

From Fragmented Files to Operational Nodes: The NHS-Palantir Case and the Ontological Transformation of the Patient

Research Article

Hakki Tan

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

Suggested citation: Tan, H. (2026). From Fragmented Files to Operational Nodes: The NHS-Palantir Case and the Ontological Transformation of the Patient.

Author's Note

Readers engaging with Hakki Tan's recent articles - particularly with concepts such as **Onopticon**, **Homovictimus**, and the **Reality Paradigm** - are advised to undertake retrospective readings of the author's earlier work. These concepts should not be treated as isolated theoretical terms, but as elements of a broader conceptual framework developed across a longer intellectual trajectory.

The following article should therefore be read not merely as a commentary on the NHS-Palantir case, but as part of an ongoing analysis of how contemporary infrastructures reshape visibility, subjectivity, and the conditions under which human beings become governable.

Abstract

This article examines the NHS-Palantir controversy through the conceptual lens of infrastructural power, datafication, security-state rationality, and the ontological transformation of the patient. Rather than treating the case merely as a privacy dispute, data-security concern, or procurement controversy, the article argues that the deeper issue concerns the transformation of the patient from a fragmented clinical subject into an operational node within an integrated data architecture. While patient datafication long predates Palantir, the Federated Data Platform and the National Data Integration Tenant reveal a new scale of integration, where health data can be linked to operational categories such as capacity, risk, flow, priority, and resource allocation. The article also situates Palantir within its broader intelligence, defence, policing, immigration-enforcement, and security-state genealogy. It argues that the NHS controversy is not only about health data governance, but also about the migration of actionable-intelligence logics into civilian infrastructures of care. Through the concepts of Onopticon, Homovictimus, and the right to opacity, the article argues that contemporary health infrastructures do not merely observe the patient; they participate in constructing the conditions under which the patient becomes visible, calculable, actionable, and governable.

Keywords

Keywords: Onopticon; Homovictimus; Reality Paradigm; Palantir; NHS; Federated Data Platform; National Data Integration Tenant; datafication; health data; infrastructural power; right to opacity; digital governance; biopolitics; operational ontology; patient subjectivity; intelligence infrastructure; actionable intelligence; national security; Maven Smart System; TITAN; ICE; ELITE; ImmigrationOS; IRS; Gotham; security state; military AI; law-enforcement intelligence; data integration; operational governance.

Introduction

The way the state governs the body is changing. This transformation is no longer written only in legal texts, hospital protocols, or the doctor-patient relationship. It is increasingly inscribed in external software architectures.

According to reporting by the Financial Times and Reuters in May 2026, NHS England agreed to create a new "admin" role that would grant external contractor personnel, including staff from Palantir, broad access to identifiable patient data within the National Data Integration Tenant - NDIT - a component of the Federated Data Platform. The reports state that the NDIT functions as a staging environment before pseudonymisation, while NHS England argues that such access is governed by security clearance, director-level approval, monitoring, and audit mechanisms (Financial Times, 2026; Reuters, 2026a).

This development should not be understood merely as a data breach, a procurement controversy, or a technical access issue. At a deeper level, it concerns how the modern health system recognises, classifies, prioritises, and manages the patient. In other words, the central question is not simply: Who can see patient data? The more fundamental question is: Within which data architecture does the patient become real, processable, and governable?

Why the NDIT Matters

The NDIT is one of the national data integration environments within NHS England's Federated Data Platform. NHS England's own product privacy notice states that NDIT processes personal data about patients that NHS England is legally required to manage, and that this information is arranged before identifiers are removed for dashboard use. The notice lists categories of directly identifiable data that may be processed, including name, address, date of birth, NHS number, health condition, diagnosis, treatment, ethnicity, religion or beliefs, genetic data, and location-related information (NHS England, 2026a).

This technical detail is crucial. The controversy does not concern only access to final dashboards, aggregated reports, or anonymised statistics. It concerns an integration environment where data is organised, matched, prepared for processing, and, according to the Financial Times report, exists before pseudonymisation. This shifts the centre of gravity of the debate from ordinary data access to infrastructural access (Financial Times, 2026).

For this reason, "admin access" should not be treated merely as a technical permission level. What is at stake is access to the infrastructural zone through which the health system acquires the capacity to see, classify, and manage itself.

