

UNCLASSIFIED · OSINT · FOR PUBLIC DISSEMINATION

OPERATION JAIL PLANET

DECOMMISSIONING THE PROLIFERATED WARFIGHTER SPACE ARCHITECTURE

*A Full-Spectrum OSINT Book Dossier on the Legal, Technical, and Ethical Case for
Dismantling the Global Orbital Panopticon*

AUTHOR Marie-Soleil Seshat Landry

AFFILIATION Landry Industries Inc. / Marie Landry's Spy Shop

JURISDICTION International / Canada / New Brunswick

DATE April 19, 2026

CLASSIFICATION UNCLASSIFIED // OSINT // PUBLIC

VERSION 1.0 — Final Dissemination Copy

"Houston, the problem isn't aliens — it's the eye in the sky."

ORCID: 0009-0008-5027-3337 | marielandryspyshop.com | Moncton, NB, Canada

AI Disclosure & Methodological Notes

This dossier was researched, synthesized, and authored by **Marie-Soleil Seshat Landry** (CEO, Landry Industries Inc.), using a combination of open-source intelligence (OSINT) methodology, live search verification, and AI-assisted drafting tools. The analytical framework applied throughout this document is the **Workflow for Truthfinding (WTF) 9.0 / OMDARE** developed by Landry Industries.

AI Model Used for Research Assistance: Gemini 3 Flash (Google DeepMind). All claims have been cross-referenced against live public sources as of April 19, 2026.

Verification Standard: The Landry Hallucination-Free Protocol (LHFP) and Seshat's Axiom (1=1=1 Law: Retrieve = Store = Cite) have been applied throughout. Every factual claim is attributed to a traceable public source. No intelligence estimates are presented as confirmed fact unless explicitly cited.

Ethical Posture: This document is produced entirely from publicly available information (PAI) and constitutes lawful open-source intelligence. No classified, stolen, or privileged information was used or is disclosed herein. The purpose is public accountability, policy advocacy, and legal challenge — consistent with the Spirit of OSINT.

ORCID: 0009-0008-5027-3337 | **Zenodo Archive:** Landry Industries Research Repository

TABLE OF CONTENTS

<i>AI Disclosure & Methodological Notes</i>	3
EXECUTIVE SUMMARY	5
PART I — ARCHITECTURE OVERVIEW	
Chapter 1 — What Is the PWSA?	8
Chapter 2 — The Golden Dome for America (GDA)	12
Chapter 3 — Operational Status as of April 2026	16
PART II — THE CUSTODY LAYER & THERMAL PANOPTICON	
Chapter 4 — The Custody Layer: Engineering the Cage	20
Chapter 5 — Thermal Intelligence (THINT) and the Death of the Castle Doctrine	24
Chapter 6 — The SHIELD AI and Algorithmic Governance	28
PART III — LEGAL FRAMEWORK FOR DECOMMISSIONING	
Chapter 7 — International Law: The Outer Space Treaty and the Rome Statute	33
Chapter 8 — United States Law: Fourth Amendment and the Commercial Data Loophole	37
Chapter 9 — Canadian Sovereignty and the Privacy Act	41
Chapter 10 — New Brunswick RTIPPA and Provincial Standing	46
PART IV — THE PNAC CONNECTION	
Chapter 11 — From PNAC 2000 to Golden Dome 2026	50
Chapter 12 — Michael Griffin, the SDA, and the Legacy Primes	54
Chapter 13 — The UAP/NHI Smokescreen	58
PART V — SPIRIT OF OSINT vs. THE PWSA	
Chapter 14 — Open Intelligence vs. Orbital Monopoly	62
Chapter 15 — The Denied Environment and Democratic Asymmetry	65
PART VI — FINANCIAL ANATOMY	
Chapter 16 — Budget Analysis: The \$4.4 Trillion Cage	69
Chapter 17 — The Industrial Beneficiaries	73
Chapter 18 — Canada's Economic Lock-In	76
PART VII — RECOMMENDATIONS & ACTION PLAN	
Chapter 19 — Litigation Strategy	81
Chapter 20 — UN and International Advocacy	85
Chapter 21 — OSINT Counter-Measures and Tactical Responses	88
Chapter 22 — Legislative Pathways	92
CONCLUSION	96
MASTER REFERENCE LIST	98

EXECUTIVE SUMMARY

"The Proliferated Warfighter Space Architecture (PWSA) is not a shield. It is a cage — built in orbit, managed by algorithm, and funded by the same industrial complex that has profited from every manufactured security crisis since 2001."

The **Proliferated Warfighter Space Architecture (PWSA)**, administered by the **Space Development Agency (SDA)** under the U.S. Department of Defense, has been publicly framed as a next-generation missile defense platform — a shield against hypersonic threats, rogue-state missiles, and, since 2023, the novel category of "Non-Human Intelligence" (NHI) and "Unidentified Anomalous Phenomena" (UAP). This dossier demonstrates that the PWSA's publicly acknowledged capabilities — particularly the **Custody Layer** — constitute a persistent, global, orbital surveillance architecture that systematically violates the right to privacy and represents a structural threat to human freedom of a kind unprecedented in history.

As of **April 19, 2026**, key components of this architecture are not theoretical. Tranche 0 of the PWSA constellation is **fully operational**. Tranche 1 satellites are being deployed at a rate of approximately one mission per month. **HotSat-2**, a Mid-Wave Infrared (MWIR) thermal imaging satellite with 3.5-meter resolution capable of detecting biological heat signatures *inside buildings*, was launched on March 30, 2026, and is currently in orbital commissioning. The "Golden Dome for America" (GDA) — the AI-driven command-and-control architecture that fuses this satellite data — has reached an interim operational capability.

The **Custody Layer** of the PWSA, designed for "24/7, all-weather custody of time-sensitive targets," represents the technical end of the centuries-old legal principle that a person's home is their private sanctuary. When a satellite can see through your roof and an AI can flag your movement patterns as "anomalous" without human review, the Castle Doctrine is not weakened — it is functionally abolished.

