrypted form and can be readable to parties within range, which underscores the infrastructural rather than merely intentional character of the risk (Karlsruhe Institute of Technology 2025).

Dimension	Correct formulation	Incorrect formulation
Device condition	The target's own device is not necessarily required; suitable AP-client BFI traffic is required.	No device, channel or AP condition is required.
Recognition type	Closed-set, reference-based identity inference.	Universal recognition of any newly encountered person.
Machine-learning status	Classification among identities in a reference set.	Open-set or zero-shot identification.
Evidentiary status	Technical capacity evidence.	Evidence of a completed social On-opticon.
Onoptic status	Referential infrastructural threshold.	Completed Onopticon.

7. Consumer LiDAR and the Perceptual Onoptic Threshold

Consumer LiDAR discloses a different threshold. Here the issue is not identity inference. It is the technical weakening of non-visibility. A hidden or non-line-of-sight object becomes perceptible through consumer sensing.

Somasundaram, Young, Dave, Pediredla and Raskar introduce a motion-induced aperture sampling model that unifies object shape, object motion and camera motion under a single measurement model. They demonstrate three non-line-of-sight capabilities on smartphone-grade LiDAR: three-dimensional reconstruction, single- and multi-object tracking and camera localisation using hidden objects. Their article also states that NLOS imaging had previously been restricted to bulky and expensive research-grade hardware requiring set-up and calibration, whereas their result points towards plug-and-play NLOS imaging with off-the-shelf hardware costing less than US\$100 (Somasundaram et al. 2026).

The onoptic significance of this work is not that it identifies persons. It does not. Its significance lies in showing the **infrastructural production of perceptibility**. The distinction between visible and non-visible is technically weakened. What matters is not that a hidden object is "watched", but that the environment is restructured so that hiddenness no longer guarantees imperceptibility.

Consumer LiDAR therefore expands the onoptic threshold beyond identity. Some thresholds begin not with recognition, but with perception. The hidden object is not yet classified as a subject, target or risk. Yet it has crossed into a technical field of possible processing.

8. Pegasus and the Device-Internal Operational Threshold

Pegasus is a harder case than BFId or consumer LiDAR. BFId extracts a referenceable body pattern from the environment. Consumer LiDAR makes the hidden perceptible. Pegasus converts the personal device itself into an operational infrastructure.

In this threshold, the phone is no longer merely a communication tool. It can become a sensor, archive, location trace, microphone, camera, contact map and testimony repository accessible to an external operator. Citizen Lab's FORCEDENTRY report documents an NSO Group iMessage zero-click exploit that was discovered while analysing the phone of a Saudi activist infected with Pegasus. The exploit targeted Apple's image rendering library and was effective against iOS, macOS and watchOS devices. Google Project Zero later provided a technical analysis of the NSO zero-click iMessage exploit, based on a sample shared by Citizen Lab (Marczak et al. 2021; Beer and Groß 2021).

Pegasus matters because zero-click intrusion collapses behavioural blame. The target need not click a link, download a file or visibly consent to any interaction. Amnesty International's forensic methodology report states that Pegasus attacks included zero-click attacks that did not require target interaction and documents forensic traces on iOS and Android devices following Pegasus targeting (Amnesty International 2021).

Pegasus does not need to "break" end-to-end encryption mathematically. Once the endpoint is compromised, messages may be accessible before encryption or after decryption. The problem is not the collapse of cryptography as such, but the conversion of the endpoint into an operational surface.

Pegasus's onoptic significance therefore lies not merely in data theft. It lies in **device-internal infrastructural imposition**. The subject is not only observed from outside. The subject's own digital intermediary becomes an imposed field through which communication, movement, memory, association and testimony can be rendered operationally accessible.

Pegasus remains below completed Onopticon in the strict sense. Infection does not automatically produce arrest, silencing, exile or legal exclusion. Yet Pegasus is closer to operational onoptic closure than the other two cases because it can connect device-internal access to targeting infrastructures. The WhatsApp v. NSO litigation makes visible the institutional and legal interface of this operational threshold: the district court ruled in favour of WhatsApp in late 2024, a jury awarded damages in 2025 and a permanent injunction was later entered (Knight First Amendment Institute 2026).

9. Onoptic Thresholds: Definition and Stratification

An **onoptic threshold** is the intermediate level at which a subject, object, device or environment has not yet been enclosed within a completed Onopticon, but has been infrastructurally made perceptible, referenceable, exploitable, processable or attachable to decision systems.