There is, however, an important nuance. The phrase "unlimited access" should not automatically be read as meaning absolute absence of oversight. NHS England maintains that access would be governed by security clearance, senior approval, monitoring, and limits on the number of authorised personnel. Palantir also presents itself as a data processor acting under NHS instructions (Reuters, 2026a).

Yet the existence of oversight does not eliminate the structural problem. The deeper issue is not only whether such access might be abused. It is whether this form of access regime becomes normalised within the operational architecture of the health system.

Palantir Did Not Begin Datafication; It Changes Its Scale

The transformation of the patient into a data object did not begin with Palantir. Modern health systems have long datafied patients through discharge summaries, laboratory records, radiology images, prescription systems, electronic health records, insurance files, and performance metrics.

Therefore, to say that "the patient has now become data" is not, by itself, a new observation. The patient was already being recorded, measured, coded, and categorised. What distinguishes the older regime is that these records were largely fragmented.

The laboratory kept its own results. Radiology produced its own images. The general practitioner maintained a medical history. The hospital produced its own discharge summary. Insurance or payment systems recorded their own transactional data.

Each of these systems transformed the patient into data, but usually within a limited, specialised, and contextual domain. The patient was a clinical subject divided across institutional files.

The novelty of Palantir/FDP-type infrastructures is not that they initiate datafication, but that they render datafication horizontally and vertically integrable. The patient is no longer merely a blood test result, a diagnostic code, a waiting-list entry, or a surgical record. The patient can be linked simultaneously to bed capacity, discharge flows, waiting lists, resource allocation, workforce planning, population health, and operational risk categories.

NHS England's FDP privacy notice states that different products within the platform are designed for purposes such as direct care, planning, care coordination, population health, and operational management. It also states that personal data processed within the FDP may include identifying information and information about health and treatment, while access is supposed to be restricted according to purpose and role (NHS England, 2026b).

This is not simply the collection of more data. It is a transformation in the ontological status of the patient within the health system.

From Fragmented File to Operational Node

This transformation can be stated clearly: old regime, the fragmented file; new regime, the operational node.

Old regime	Fragmented file
New regime	Operational node

In the fragmented-file regime, the patient is represented separately within the record systems of different specialisms. The patient appears as a clinical case, a diagnostic file, a laboratory result, an imaging record, or a prescription history.

In the operational-node regime, the patient becomes a calculable point of connection at the intersection of multiple systems. This node is not merely medical. It is also logistical, administrative, financial, demographic, and operational.

NHS England's official explanations of the FDP emphasise its intended use in areas such as waiting-list management, discharge processes, care coordination, population health, and resource management. These

objectives cannot be dismissed as irrelevant. Patients being delayed, lost between institutions, or treated inefficiently because of fragmented health data is a genuine problem (NHS England, 2026b).

But this is precisely where the tension begins. Data integration promises better care, faster decisions, and more efficient use of resources. At the same time, it redefines the patient within the operational logic of health-system efficiency.

The patient is no longer only a person in need of care. The patient also becomes a node processed through the system's logics of capacity, risk, cost, flow, and priority.

Palantir's Architectural Power: Ontology

What makes Palantir significant in this debate is not merely that it provides software to the NHS. In Palantir's own Foundry/Ontology documentation, the Ontology is described as an operational layer that sits on top of digital assets such as datasets, virtual tables, and models, connecting them to real-world objects, relationships, and processes. Palantir also describes the Ontology as containing semantic elements such as objects and links, as well as kinetic elements such as actions, functions, and dynamic security (Palantir, n.d.).

This point is critical. Data is not merely stored here. It is related, modelled, linked to action, and embedded in decision-making processes. Palantir's documentation explicitly frames the Ontology as a means of enabling workflows, decision-making, and organisational action at scale (Palantir, n.d.).

A careful distinction is necessary: in the specific NHS-Palantir case, there is no evidence that Palantir has access to all non-health data domains such as education, finance, culture, or broader social data. The available sources concern health and care data within the NHS/FDP/NDIT context. However, Palantir's architectural power lies in its capacity to relate different data worlds within a single operational ontology.

Thus, the central danger is not only which data is accessed today. It is also what kind of decision infrastructure such an architecture could provide for connecting further data domains in the future.

Palantir's Operational Genealogy: Intelligence, Targeting, Policing, and the Civilian Migration of Security-State Logic

Palantir's role in the NHS controversy cannot be understood solely through its current contractual status as a technology supplier or data processor. The company also carries an operational genealogy shaped by intelligence, defence, policing, border enforcement, and security-state infrastructures. This genealogy does not prove malicious intent in the NHS context. Nor does it mean that NHS patient data is being transferred to intelligence agencies. Such a claim would go beyond the available evidence. The more precise issue is structural: a form of data integration historically refined in intelligence and security environments is now being normalised inside civilian infrastructures of care.