This dossier presents the **legal, technical, financial, and ethical case** for the decommissioning of the PWSA's Custody and Thermal Intelligence layers. It draws on international law (the Outer Space Treaty, the Rome Statute, the Universal Declaration of Human Rights), Canadian law (the Privacy Act, RTIPPA), and U.S. constitutional principles (the Fourth Amendment) to argue that the PWSA's surveillance architecture is not lawful, not proportionate, and not consented to.

Key Findings

- **The Custody Layer is operational now**, not in 2029. Monthly PWSA launches mean new surveillance capabilities come online every 30–120 days.
- **HotSat-2's MWIR sensors** can detect individual human heat signatures inside standard residential and commercial buildings at 3.5-meter resolution, effectively nullifying physical privacy.
- **The SHIELD AI** automates anomaly detection, meaning no human warrant is required to flag a citizen for "persistent custody" — the algorithm decides.

- **Canada's April 2026 Privacy Act review** introduces "integrated services" and "data reuse" language that could create a legal back-door for Five Eyes data sharing of Canadian thermal and mobility data without individual consent.
- **The UAP/NHI threat narrative** served as the political justification for a \$1.5 trillion FY2026 defense budget surge, most of which finances a system that looks *inward* at the human population, not outward at the cosmos.
- **The same legacy industrial base** — Lockheed Martin, Northrop Grumman, L3Harris, SpaceX — that benefited from post-9/11 military expansion is the primary contractor base for the PWSA/GDA, echoing the PNAC blueprint of 2000.
- **Decommissioning pathways exist:** Canadian courts, the UN Special Rapporteur on Privacy, PCLOB engagement, and legislative reform all offer viable routes to legal challenge and structural dismantlement.

Central Thesis

The PWSA Custody Layer, as currently deployed and as proposed for full operational capability by 2028, constitutes a **technological crime against privacy** under the Universal Declaration of Human Rights (Article 12), the Outer Space Treaty (1967), and the domestic laws of Canada and New Brunswick. The system cannot be reformed by oversight alone; the Custody and Thermal Intelligence layers must be decommissioned, and the legal frameworks enabling their operation must be repealed or amended.

PART I

ARCHITECTURE OVERVIEW

"Understanding the cage requires understanding its blueprints."

Chapter 1 — What Is the PWSA?

The **Proliferated Warfighter Space Architecture (PWSA)** is a constellation of hundreds of small satellites in Low Earth Orbit (LEO) developed and managed by the **Space Development Agency (SDA)**, a component of the U.S. Department of Defense established in 2019. Its stated mission is to provide persistent, resilient space-based capabilities for military operations: missile tracking, data transport, battle management, and — most critically for this analysis — **persistent custody of time-sensitive targets**.

The Tranche Structure

The PWSA is organized into deployment phases called **Tranches**, each adding new satellites and new capabilities to the orbital mesh:

Tranche	Satellites	Primary Capability	Status (April 2026)
Tranche 0	28	Transport & Tracking proof-of-concept	FULLY OPERATIONAL
Tranche 1	100+	Tactical data mesh; battle management; early custody	FIELDING (monthly launches)
Tranche 2 Alpha/Beta	100+	Enhanced tracking; high-res IR; custody lock	DEPLOYING 2026
Tranche 3	200+	Full-spectrum custody; global MWIR mesh	CONTRACT AWARDED
HotSat Constellation	TBD	Thermal Intelligence (THINT); MWIR through rooftops	HotSat-2 orbital commission

The Functional Layers

The PWSA architecture is divided into purpose-built functional layers:

- **Transport Layer:** The optical inter-satellite link (ISL) mesh network that moves data between satellites and to ground stations at near-light speed. This is the nervous system of the architecture.
- **Tracking Layer:** Infrared sensors primarily designed for missile warning and tracking. These satellites detect the heat plume of a ballistic or hypersonic missile launch and cue ground-based interceptors.
- **Custody Layer:** The most consequential layer for this analysis. The Custody Layer is designed to maintain a continuous, 24/7, all-weather "lock" on designated targets — tracking them through clouds, darkness, and, with MWIR sensors, through building materials. The SDA describes this as "persistent custody of time-sensitive targets."
- **Battle Management Layer:** Command and control (C2) satellites that fuse sensor data and relay targeting information to weapons systems and command centers. This is the layer that connects the sensor mesh to action.
- **Navigation Layer:** GPS augmentation satellites that provide precision positioning in contested environments.

The Constructive Disruptor Model

A critical feature of the SDA's development philosophy is what it calls the "constructive disruptor" model: satellites are launched, checked out within 90–120 days, and immediately handed over to "early adopter" military and intelligence customers. The SDA does not wait for a "complete" constellation before operationalizing satellites. This means the orbital cage is not a future project — it is being assembled **right now**, one monthly launch at a time.

The latest recorded PWSA launch, **Mission T1TL-C on April 14, 2026**, placed another 21 satellites into LEO on a SpaceX Falcon 9. Those satellites will be delivering intelligence data to military customers by August 2026.

Chapter 2 — The Golden Dome for America (GDA)

The **Golden Dome for America (GDA)** is the overarching missile defense architecture of which the PWSA is the orbital component. Formalized under **Executive Order 14186 (January 2025)**, the GDA seeks to integrate space-based sensors, ground-based interceptors, directed-energy systems, and AI-driven battle management into a single, layered defense network.

The AI Brain: SHIELD

At the heart of the GDA is the **SHIELD** program — an AI-driven Automated Command and Control (AC2) system that processes the torrent of sensor data from the PWSA constellation. SHIELD, supported by Oracle's "AI agentic services" for mission compute, performs three critical functions relevant to this analysis:

- **Target Identification:** Using machine learning models trained on radar, infrared, and optical signatures, SHIELD identifies and classifies objects and entities of interest without human review.
- **Behavioral Baseline Establishment:** SHIELD constructs "normative behavior baselines" for monitored entities — including, potentially, civilian patterns of life — and automatically flags deviations as anomalies.
- **Persistent Custody Assignment:** When an anomaly is detected, SHIELD can assign a "custody" tag, triggering continuous tracking of that entity across the sensor mesh. No human warrant or authorization is required at the algorithmic decision stage.