This threshold is not where surveillance begins. It is where the environment that makes surveillance, control, extraction, profiling or decision possible is technically structured. Control is a

possible result. Infrastructural structuring is the condition. The analytical point is not completion, but threshold formation.

Threshold	Meaning	BFI _d	Consumer LiDAR	Pegasus
Perceptual threshold	The normally hidden or inaccessible becomes perceptible.	The body becomes an RF/BFI disturbance pattern.	A hidden object becomes NLOS-imaged.	Device contents and sensors become visible to an operator.
Referential threshold	A pattern becomes attachable to identity, record or profile.	Closed-set identity inference.	No direct identity inference; object tracking only.	Device owner, contact graph, location and communications become referenceable.
Consumerisation threshold	Capacity moves towards off-the-shelf devices or service markets.	Ordinary WiFi infrastructures become relevant to sensing attacks.	Smartphone-grade LiDAR supports NLOS imaging.	Commercial spyware becomes operational service.
Device-internal threshold	The personal device becomes a hostile sensor/archive infrastructure.	Not direct.	Not direct.	Central threshold.
Operational threshold	Perception, reference or access attaches to security, risk or targeting systems.	Not directly demonstrated.	Not directly demonstrated.	Strongly plausible through state and client operations.
Onoptic closure	Attachment narrows real possibilities.	If connected to access, policing or exclusion systems.	If connected to spatial control or security systems.	Approaches closure through targeting, intimidation, prosecution, coercion or self-censorship.

This stratification prevents conceptual inflation. The three cases are arranged according to the kind of infrastructural imposition they disclose.

10. Onoptic Thresholds as Environmental and Device-Internal Structuring

BFI_d, consumer LiDAR and Pegasus should be read as technical forms of environmental and device-internal structuring. They do not merely add new data flows to an already given world. They alter the conditions under which bodies, objects and devices can appear as processable.

BFI_d structures the RF environment as a field of recognisability. Consumer LiDAR structures hidden space as a field of perceptibility. Pegasus structures the device as a field of operational accessibility. In all three cases, the decisive operation occurs before final decision. The target is not yet necessarily punished, excluded, silenced or denied access. Yet the prior field in which punishment, exclusion, silencing or denial could later occur has been technically prepared.

This is why the language of control society is insufficient. Societies of control describe modulation, access codes and dividualised flows. The cases here show the prior infrastructural condition of modulation: first the body must become an RF pattern; first the hidden object must be

come perceptible; first the device must become operationally accessible. Only then can control attach itself.

The same applies to algorithmic governmentality. Rouvroy's framework explains how traces, correlations and profiles may govern possible behaviours once a subject has already become datafiable. But BFI, consumer LiDAR and Pegasus disclose the material thresholds before that stage: the production of the trace, the perceptibility of the hidden and the conversion of the device into an operational surface.

11. Homovictimus: From Exposure to Device-Internal Compulsory Inclusion

Homovictimus must be analysed through stages. Not every exposure to a signal, sensor or device ecosystem produces full onoptic closure. The point is to identify the steps through which compulsory inclusion becomes possible.

Stage	Definition	BFI	Consumer LiDAR	Pegasus
Environmental exposure	Person/object/device is within a technical field.	Person is in WiFi RF space.	Object is outside line of sight but measurable.	Device is in communication ecosystems.
Perceptual capture	Technical trace becomes separable.	BFI disturbance is extracted.	NLOS reflections are modelled.	Messages, location, sensors and files become accessible.
Referencing	Trace attaches to identity, object or profile.	Closed-set identity inference.	Object tracking, not identity.	Device owner, communication graph and location profile.
Device-internal operation	Personal device becomes an operational field.	Absent.	Absent.	Core Pegasus threshold.
Operational attachment	Trace or access attaches to decision or targeting.	Potential.	Potential.	Strong.
Onoptic closure	Possibilities become concretely narrowed.	If attached to exclusion systems.	If attached to spatial control.	Through targeting, intimidation, coercion or silencing.

Pegasus sharpens the figure of Homovictimus by showing how everyday digital agency can become the medium of compulsory inclusion. The phone is not merely an object; it is memory, communication, work, location, witness, association and archive. When that device is converted into an external operational infrastructure, agency itself becomes processable.

12. Homovictimus and Compulsory Agency

Homovictimus is not a passive victim. Compulsory inclusion does not mean inactivity. It means that the subject continues to act, while the infrastructural conditions of action are already

shaped in advance. Homovictimus walks, writes, testifies, communicates, works, travels, uses devices and forms relationships. Yet these practices can be technically converted into another field of processing.