Palantir's own public filings make this genealogy explicit. Its Form 10-K states that Gotham, the company's first platform, was built for government operatives in the defence and intelligence sectors. The filing states that Gotham enables users to identify hidden patterns across datasets ranging from signals intelligence to reports from confidential informants, and that it facilitates the hand-off between analysts and operational users who plan and execute real-world responses to identified threats (Palantir Technologies Inc., 2021).

This is the key point: Palantir's software is not merely a passive repository. Its core historical function is to transform fragmented data into operational knowledge - knowledge that can be acted upon.

This operational logic is visible in contemporary military systems. In 2026, the U.S. Marine Corps described the Maven Smart System as an AI-enabled command-and-control platform that ingests and fuses data from multiple sources to inform and accelerate fire missions. The same Marine Corps account frames modern military integration through concepts such as data meshes, AI workflows, machine-to-machine targeting, and the reduction of the sensor-to-shooter gap (U.S. Marine Corps, 2026).

The same logic appears in the U.S. Army's Tactical Intelligence Targeting Access Node, or TITAN. The Army awarded Palantir a \$178.4 million agreement to develop and deliver ten TITAN prototypes. According to the Army, TITAN leverages artificial intelligence and machine learning to process sensor data from space, high-altitude, aerial, and terrestrial layers, supporting targeting and situational awareness while reducing the sensor-to-shooter timeline (U.S. Army CPE ISW, 2024).

This correction matters. TITAN should not be described as a 1.784 billion dollar contract. The currently cited Army award is 178.4 million dollars. Precision is not a minor detail here; overstating the figure weakens the argument. The stronger point is not an inflated contract value, but the operational function of the system: turning multi-source sensor data into targeting-relevant knowledge.

The broader defence trajectory is even clearer in Maven. Reuters reported in March 2026 that the Pentagon planned to adopt Palantir's Maven AI system as a core military command-and-control platform and program of record. Reuters described Maven as a platform that analyses battlefield data, identifies targets, and rapidly processes information from satellites, drones, radar, sensors, and intelligence reports. Palantir says its software does not make lethal decisions and that humans remain responsible for selecting and approving targets (Reuters, 2026b).

The 10 billion dollar claim also requires careful wording. Reuters reported that the U.S. Army consolidated numerous Palantir-related contracts into an enterprise agreement allowing the option to purchase up to 10 billion dollars in products and services over a decade. The same report notes that the deal does not itself commit the Army to new purchases. It is therefore more accurate to describe this as an enterprise purchasing framework rather than a single direct Maven/TITAN contract (Reuters, 2025).

The logic is not confined to war. It also appears in immigration enforcement. According to 404 Media and the Electronic Frontier Foundation, Palantir has worked on an ICE tool called ELITE - Enhanced Leads Identification and Targeting for Enforcement - that can map potential deportation targets, produce dossiers, and provide confidence scores about current addresses. EFF, citing 404 Media's reporting, states that the tool receives address data from the Department of Health and Human Services, including Medicaid-linked sources, among others (404 Media, 2026; Electronic Frontier Foundation, 2026).

This is where the theoretical distinction becomes concrete. In the NHS context, the patient is not being treated as a suspect, enemy, or deportation target. That would be an inaccurate and inflammatory claim. But the ICE example demonstrates the general operational form of Palantir's architecture: heterogeneous personal data can be integrated, mapped, scored, and routed toward intervention. The same formal logic - identify, link, rank, prioritise, route, intervene - can travel across domains even when the object of intervention changes.

ICE's ImmigrationOS contract makes this even clearer. Wired reported that ICE is paying Palantir 30 million dollars to develop ImmigrationOS, a platform intended to provide near real-time visibility into self-deportations, support targeting and enforcement prioritisation, and streamline the identification and removal process (Wired, 2025).

Guardian reporting based on internal ICE documents, training materials, and emails also shows that Palantir tools were deeply embedded in ICE investigations and field operations, including Falcon and

Investigative Case Management systems used to search across government and private databases, analyse driver's license scans, use location data, and support enforcement operations (The Guardian, 2025).