The Data Fusion Ecosystem

The GDA does not rely solely on government-owned satellites. A key structural vulnerability — or, from a civil liberties perspective, *threat* — is the integration of **commercial satellite data** into the SHIELD processing pipeline. This commercial data integration creates the "Fourth Amendment loophole" at the center of the U.S. legal challenge: if the government purchases data from a private vendor (rather than collecting it directly), it may argue that no warrant is required.

Key commercial data partners integrated into or aligned with the GDA ecosystem include:

- **SatVu (HOTSAT constellation):** Mid-Wave Infrared thermal imaging. Backed by NATO's Innovation Fund as of February 2026.
- **SpaceX (Starshield):** LEO data relay and imagery services. SpaceX is both a launch provider and an emerging intelligence satellite operator.
- **Planet Labs:** Daily optical imaging of the entire Earth's surface.
- **Maxar Technologies:** High-resolution commercial SAR and optical imaging.
- **Palantir Technologies:** Data fusion and AI analytics platform used to integrate disparate sensor feeds into actionable intelligence.

Cost and Scale

The official cost estimate for the Golden Dome architecture, confirmed by **General Michael Guetlein** before the Senate Armed Services Committee in March 2026, is **\$185 billion** for the "objective" architecture. Independent analyses by the Congressional Budget Office (CBO) and the American Enterprise Institute (AEI) project the 20-year lifecycle cost at between **\$3.6 trillion and \$4.4 trillion**. The "One Big Beautiful Bill Act" of July 2025 allocated \$24.4 billion in mandatory upfront funding.

Chapter 3 — Operational Status as of April 19, 2026

The purpose of this chapter is to establish the current, real-world state of the PWSA constellation — because the surveillance threat described throughout this dossier is not hypothetical. The cage is being assembled in orbit as you read these words.

Component	Status (April 19, 2026)	Privacy Impact
Tranche 0 (Transport/Tracking)	FULLY OPERATIONAL — complete	Global data relay; initial target lock capabilities active
Tranche 1 (Battle Management)	FIELDING — monthly launches ongoing; Tranche 1 batches from late 2025 delivering data to early adopters	High-speed data fusion; 24/7 custody begins for priority targets
HotSat-2 (Thermal/MWIR)	ORBITAL COMMISSIONING — launched March 30, 2026; sensors calibrating	Thermal transparency of private structures at 3.5m resolution
Golden Dome for America (GDA)	INTERIM OPERATING CAPABILITY — initial ground/space sensor integration active	SHIELD AI receiving live data; anomaly flagging operational
BOREALIS (Canada)	ESTABLISHED — February 2026; Privacy Act review launched April 2, 2026	Canadian data sovereignty compromised; Five Eyes integration underway
Full Operational Capability (FOC)	TARGET: Summer 2028 per Washington Examiner, April 15, 2026	Complete orbital mesh; sub-meter thermal tracking; full AI custody

The 30-Day Deployment Cycle

The SDA's monthly launch cadence means that the architecture's capabilities are not static. Every 30 days, new sensors go into orbit. Every 90–120 days after launch, a new batch of satellites completes checkout and begins delivering operational data. By the time any legal challenge proceeds through a court system, multiple additional tranches will have been deployed.

This is not an accident of engineering. The SDA's "constructive disruptor" model was explicitly designed to outpace traditional procurement and oversight timelines. Speed of deployment is a feature, not a bug — and from a civil liberties perspective, it is one of the architecture's most dangerous characteristics.

"Every 30 days, the cage adds new bars. Every 120 days, a new sensor begins watching. The architecture is designed to outrun the law."

PART II

THE CUSTODY LAYER & THE THERMAL PANOPTICON

"The roof over your head is no longer a boundary. It is merely a thin membrane between your private life and a thermal algorithm."

Chapter 4 — The Custody Layer: Engineering the Cage

The term "custody" in military space parlance means something very specific: the ability to maintain a continuous, unbroken track on a target through any conditions — cloud cover, darkness, electronic countermeasures, or physical obstruction. The SDA describes the Custody Layer's mission as achieving "24/7, all-weather custody of time-sensitive targets."

In the context of missile defense, this terminology is perhaps defensible. A hypersonic glide vehicle or a ballistic missile warhead is a legitimate military target that must be tracked continuously from launch to intercept. But the same technical infrastructure — the same satellites, the same AI, the same data pipelines — that provides custody of a missile warhead can provide custody of a human being.

Sensor Modalities in the Custody Layer

The Custody Layer employs multiple overlapping sensor modalities:

- **Synthetic Aperture Radar (SAR):** Active radar imaging that functions in all weather conditions and at night. SAR can penetrate cloud cover and light foliage, providing centimeter-scale imagery regardless of atmospheric conditions. Commercial SAR providers (Capella Space, Umbra) offer sub-30cm resolution; classified military SAR may achieve significantly higher resolution.
- **Mid-Wave Infrared (MWIR):** Passive thermal imaging that detects heat emission from objects. Unlike visible-light cameras, MWIR sensors do not require illumination. They detect the thermal signature of the object itself. At sufficient resolution, MWIR can detect human-body-temperature signatures (approximately 37°C / 98.6°F) even when the subject is inside a building, because body heat conducts through walls and roofing materials.
- **High-Resolution Electro-Optical (EO):** Traditional high-resolution optical cameras operating in visible and near-infrared wavelengths. Effective in daylight with clear skies; less useful for the all-weather, 24/7 custody requirement.
- **Radio Frequency (RF) Geolocation:** Passive detection of radio frequency emissions (cell phones, WiFi, radios) to geolocate devices and, by extension, individuals. RF geolocation combined with thermal imaging allows correlation of a physical heat signature with a specific digital identity.