In BFIId, gait and bodily presence may become RF/BFI patterning. In consumer LiDAR, the assumption of hiddenness may become spatially modelled data. In Pegasus, communication, testimony, location and association may become device-internal operational data.

This is also where Tan departs sharply from Rouvroy. Rouvroy's account describes the bypassing or evacuation of the reflexive subject through infra-individual traces and supra-individual profiles. Tan's Homovictimus does not disappear into data. Homovictimus remains socially active, but those actions are compelled into infrastructures that make them processable. The tragedy is not the disappearance of the subject; it is the conversion of continuing agency into an imposed processing field.

Resistance appears here not as a reform prescription but as an analytic marker. Different thresholds generate different possible forms of contestability. BFIId raises questions of RF environments and AP-BFI traffic. Consumer LiDAR raises questions of spatial positioning, reflection and sensor access. Pegasus raises questions of platform vulnerability, forensic traceability, device security and state or mercenary operational chains. These differences show that Homovictimus is neither inert nor sovereign in the classical sense. Homovictimus acts, but acts within a field whose conditions of processability may have already been imposed.

13. The Unequal Distribution of Onoptic Thresholds

Onoptic thresholds are not distributed evenly. Homovictimus is a universal possibility but not a homogeneous position. Technical environments may, in principle, process anyone; in practice, they intensify around particular infrastructures, professions, political locations and capacities to contest.

Pegasus makes this most visible. Journalists, human rights defenders, lawyers, political opponents and activists face heightened exposure to device-internal operational thresholds. Amnesty International's forensic report describes analysis of devices from human rights defenders and journalists and documents forensic traces associated with Pegasus targeting. Citizen Lab's FORCEDENTRY report likewise places Pegasus in the context of targeted surveillance (Amnesty International 2021; Marczak et al. 2021).

BFIId and consumer LiDAR also imply unequal environments. WiFi-dense spaces such as campuses, offices, transport hubs, commercial centres and border facilities are more favourable to RF-based sensing. LiDAR and similar sensors intensify where smartphones, robotics, spatial mapping, logistics and security infrastructures are dense. The onoptic threshold is therefore not only technical. It is distributed through class, profession, political exposure, geography, urban density, infrastructure, device ownership and contestability.

The Reality Paradigm does not turn this observation into a policy programme. It diagnoses the asymmetry: imposed infrastructural reality is not imposed uniformly. Some subjects become recognisable earlier, more intensely and with weaker contestability than others.

14. Onopticon Criteria Across the Three Cases

Tan's methodological boundary requires that Onopticon not be applied to everything. A case must be tested through compulsory recognition, foreclosure of possibility and weak contestability. The three cases can be positioned as follows:

Criterion	BFI ^d	Consumer LiDAR	Pegasus
Compulsory recognition / perceptibility	Target's own device may not be necessary; suitable AP-BFI traffic may suffice.	Hidden objects may become perceptible through consumer LiDAR.	Zero-click infection may occur without user interaction.
Foreclosure of possibility	Not produced by BFI ^d alone.	Not produced by LiDAR alone.	Can attach to targeting, intimidation, prosecution or coercion.
Weak contestability	The person may not know which BFI traffic or model renders them processable.	Hiddenness no longer ensures imperceptibility.	Strongest: device compromise may remain invisible to the user.

BFI^d and consumer LiDAR remain threshold cases. Pegasus is closer to operational Onopticon because it can connect device access to state or client action. The concept becomes analytically strong only when these distinctions are preserved.

15. Six Onoptic Operations Across BFI^d, LiDAR and Pegasus

Tan's later formulation of Onopticon as environmental structuring allows the cases to be compared through six operations: conversion into processable units, conditional inclusion, shifting from decision to decision-horizon, distributed responsibility, technical legitimation and preconditioning of response (Tan 2026b).

Onoptic operation	BFI ^d	Consumer LiDAR	Pegasus
Conversion into processable units	Body becomes RF/BFI pattern.	Hidden object becomes NLOS measurement object.	Phone becomes sensor, archive and tracking infrastructure.
Conditional inclusion	Person enters recognition field without being a user.	Hidden object enters perceptual field.	Person enters device-internal processing without click or consent.
Decision-to-horizon shift	Produces recognisability before decision.	Opens hidden space before decision.	Produces device-internal data horizon for targeting.
Distributed responsibility	AP, client, standard, model, dataset and institution.	Sensor maker, algorithm, device, app and user.	NSO, state client, platform, device vendor and operator.
Technical legitimation	"Only beamforming feedback."	"Only consumer LiDAR."	"Counter-terrorism and serious crime" rhetoric.
Preconditioning of response	Environmental recognisability.	Non-line-of-sight perceptibility.	Communication, location and testimony become operational.