This is why the data processor defence has limits. In legal terms, Palantir may not own the data and may process data only under client instructions. Yet in operational terms, its platforms can structure how data becomes actionable. The decisive question is not only who owns the data, but how data is transformed into a field of intervention.

The same pattern appears in financial enforcement. TechCrunch, summarising reporting based on records obtained by American Oversight, reported that the IRS Criminal Investigations office has used Palantir tools since at least 2018 and has paid the company about 130 million dollars to analyse financial records. American Oversight has separately sued for records concerning the use of Palantir systems by agencies including CDC, DHS, ICE, IRS, and SSA, arguing that the public deserves transparency about how sensitive personal data is collected, analysed, and safeguarded (TechCrunch, 2026; American Oversight, 2026).

European policing cases show that these concerns are not limited to the United States. In Germany, the Federal Constitutional Court ruled in 2023 that legal provisions in Hesse and Hamburg authorising automated police data analysis were unconstitutional because they insufficiently limited the creation of broad profiles and cross-references. The case concerned automated police data analysis and interpretation, and the Court treated such analysis as an interference with informational self-determination (German Federal Constitutional Court, 2023).

The Dutch case adds another dimension: secrecy. NL Times, citing Volkskrant's analysis of documents obtained under Dutch transparency law, reported that Dutch police have used Palantir software since 2012, that 99 percent of disclosed documents were blacked out, and that Dick Schoof was involved in the 2011 procurement as Director General of the Dutch police (NL Times, 2025).

Taken together, these cases show that Palantir's significance lies not only in its software products, but in a recurring operational pattern: fragmented data is integrated into an actionable field; persons become nodes within that field; and institutional decisions become faster, more centralised, and less transparent to those affected.

This is the deeper relevance for the NHS case. The concern is not that health care has become identical to war, policing, taxation, or deportation. The concern is that a security-state style of data integration - one historically shaped by intelligence, targeting, enforcement, and operational decision-making - is being translated into the civilian domain of care.

The object changes. The logic remains recognisable.

In war, the operational node may be a target. In immigration enforcement, it may be a deportable person. In tax enforcement, it may be a suspect financial relation. In policing, it may be a potentially suspicious association. In health care, it becomes the patient.

The patient is not transformed into an enemy. But the patient can become an operational object: a being whose needs, risks, movements, delays, vulnerabilities, and priorities become governable through an infrastructure of continuous calculation.

This is where the concepts of Onopticon and Homovictimus become sharper. Onopticon does not merely observe; it constructs the field in which a person becomes actionable. Homovictimus is not simply the harmed subject; it is the subject who must become processable in order to receive protection, care, or recognition. In the NHS-Palantir case, the danger is therefore not only privacy loss. It is the migration of actionable-intelligence logic into the infrastructure of care.

The Limit of the Data Processor Defence

The defence offered by NHS England and Palantir is largely framed in terms of legal roles. NHS England states that it remains responsible for the data, while Palantir is described in NHS documentation as a processor acting on behalf of NHS England and acting on NHS England's instructions (NHS England, 2026a).

This defence is not meaningless. The fact that Palantir does not legally own NHS data and is formally constrained by contractual and data-protection obligations is an important limitation.

However, legal role and infrastructural effect are not the same thing.

A company may not own the data, yet still shape how data is related, through which workflows it is processed, through which objects and categories it is read, through which dashboards it becomes visible, and into which operational decisions it is inserted.

The issue, therefore, is not the crude claim that sovereignty has been fully transferred to Palantir. A more precise formulation is this: sovereignty is not being completely transferred; rather, the way public authority exercises sovereignty is transformed as it becomes increasingly dependent on private data infrastructures.

In this transformation, sovereignty no longer resides only in law, ministries, or contracts. It is distributed across data models, APIs, access roles, integration layers, dashboards, and operational decision flows.

Public Benefit and Infrastructural Risk

A nostalgic defence of the fragmented-file regime is neither analytically serious nor ethically defensible. Fragmented health bureaucracies can kill through delay, duplication, miscommunication, lost records, and institutional blindness. Nor should one fall into the opposite error: a technological determinism that assumes integrated data systems will function neutrally, rationally, or benevolently simply because they promise coordination, speed, and optimisation.

The problem is not that integration has no value. It clearly does. The problem is that the life-saving promise of integration does not abolish the ontological reduction it performs.