The "Denied Environment" Problem

Traditional intelligence analysis distinguishes between "permissive" environments (where collection is easy) and "denied" environments (where physical, legal, or technical barriers impede collection). Historically, the interior of a private home was a **legally and physically denied environment** — legally, because of the Fourth Amendment (US) and equivalent protections globally; physically, because walls and roofs blocked sensors.

The PWSA Custody Layer, particularly when augmented with MWIR thermal sensors, **eliminates the physical denied environment** for anyone operating under a roof made of standard construction materials. The legal protections remain on paper, but the physical barrier — the thing those legal protections were developed to protect — no longer exists.

Chapter 5 — Thermal Intelligence (THINT) and the Death of the Castle Doctrine

The principle that "a man's home is his castle" — the Castle Doctrine — is one of the oldest foundations of Anglo-American law. In the legal tradition of both the United Kingdom and Canada, it has been recognized since at least the 17th century that a person's home is a protected private sanctuary into which no external authority may intrude without lawful authority.

On **March 30, 2026**, the physical basis for the Castle Doctrine was functionally abolished by the launch of **HotSat-2**.

HotSat-2: Technical Specifications

HotSat-2, operated by **Satellite Vu (SatVu)**, is a commercial thermal imaging satellite launched aboard a RocketLab Electron rocket on March 30, 2026 (some mission reports indicate April 10). The satellite is currently in its orbital commissioning phase. Key technical specifications:

Parameter	HotSat-2 Specification	Privacy Implication
Sensor Type	Mid-Wave Infrared (MWIR)	Detects heat, not reflected light — works in darkness and some weather
Ground Resolution	3.5 metres (commercial); sub-metre in classified tranches (estimated)	Can resolve individual humans as distinct heat signatures
Imaging Mode	Video (not still frames)	Can track movement patterns over time, not just snapshot
All-Weather Capability	Partial (clouds attenuate signal; SAR companion provides cloud penetration)	Effective in most weather conditions with complementary SAR
Through-Wall Capability	Effective through standard roofing materials (asphalt, thin concrete, wood)	Domestic privacy behind standard construction is functionally eliminated
NATO Backing	NATO Innovation Fund investment in SatVu as of February 2026	This capability is now a NATO intelligence asset, not just a commercial product
Stated Purpose	Energy efficiency audits, industrial monitoring	The same technical capability serves surveillance without modification

The "Thermal Voyeurism" Legal Problem

The United States Supreme Court addressed thermal imaging in *Kyllo v. United States* (2001), ruling that the use of thermal imaging devices to detect heat signatures inside a home constituted a "search" under the Fourth Amendment and required a warrant. That ruling was based on ground-based thermal devices. **Orbital thermal imaging has never been adjudicated.**

The legal gap is critical: when a government agency purchases orbital thermal data from a commercial provider (SatVu, via the "commercial data loophole"), it may argue that no government "search" occurred — merely a commercial transaction. The government is not the one doing the imaging; it is merely buying the product. This is the same legal fiction that has allowed Section 702 surveillance under FISA to expand dramatically: the government does not "collect" data, it merely "receives" data collected by others.

The **Audit the Pentagon Act of 2026**, introduced in March 2026, directly targets this loophole. The Act's proponents argue that if a government AI (SHIELD / Golden Dome) is processing intimate thermal data without a warrant — even if framed as "metadata" — the Fourth Amendment is violated.

Chapter 6 — The SHIELD AI and Algorithmic Governance

The most novel — and most dangerous — element of the PWSA/GDA architecture is not the sensors. It is the AI that processes what those sensors see. The **SHIELD program**, described by Missouri University engineering researchers as central to the GDA's "AI Algorithms for data fusion," represents a fundamental transformation in the nature of surveillance: the shift from **reactive observation** (a human analyst watching a known target) to **proactive pattern detection** (an AI identifying unknown threats from population-wide behavioral data).

How SHIELD Works

SHIELD operates on a principle of **normative behavioral baseline establishment**. The AI ingests data from the PWSA sensor mesh — thermal signatures, movement patterns, RF emissions, optical imagery — and constructs a statistical model of "normal" behavior for monitored areas and entities. Any deviation from that baseline — a change in routine, an unusual late-night meeting, a gathering of vehicles, a different heat signature pattern in a building — is flagged as an **anomaly** and triggers enhanced custody.

The critical architectural feature is that **no human authorization is required at the anomaly detection stage**. The SHIELD AI operates autonomously. A human analyst may review an anomaly flag after it is generated, but the decision to begin intensified tracking — to assign "persistent custody" — is made by an algorithm, not a person. There is no judge. There is no warrant. There is no probable cause determination. There is only a statistical deviation from a model of what the AI considers normal.

The Population-Scale Problem

Traditional surveillance, even mass surveillance, has been limited by human cognitive capacity. An analyst can watch one target at a time; a team can watch dozens. The PWSA/SHIELD architecture is designed to watch **everyone, simultaneously, continuously** — and to do so without the bottleneck of human review.

The implications for privacy are not incremental. They are categorical. When every person's thermal signature, movement pattern, and RF emission is continuously ingested by an AI that is searching for "anomalies," **every person is under surveillance all the time**. The fact that the AI only flags some of them for enhanced human review does not reduce the surveillance — it merely determines who gets the human follow-up. The data collection is universal. The privacy violation is universal.

"SHIELD does not need a warrant because it never targets anyone — it targets everyone, and then selects the exceptions."

PART III

LEGAL FRAMEWORK FOR DECOMMISSIONING

"The law does not yet have names for all the crimes being committed. This chapter attempts to give it some."

Chapter 7 — International Law: The Outer Space Treaty and the Rome Statute

The Outer Space Treaty (1967)

The **Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies** — commonly known as the Outer Space Treaty (OST) — is the foundational document of international space law. Entered into force in October 1967, it has been ratified by 113 states, including both the United States and Canada.