These are not identical cases. Their commonality lies not in a single surveillance function, but in the preconditioning of processability.

16. Opacity as Boundary, Not Solution

Opacity is not treated here as a policy instrument. It is treated as a boundary concept: the name for what is eroded when a subject, object or device becomes totally processable.

In Tan's framework, opacity marks the refusal of total operational reduction. This position also differentiates Tan from Rouvroy. Rouvroy's critique retains a political and juridical orientation towards emancipation, due process and democratic contestability. Tan's opacity, as used in this article, is a diagnostic boundary that names the limit being eroded.

In BFI_d, opacity is eroded when bodily presence can become a referenceable RF pattern without active participation. In consumer LiDAR, opacity is eroded when non-line-of-sight hiddenness becomes perceptible through consumer sensing. In Pegasus, opacity is eroded when the personal device becomes a hostile sensor and archive. These examples matter because they show that environments and devices are no longer neutral media. They can become infrastructures that precondition recognisability, perceptibility and operational accessibility.

17. Methodological Positioning

This article uses comparative case analysis. It does not offer exhaustive empirical proof of a completed social regime. It uses three technical cases as capacity evidence for different onoptic thresholds.

Level of analysis	Question	BFI _d	Consumer LiDAR	Pegasus
Technical capacity	Can signal, sensor or exploit data support identity, perception or access?	BFI supports closed-set identity inference.	LiDAR supports NLOS reconstruction and tracking.	Zero-click exploitation supports device access.
Environmental/device capacity	Can a person/object/device enter processing without active participation?	Yes, under suitable AP-BFI conditions.	Yes, hidden objects may become perceptible.	Yes, the user may not interact at all.
Referential capacity	Can the trace be attached to identity or record?	Yes, in closed-set form.	Not directly; object tracking only.	Strongly, through device owner, contact graph and location.
Onoptic capacity	Is the trace attached to decision, exclusion or targeting?	Not directly shown.	Not directly shown.	Strongly plausible and empirically documented through spyware operations.
Rouvroy-Tan distinction	Is this data-processing or the prior production of the capacity to be transformed into data?	Prior production of RF datafiability.	Prior production of perceptual datafiability.	Prior production of device-internal operational datafiability.

This method protects the article from two errors: reducing the cases to technical curiosities, or inflating them into completed total domination. Their analytical value lies in the threshold.

18. Discussion: What These Cases Prove and Do Not Prove

BFI_d proves that BFI can function as a source for closed-set identity inference and that WiFi environments may produce referenceable bodily patterns. It does not prove that every WiFi environment identifies everyone, nor that unknown persons can be universally named (Todt, Morsbach and Strufe 2025).

Consumer LiDAR proves that non-line-of-sight imaging capabilities can be demonstrated with smartphone-grade LiDAR, including 3D reconstruction, object tracking and camera localisation using hidden objects. It does not prove person-identification, institutional surveillance or direct exclusion (Somasundaram et al. 2026).

Pegasus proves that zero-click device compromise associated with Pegasus has been documented, that forensic traces can be analysed and that device-internal access can become operationally significant. It does not prove that all phones are infected, that encryption protocols are mathematically broken or that every Pegasus incident is automatically a completed Onopticon (Marczak et al. 2021; Amnesty International 2021).

Rouvroy proves conceptually useful for analysing what happens once data, correlations and profiles are already available. Yet BFI_d, consumer LiDAR and Pegasus disclose a prior level: the material thresholds on which algorithmic governmentality may later depend. In this sense, algorithmic governmentality is not rejected, but relocated. It is one possible downstream mode of infrastructural imposition.

Theoretical discipline matters here. The Reality Paradigm becomes stronger when it does not overclaim. BFI_d, consumer LiDAR and Pegasus should be treated not as identical technologies but as differentiated thresholds of infrastructural imposition.

19. Conclusion

BFI_d, consumer LiDAR and Pegasus do not redefine Tan's Onopticon; they test its analytical reach. Each case gives empirical weight to the central claim of the Reality Paradigm: contemporary power does not merely observe reality, but can impose the conditions under which reality is encountered, processed and contested.