Fragmented systems can delay care, duplicate procedures, obscure responsibility, and in extreme cases abandon patients to institutional failure. Integrated systems can shorten waiting lists, accelerate discharge, reduce administrative blindness, and help institutions identify patients who might otherwise disappear between fragmented systems. Yet integrated systems can also convert the patient into a continuously calculable object of intervention.

The task, therefore, is not to defend fragmentation against integration. The task is to ask what kind of subject is produced when integration becomes the condition of care.

This is the central tension of the NHS-Palantir case. Data integration may save lives; it may also reduce the patient to an object of continuous operational intervention. These two truths do not cancel each other.

The defence of the FDP is built precisely on the language of public benefit: connecting fragmented systems, enabling decision-makers to access the right information at the right time, and improving patient care. NHS England's privacy materials frame the FDP through purposes such as operational planning, care coordination, population health, and better data use (NHS England, 2026b).

Yet the public-benefit argument does not eliminate infrastructural risks. Indeed, this is one of the most powerful features of contemporary data regimes: domination often legitimises itself not through the language of coercion, but through the language of efficiency and care.

The issue, therefore, is not limited to the presence of Palantir. The deeper issue is that a public service binds its own capacity to function to private infrastructures. When public authority begins to perceive its own health reality through a private operational layer, the dependency becomes not merely technical but epistemic.

Onopticon: Not Merely Seeing, but Constructing

Classical discussions of surveillance are built around the visibility of the subject. In the Panopticon, power sees; the subject modifies behaviour because it knows it may be seen.

The NHS-Palantir case points to something further. The issue is not only that the patient is seen. The issue is the data forms within which the patient counts as real. For this reason, the concept of the Onopticon is more illuminating.

The Onopticon is not merely a system that observes. It is an infrastructural order that constructs reality, defines categories, identifies objects of intervention, and renders the subject calculable.

The patient is no longer merely visible to the system. The patient becomes a being that must be pre-processed for the system to function. The right to care is increasingly tied to the patient's readability within a data architecture.

At this point, the right to privacy becomes conceptually insufficient. Privacy asks: Who saw my data? The deeper question is: Am I required to become entirely calculable, predictable, and operationally governable?

This question leads to the right to opacity.

The Right to Opacity and Homovictimus

The right to opacity demands that the human being not be reduced to an entirely decipherable object of systems. In a vital domain such as health care, this right has particular significance. The patient cannot easily exit the system. In illness, "do not use it if you do not want to" is not a real option.

A person seeking health care must enter hospital records, digital systems, waiting lists, prescription infrastructures, laboratory platforms, and increasingly centralised data architectures. This inclusion is not a free choice. It is an existential necessity.

This is where the figure of Homovictimus appears.

Homovictimus is not merely a person who has been harmed. Homovictimus is the person who must accept their own processability in order to access a vital service. In the modern health system, the patient must first become a data form that the system can recognise in order to receive help.

This transformation does not occur through overt violence. Nobody says that the patient is being forcibly converted into a data object. On the contrary, the process operates through the language of care, speed, coordination, efficiency, and public benefit. Yet the outcome remains: because of biological vulnerability, the patient becomes bound to infrastructural readability.

Conclusion: The Ontological Transformation of the Patient

The NHS-Palantir case cannot be reduced to a narrow question of data-security protocols. Access controls, security clearance, public transparency, information governance, and accountability are all necessary. MPs and patient organisations have warned that Palantir's access to identifiable NHS England patient data may damage public trust and that the public has not been adequately consulted (The Guardian, 2026).

But these concerns do not exhaust the deeper question: Which infrastructure constructs public health reality?

What begins with Palantir is not the datafication of the patient. That process is a much older feature of modern health bureaucracy. What becomes visible through Palantir/FDP is the centralisation of datafication at the level of scale, integration, and decision architecture.

In the old regime, the patient was a clinical subject divided across fragmented files. In the new regime, the patient becomes a calculable operational node across systems.

This transformation also changes the form of the right to health. The right may continue to exist on paper; in practice, however, it becomes tied to infrastructural readability. To receive care, the patient must do more than become visible to the system. The patient must enter a form that the system can calculate, rank, relate, and manage.

This ontological rupture is intensified by Palantir's operational genealogy. The company's platforms have been used or described in contexts ranging from military targeting and battlefield command-and-control to immigration enforcement, financial crime investigation, and police data mining. The problem is not that health care has become identical to war, policing, or deportation. Rather, the problem is that a mode of data integration historically shaped by intelligence and security operations is being translated into the civilian domain of care.