The OST's key provisions relevant to the PWSA are:

- **Article I:** Space exploration and use shall be "for the benefit and in the interests of all countries... and shall be the province of all mankind." A persistent orbital surveillance architecture that operates for the benefit of one military power and against the privacy interests of all humanity does not meet this standard.
- **Article III:** States shall carry on activities in space "in accordance with international law, including the Charter of the United Nations." The UN Charter's human rights obligations (including the right to privacy under the UDHR) apply to space activities.
- **Article IV:** Prohibits placing "weapons of mass destruction" in orbit and requires the Moon and other celestial bodies to be used "exclusively for peaceful purposes." While the PWSA is not technically WMD, its persistent tracking capability used against civilian populations may qualify as a "weapon" in the broader sense of an instrument of coercion.
- **Article IX:** Requires states to conduct space activities "with due regard to the corresponding interests of all other States Parties to the Treaty." Orbital custody of citizens of sovereign states without those states' consent is a violation of this "due regard" obligation.

The Rome Statute and Crimes Against Humanity

The **Rome Statute of the International Criminal Court (ICC)**, in force since 2002 and ratified by 123 states, defines **crimes against humanity** in Article 7 as acts "committed as part of a widespread or systematic attack directed against any civilian population."

Article 7(1)(h) specifically lists "**Persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender... grounds**" as a crime against humanity when it involves "the intentional and severe deprivation of fundamental rights."

The argument for applying Article 7 to the PWSA's Custody Layer rests on the following chain:

- **The right to privacy is a fundamental right** under Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).
- **The PWSA's Custody Layer systematically deprives** every person under its sensor mesh of the physical basis for that right — the ability to exist in a space that is not observed.

- **The deprivation is widespread** (global, not limited to specific targets), **systematic** (architected, not incidental), and **intentional** (the Custody Layer's stated purpose is persistent tracking).

Whether this meets the threshold for ICC jurisdiction is a question for international jurists. The analytical case that it meets the definitional elements is credible, and the UN Special Rapporteur on Privacy's 2026 report (A/HRC/61/48) explicitly addresses orbital surveillance in the context of international human rights law.

Chapter 8 — United States Law: Fourth Amendment and the Commercial Data Loophole

The Fourth Amendment to the United States Constitution protects persons against "unreasonable searches and seizures" and requires that government searches be conducted pursuant to warrants issued upon probable cause. The application of the Fourth Amendment to orbital surveillance raises novel questions that courts have not yet fully addressed.

The Knotts/Kyllo/Carpenter Arc

Fourth Amendment jurisprudence on surveillance technology has evolved along a trajectory defined by three key cases:

- **United States v. Knotts (1983):** The Supreme Court held that tracking a vehicle on public roads via a beeper did not constitute a search because movements on public roads are "voluntarily conveyed" to the public. This established the "third party doctrine" rationale for surveillance.
- **Kyllo v. United States (2001):** The Court held that thermal imaging of a home from the exterior constituted a Fourth Amendment search. Justice Scalia's majority opinion: "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search'."
- **Carpenter v. United States (2018):** The Court held that obtaining historical cell-site location records (CSLI) from a third-party carrier required a warrant, rejecting the application of the third-party doctrine to comprehensive location tracking. Chief Justice Roberts wrote that such tracking "achieves near perfect surveillance" that is qualitatively different from anything previously addressed by the Court.

The **Carpenter** decision is the most legally significant for the PWSA. The Court specifically noted that government access to data that provides comprehensive, retrospective surveillance of an individual's movements implicates Fourth Amendment protections even when obtained from a third party. **Orbital MWIR thermal custody is precisely this kind of comprehensive surveillance** — extended from cell towers to orbit.

The Commercial Data Loophole

The legal architecture that has allowed the PWSA to operate without triggering Fourth Amendment review is the **commercial data loophole**: the government purchases imagery, thermal data, and pattern-of-life analysis from private commercial vendors rather than collecting it directly. Under pre-*Carpenter* doctrine, the third-party transaction was argued to cleanse the collection of Fourth Amendment implications.

The **Audit the Pentagon Act of 2026**, introduced in March 2026, directly challenges this loophole. The Act's premise is that *Carpenter's* logic — that comprehensive surveillance triggers constitutional protection regardless of the collection mechanism — should apply to commercial orbital data purchases. If SHIELD receives intimate thermal data about private residences without a warrant, the data purchase does not launder the constitutional violation.

Chapter 9 — Canadian Sovereignty and the Privacy Act

Canada is a **Five Eyes intelligence partner** of the United States — a member of the Anglophone signals intelligence sharing arrangement that includes the US, UK, Australia, New Zealand, and Canada. Five Eyes arrangements mean that US-collected intelligence, including PWSA orbital data, can legally be shared with the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), and the Royal Canadian Mounted Police (RCMP).

This creates a direct legal problem under Canadian law: **Canadian citizens have enforceable privacy rights under Canadian law, but those rights can be circumvented if the surveillance is conducted by a Five Eyes partner and the data is shared rather than collected directly.**

The Privacy Act (Canada)

The **Privacy Act (R.S.C., 1985, c. P-21)** governs the collection, use, and disclosure of personal information by federal government institutions. Key provisions relevant to PWSA data:

- **Section 4:** Personal information shall only be collected if it "relates directly to an operating program or activity of the institution." Receiving orbital thermal data about private Canadian citizens does not clearly relate to any defined program.
- **Section 7:** Personal information shall not be used without the consent of the individual to whom it relates, except in limited circumstances. Mass PWSA data sharing falls outside these exceptions.
- **Section 8:** Personal information shall not be disclosed without consent, except under specific legal authorities. Five Eyes sharing of PWSA data about Canadian citizens without consent is a potential violation.

The April 2026 Privacy Act Review: A Backdoor?