BFI_d shows the infrastructural production of recognisability. Consumer LiDAR shows the infrastructural production of perceptibility. Pegasus shows the infrastructural production of device-internal operational accessibility. These are not simply cases of surveillance, control, algorithmic governmentality or data extraction. They disclose prior material thresholds on which those regimes may later depend.

Rouvroy's algorithmic governmentality explains the governance of possible behaviours once data, correlations and profiles are already available. The Reality Paradigm asks a prior question:

under what infrastructural conditions do bodies, objects and devices become datafiable, referenceable and processable in the first place? BFI_d, consumer LiDAR and Pegasus are therefore better understood as differentiated thresholds of infrastructural imposition.

Homovictim_{us} names the subject compelled to act through environments and devices whose conditions of processability have already been structured. This compulsory inclusion is unequally distributed: journalists, activists, dissidents, border populations, sensor-dense urban subjects and technically weakly contesting groups may encounter onoptic thresholds earlier and more intensely than others.

Final thesis. BFI_d produces recognisability; consumer LiDAR produces perceptibility; Pegasus produces device-internal operational accessibility. The Onopticon is not another name for control society, surveillance capitalism or algorithmic governmentality. It names the imposed technical and environmental conditions under which control, surveillance, datafication, profiling and decision become possible.

This article does not propose reform. It names the condition.

References

- Amnesty International. 2021. 'Forensic Methodology Report: How to Catch NSO Group's Pegasus'. Amnesty International Security Lab. <https://www.amnesty.org/en/wp-content/uploads/2021/08/DOC1044872021ENGLISH.pdf>.
- Beer, Ian, and Samuel Groß. 2021. 'A Deep Dive into an NSO Zero-Click iMessage Exploit: Remote Code Execution'. Google Project Zero. <https://projectzero.google/2021/12/a-deep-dive-into-nso-zero-click.html>.
- Deleuze, Gilles. 1992. 'Postscript on the Societies of Control'. *October* 59: 3-7.
- Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon.
- Karlsruhe Institute of Technology. 2025. 'The Spy Who Came in from the WiFi: Beware of Radio Waves'. *EurekaAlert!*. <https://www.eurekaalert.org/news-releases/1101595>.
- Knight First Amendment Institute. 2026. 'WhatsApp v. NSO Group'. Columbia University. <https://knight-columbia.org/cases/whatsapp-v-nso-group>.
- Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan and Ron Deibert. 2021. 'FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild'. *Citizen Lab Research Report No. 143*. University of Toronto. <https://citizenlab.ca/research/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.
- Rouvroy, Antoinette. 2013. 'The End(s) of Critique: Data Behaviourism versus Due Process'. In *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, edited by Mireille Hildebrandt and Katja de Vries, 143-167. London: Routledge.
- Rouvroy, Antoinette. 2020. 'Algorithmic Governmentality and the Death of Politics'. *Green European Journal*, 27 March. <https://www.greeneuropeanjournal.eu/algorithmic-governmentality-and-the-death-of-politics/>.

- Rouvroy, Antoinette, and Thomas Berns. 2013. 'Algorithmic Governmentality and Prospects of Emancipation: Disparateness as a Precondition for Individuation through Relationships?' *Réseaux* 177(1): 163-196. DOI: [10.3917/res.177.0163](https://doi.org/10.3917/res.177.0163).
- Somasundaram, Siddharth, Aaron Young, Akshat Dave, Adithya Pediredla and Ramesh Raskar. 2026. 'Imaging Hidden Objects with Consumer LiDAR via Motion-Induced Sampling'. *Nature* 653: 693-699. DOI: [10.1038/s41586-026-10502-x](https://doi.org/10.1038/s41586-026-10502-x).
- Tan, Hakkı. 2026a. *Reality Paradigm, Onopticon and Homovictimus: A Theoretical, Manifestal and Case-Based Inquiry into the Regime of Infrastructural Imposition*. DOI: [10.13140/RG.2.2.15728.42241](https://doi.org/10.13140/RG.2.2.15728.42241).
- Tan, Hakkı. 2026b. *Down to the Cell Membrane: Onopticon, Homovictimus, and the Pre-Regulation of Life: Sovereignty as Environmental Structuring from the State to Cellular Responsiveness*. DOI: [10.2139/ssrn.6659878](https://doi.org/10.2139/ssrn.6659878).
- Todt, Julian, Felix Morsbach and Thorsten Strufe. 2025. 'BFId: Identity Inference Attacks Utilizing Beamforming Feedback Information'. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25)*. DOI: [10.1145/3719027.3765062](https://doi.org/10.1145/3719027.3765062).
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.