The patient is not transformed into an enemy. But the patient can become an operational object: a being whose needs, risks, movements, delays, vulnerabilities, and priorities become governable through an infrastructure of continuous calculation.

The NHS-Palantir case is therefore more than a privacy crisis. It is an ontological rupture that reveals the passage of the modern patient from fragmented clinical records to operational nodes - and the migration of actionable-intelligence logic into the infrastructure of care.

References

- 404 Media. (2026, January 15). 'ELITE': The Palantir app ICE uses to find neighborhoods to raid. <https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/>
- American Oversight. (2026, April 21). American Oversight sues for records on Trump administration use of Palantir tools amid growing privacy, data collection concerns. <https://americanoversight.org/palantir-data-collection-tools-foia/>
- Electronic Frontier Foundation. (2026, January 15). Report: ICE using Palantir tool that feeds on Medicaid data. <https://www.eff.org/deeplinks/2026/01/report-ice-using-palantir-tool-feeds-medicaid-data>
- Financial Times. (2026, May 11). NHS to grant Palantir contractors 'unlimited access' to patient data. <https://www.ft.com/content/8ce1b9be-1d51-466b-90de-54bff1a504ca>
- German Federal Constitutional Court. (2023, February 16). Judgment of 16 February 2023 - automated data analysis by the police. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2023/02/rs20230216_1bvr154719en.html

- NHS England. (2026a, January 9). National Data Integration Tenant (NDIT) Federated Data Platform product privacy notice. <https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/security-privacy/nhs-fdp-information-governance-framework/national-fdp-products/national-data-integration-tenant-ndit-federated-data-platform-fdp-product-privacy-notice/>
- NHS England. (2026b). NHS Federated Data Platform privacy notice. <https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/security-privacy/nhs-fdp-privacy-notice/>
- NL Times. (2025, August 22). Dutch police also use controversial AI intelligence software by American Palantir. <https://nltimes.nl/2025/08/22/dutch-police-also-use-controversial-ai-intelligence-software-american-palantir>
- Palantir. (n.d.). Ontology building: Overview. <https://palantir.com/docs/foundry/ontology/overview/>
- Palantir Technologies Inc. (2021). Form 10-K annual report. U.S. Securities and Exchange Commission. <https://www.sec.gov/Archives/edgar/data/1321655/000119312521060650/d65934d10k.htm>
- Reuters. (2025, August 1). U.S. Army pools contracts into up to \$10 billion Palantir deal. <https://www.reuters.com/business/us-army-pools-contracts-into-up-10-billion-palantir-deal-2025-07-31/>
- Reuters. (2026a, May 11). Britain's NHS to grant Palantir contractors 'unlimited access' to patient data, FT reports. <https://www.reuters.com/world/uk/britains-nhs-grant-palantir-contractors-unlimited-access-patient-data-ft-reports-2026-05-11/>
- Reuters. (2026b, March 20). Pentagon to adopt Palantir AI as core U.S. military system, memo says. <https://www.reuters.com/technology/pentagon-adopt-palantir-ai-as-core-us-military-system-memo-says-2026-03-20/>
- TechCrunch. (2026, April 24). Palantir is reportedly helping the IRS investigate financial crimes. <https://techcrunch.com/2026/04/24/palantir-is-reportedly-helping-the-irs-investigate-financial-crimes/>
- The Guardian. (2025, September 22). Documents offer rare insight on ICE's close relationship with Palantir. <https://www.theguardian.com/us-news/ng-interactive/2025/sep/22/ice-palantir-data>
- The Guardian. (2026, May 11). Palantir's access to identifiable NHS England patient data is 'dangerous', MPs say. <https://www.theguardian.com/society/2026/may/11/palantir-access-nhs-england-patient-data>
- U.S. Army CPE ISW. (2024, March 6). Army Tactical Intelligence Targeting Access Node (TITAN) ground station prototype - award. <https://cpeisw.army.mil/2024/03/06/army-tactical-intelligence-targeting-access-node-titan-ground-station-prototype-award/>
- U.S. Marine Corps. (2026, March 27). Closing the sensor-to-shooter gap, one Dynamis serial at a time. <https://www.marines.mil/News/News-Display/Article/4445978/closing-the-sensor-to-shooter-gap-one-dynamis-serial-at-a-time/>
- Wired. (2025, April 18). ICE is paying Palantir \$30 million to build ImmigrationOS surveillance platform. <https://www.wired.com/story/ice-palantir-immigrationos/>