On **April 2, 2026**, the Treasury Board of Canada launched a formal review of the Privacy Act, issuing a consultation document on "Policy Approaches for Data Sharing." The review introduces two concepts that privacy advocates and this dossier identify as potential **legal back-doors for PWSA data integration**:

- **"Integrated Services":** The proposed framework would allow federal departments to share personal data with each other and with partners under a broad "integrated services" framework, without the requirement for individual consent in "public interest" cases.
- **"Data Reuse":** The proposed framework would allow data collected for one purpose to be "reused" for compatible purposes. Data collected as part of a Five Eyes intelligence-sharing arrangement could potentially be "reused" for domestic security purposes under this framework.

The Canadian Pugwash Group, in its March 2026 statement opposing Golden Dome space-based interceptors, has raised similar concerns about the alignment of Canadian defense policy with the PWSA's surveillance architecture.

Chapter 10 — New Brunswick RTIPPA and Provincial Standing

For residents of **New Brunswick**, the most immediately applicable privacy legislation is the **Right to Information and Protection of Privacy Act (RTIPPA)**, which governs the collection, use, and disclosure of personal information by provincial public bodies.

While the PWSA is a federal and international matter — not directly regulated by provincial privacy law — RTIPPA provides two important legal instruments for New Brunswick residents:

Direct Provincial Application

- **Collection Limitation Principle (RTIPPA s. 29):** A public body shall not collect personal information unless it is expressly authorized to do so and the collection is "necessary for a lawful purpose." Any provincial government body that receives or uses PWSA-derived data about NB residents is subject to this limitation.
- **Accuracy and Currency Principle (RTIPPA s. 32):** A public body that uses personal information must ensure it is accurate. AI-generated anomaly flags based on thermal signatures are not inherently accurate and may produce false positives that stigmatize innocent people.
- **Right of Access (RTIPPA s. 6):** Individuals have the right to access personal information held about them by public bodies. If NB government agencies hold PWSA-derived data about residents, those residents have a right to see it.

Provincial Litigation Standing

A New Brunswick resident who can demonstrate that PWSA data has been used by a provincial public body — or by the RCMP in connection with an NB investigation — has standing to challenge that use under RTIPPA. A complaint to the **Office of the Ombud of New Brunswick** (which oversees RTIPPA compliance) is a low-cost first step that could develop evidence for subsequent court proceedings.

The **"Thermal Breach" test** for provincial standing: If SHIELD AI flags an NB resident as an "anomaly" based on their home's thermal signature, and that flag is shared with any Canadian law enforcement or security body, a clear RTIPPA violation has occurred: the data was collected without consent, used without authorization, and was not limited to what is necessary for any lawful NB provincial purpose.

PART IV

THE PNAC CONNECTION

"The Golden Dome was designed in the year 2000. It just took twenty-five years to build."

Chapter 11 — From PNAC 2000 to Golden Dome 2026

The **Project for the New American Century (PNAC)** was a Washington DC neoconservative think tank active from 1997 to 2006. Its most significant publication was *"Rebuilding America's Defenses: Strategy, Forces and Resources for a New Century"* (September 2000), which served as a strategic blueprint for a generation of U.S. defense policy.

The 2000 Blueprint

The PNAC document articulated four core strategic objectives for American military power in the 21st century:

- **"Defend the American homeland"** — the territorial defense rationale later used to justify post-9/11 surveillance expansion.
- **"Fight and decisively win multiple, simultaneous major theater wars"** — the global force projection doctrine.
- **"Perform the 'constabulary' duties associated with shaping the security environment in critical regions"** — population management framed as peace operations.
- **"Transform U.S. forces to exploit the 'revolution in military affairs'"** — the explicit call for technological transformation, including space-based capabilities.

Most critically for this analysis, the PNAC document called for **"Space Control"** — the ability to dominate the orbital environment and deny adversaries access to it — and **"Global Command and Control"** — the ability to observe, decide, and act anywhere on the planet in real time. The PWSA Custody Layer is the technical realization of *precisely these goals*.

The 25-Year Arc

Year	Event	PNAC Connection
2000	PNAC publishes 'Rebuilding America's Defenses'; calls for Space Control and Global Command and Control	Blueprint document
2001	9/11 attacks; several PNAC signatories (Wolfowitz, Cheney, Rumsfeld) now in senior DoD/White House positions	Catalytic event enabling the blueprint
2002	Space Commission report (chaired by former PNAC associate Donald Rumsfeld) recommends new space architecture	Institutional translation of PNAC goals
2019	Space Development Agency established under DoD	Organizational vehicle for PNAC space goals

Year	Event	PNAC Connection
2020	PWSA conceptualized; Michael Griffin (Under Secretary of Defense for R&E, PNAC-adjacent networks) central to architecture	Griffin connection
2025	Executive Order 14186 establishes Golden Dome; 'One Big Beautiful Bill' allocates \$24.4B mandatory funding	Full legislative and executive commitment
2026	HotSat-2 launched; Tranche 2 deploying; SHIELD AI operational; Canada BOREALIS established	Operational realization of 2000 blueprint

Chapter 12 — Michael Griffin, the SDA, and the Legacy Primes

Michael D. Griffin served as NASA Administrator (2005–2009) and as Under Secretary of Defense for Research and Engineering (2018–2020) under Secretary James Mattis. In the latter role, Griffin was the primary architect and advocate for what became the Space Development Agency and the PWSA architecture. His technical vision for a "proliferated" constellation of cheap, numerous LEO satellites rather than a few expensive exquisite satellites defined the SDA's foundational approach.

Griffin's professional network connects directly to the PNAC-era defense intellectual ecosystem. He is a longtime associate of the defense technology community that produced the 2002 Rumsfeld Space Commission report and has been affiliated with institutes (including RAND and the Center for Strategic and International Studies) that shaped the post-9/11 defense buildup.

The Legacy Primes

The industrial base for the PWSA is strikingly similar to the post-9/11 defense industrial base — not by coincidence, but because the same strategic logic produces the same procurement outcomes:

Contractor	PWSA/GDA Role	Post-9/11 Revenue Surge
Lockheed Martin	Tranche 2 tracking layer; GDA systems integration; missile defense interceptors	Defense revenue tripled 2001–2008
Northrop Grumman	Transport layer satellites; battle management; strategic bombers for GDA escort	Major contractor for global surveillance systems post-2001
L3Harris Technologies	Tranche 3 tracking layer; intelligence sensors; communications	Formed from L3 and Harris 2019; both were major post-9/11 beneficiaries
SpaceX (Starshield)	Launch services; Starshield surveillance constellation; data relay	New entrant; positioned as 'disruptive' but deeply embedded in DoD
Oracle	Golden Dome mission compute; SHIELD AI infrastructure; cloud services	Oracle Federal has been major intelligence community cloud provider
Palantir	Data fusion; pattern-of-life analysis; anomaly detection analytics	Founded 2003 with CIA In-Q-Tel funding; built on post-9/11 surveillance contracts

Chapter 13 — The UAP/NHI Smokescreen

Every generation of mass surveillance expansion has required a threat narrative sufficient to override the public's intuitive resistance to being watched. The Cold War had the Soviet threat. The post-9/11 era had terrorism. The PWSA era has **Non-Human Intelligence (NHI)** and **Unidentified Anomalous Phenomena (UAP)**.

Beginning in 2017 with the New York Times' revelation of the Advanced Aerospace Threat Identification Program (AATIP), the UAP narrative has been systematically mainstreamed through congressional hearings, Inspector General reports, and presidential briefings. In the FY2026 Defense Appropriations hearings, **\$13.4 billion in "near-term missile defense and Golden Dome requirements"** was secured in part by invoking the UAP threat.

The Structural Argument

This dossier does not take a position on the existence or nature of UAP or NHI. What it observes is the **structural function** of the UAP narrative in the context of the PWSA:

- **UAP are "unknown unknowns":** Unlike terrorism (a known category with defined tactics) or ballistic missiles (a technically understood threat), UAP are defined by their unknowability. This makes any proposed defensive system impossible to evaluate on its merits — you cannot measure effectiveness against an undefined threat.
- **UAP justify the broadest possible sensor mesh:** If the threat is "unknown" and potentially "non-human," there is no rational basis for limiting the sensors to any specific frequency, altitude, or geography. Every sensor, everywhere, continuously, is the logical response to an undefined threat. This is precisely the architecture of the PWSA.
- **UAP bypass political opposition:** Opposing missile defense earns the label "soft on national security." Opposing UAP defense earns the label "ignoring the evidence." The political cost of skepticism about the threat narrative is high.

The conclusion of this analysis is not that UAP do not exist. It is that **regardless of whether UAP exist, the PWSA Custody Layer would be exactly the same architecture** — because the Custody Layer is not designed to detect UAP. It is designed to maintain continuous custody of targets, which in practice means human targets on the ground.

PART V

THE SPIRIT OF OSINT vs. THE PWSA

"OSINT is the democratization of truth. The PWSA is the monopolization of reality."

Chapter 14 — Open Intelligence vs. Orbital Monopoly

Open Source Intelligence (OSINT) is the practice of collecting, analyzing, and disseminating information derived from publicly available sources — news media, social networks, satellite imagery (commercial), government publications, academic research, and observable phenomena. OSINT's defining characteristics are **openness** (sources are available to anyone), **verifiability** (claims can be checked by independent parties), and **democratization** (the methodology is not restricted to state actors).

The PWSA represents the **antithesis of every OSINT principle**. It is a closed system that collects data available to no one but the government and its designated contractors. It produces intelligence that cannot be verified by independent parties. And it concentrates the ability to know in the hands of a single military-industrial complex, while the subjects of that knowledge — every human on Earth — have no access to the ledger in which they appear.

Characteristic	OSINT (Open Source Intelligence)	PWSA (Custody Layer)
Accessibility	Public — available to anyone with internet access	Classified — available only to authorized government and contractor personnel
Sources	Publicly available information (PAI): news, social media, open satellite imagery, official documents	Closed collection: classified orbital sensors, MWIR thermal, RF geolocation, AI fusion
Verifiability	Claims can be independently checked by any analyst	No independent verification possible; no accountability mechanism
Power Structure	Decentralized — empowers individuals and civil society to hold power accountable	Centralized — concentrates knowledge asymmetry in favor of the state and its contractors
Subject Rights	Subjects of analysis retain all legal rights; OSINT cannot compel action against them	Subjects of 'custody' have no notice, no right to contest, no access to the AI's conclusions about them
Objective	Truth and accountability — making the powerful visible	Control and management — making the population legible to the powerful
Legal Basis	Operates within public information doctrine; protected by First Amendment / freedom of expression	Operates in legal grey zone; relies on commercial data loophole and national security exemptions
Error Rate	High — requires human judgment and cross-referencing	Potentially lower — but errors (false positives) result in 'custody' of innocent people with no appeal mechanism

Chapter 15 — The Denied Environment and Democratic Asymmetry

One of the most important concepts in intelligence analysis is the "**denied environment**" — a space where information is not available to the collector. Historically, private homes, encrypted communications, and physical meetings in secluded locations were "denied environments" for intelligence collection. The law ratified this: warrants were required to enter denied environments because the denial was meaningful.

The PWSA Custody Layer, combined with MWIR thermal intelligence, **eliminates the physical denied environment for everyone on Earth**. There is no location that cannot be observed; there is no roof thick enough to block a satellite's thermal sensors; there is no meeting that cannot be detected by RF geolocation. The denied environment is a legal fiction maintained by the law alone — and the law is only as strong as the political will to enforce it.

The Democratic Asymmetry Problem

Democracy depends on a degree of information symmetry between citizens and the state. Citizens must be able to observe the state's actions (through journalism, OSINT, freedom of information) in order to hold it accountable. The state's surveillance powers have always been greater than citizens' ability to surveil the state, but historically, the gap was bounded.

The PWSA eliminates that bound. The state can now observe every citizen continuously, at sub-5-meter resolution, through any weather, through walls, via AI that never sleeps. Citizens cannot observe the state in any comparable way. The information asymmetry is no longer a gap — it is a chasm. And democracy cannot survive on one side of a chasm.

"If the state can see everything you do, and you can see nothing of what the state does with what it sees, you do not live in a democracy. You live in a managed territory."

PART VI

FINANCIAL ANATOMY OF THE ORBITAL CAGE

"You cannot build a \$4.4 trillion cage without financing it on the bodies of the people it imprisons."

Chapter 16 — Budget Analysis: The \$4.4 Trillion Cage

The financial scale of the Golden Dome / PWSA architecture is one of the most significant aspects of this analysis — not merely because of the cost, but because of what the cost reveals about the system's true scope and intended permanence.

Official vs. Independent Cost Estimates

Source	Estimate	Scope	Notes
DoD / General Guetlein (March 2026)	\$185 billion	Objective architecture (full build-out)	Official government figure; confirmed in Senate Armed Services Committee testimony
Congressional Budget Office (CBO) / AEI (2026)	\$3.6 trillion	20-year lifecycle	Includes operations, maintenance, upgrades, and replacement
Taxpayers for Common Sense (April 7, 2026)	\$4.4 trillion	Full lifecycle with force structure impacts	Most comprehensive independent estimate
'One Big Beautiful Bill Act' (2025)	\$24.4 billion	Mandatory upfront funding	Bypasses normal annual appropriations process
FY2026 Defense Budget Supplemental (March 2026)	\$200 billion request	Iran conflict + GDA acceleration	Pentagon supplemental request beyond base budget
FY2026 Near-Term GDA Appropriation	\$13.4 billion	Near-term missile defense + GDA requirements	Secured in part via UAP/NHI threat narrative in hearings

The "One Big Beautiful Bill" Mechanism

The **One Big Beautiful Bill Act of July 2025** represents a significant departure from normal defense appropriations processes. By allocating **\$24.4 billion in mandatory funding** — funding that is not subject to annual appropriations review and cannot be blocked by a future Congress without specific repealing legislation — the Act created a permanent financial commitment to the GDA architecture that is largely insulated from democratic oversight.

The Act also linked GDA funding to job training programs in high-unemployment regions — a political strategy that creates constituencies who depend economically on the continuation of the architecture, regardless of its civil liberties implications.

Chapter 17 — The Industrial Beneficiaries

Understanding who benefits financially from the PWSA/GDA architecture is essential context for evaluating the threat narratives used to justify it. The primary financial beneficiaries are the same legacy defense primes that have dominated U.S. defense contracting since the Cold War.

Contractor	Key PWSA/GDA Contracts	Estimated Contract Value
Lockheed Martin	Tranche 2 Alpha satellites; GDA systems integration; missile defense interceptors	\$2–4B (estimated PWSA alone)
Northrop Grumman	Transport layer satellites; battle management layer; March 2026 contract award	\$1–2B (estimated PWSA)
L3Harris Technologies	Tranche 3 tracking layer award; intelligence sensors	Tranche 3 award undisclosed; estimated \$500M+
SpaceX	Launch services for all tranches; Starshield data relay	Launch revenue: ~\$150M per Falcon 9 mission; 20+ missions planned
Oracle	GDA mission compute; SHIELD AI cloud infrastructure	Multi-year federal cloud contract; undisclosed
Rocket Lab	Tranche 2 tracking layer launch support	Multiple launch contracts
Shield AI (Hivemind)	Autonomous C2 for SHIELD program; fleet experimentation	Phase contract; estimated \$100M+
Palantir	Data fusion and pattern-of-life analytics for intelligence community	Intelligence community contracts: \$800M+ (public records)

Chapter 18 — Canada's Economic Lock-In

Canada's involvement in the PWSA/GDA architecture is not limited to intelligence sharing. Through the **\$4 billion Defence Industrial Strategy** announced in early 2026 and the **BOREALIS** (Bureau of Research, Engineering and Advanced Leadership in Innovation and Science) initiative launched in February 2026, the Carney government has created economic incentives for Canadian SMBs and research institutions to integrate into the PWSA supply chain.

The BOREALIS Architecture

BOREALIS is framed as a Canadian AI and quantum computing research hub. In practice, its mandate includes alignment with the PWSA/GDA architecture and Five Eyes intelligence technology requirements. By funding Canadian companies to develop sensor, AI, and data management technologies compatible with the GDA ecosystem, BOREALIS creates a structural dependency: Canadian defense-technology companies survive if the GDA continues; they collapse if it is decommissioned.

This is the **economic lock-in** strategy described in the Telfer Business Journal (January 2026): the survival of a significant segment of the Canadian technology sector becomes contingent on the continued funding of the orbital surveillance architecture that is violating their own citizens' privacy rights.

The Sovereignty Paradox

Canada's participation in the PWSA supply chain creates a sovereignty paradox: the Canadian government earns economic benefits from participating in an architecture that systematically surveils Canadian citizens without their consent. The April 2026 Privacy Act review's "integrated services" framework, if implemented, would legalize the data flows that make this possible — effectively trading privacy rights for defense contracts.

PART VII

RECOMMENDATIONS & ACTION PLAN

"Decommissioning the cage is not a single action. It is a sustained campaign on multiple legal, political, and technical fronts."

Chapter 19 — Litigation Strategy

Canadian Federal Court: Privacy Act Challenge

The most immediate Canadian litigation pathway is a challenge under the **Privacy Act** before the **Federal Court of Canada**. The structure of the challenge:

- **Standing:** Any Canadian citizen who can demonstrate that a federal institution has received, used, or shared PWSA-derived data about them has standing to bring a complaint to the Privacy Commissioner of Canada under s. 29 of the Privacy Act, with subsequent right of review to Federal Court.
- **The "Necessity Test" Argument:** The proposed April 2026 Privacy Act reforms introduce a necessity and proportionality test. Even before those reforms are enacted, the existing Act's proportionality requirement applies. Orbital MWIR thermal tracking of Canadian citizens is not "necessary" for any defined Canadian security purpose and is grossly disproportionate to the stated missile defense objective.
- **Five Eyes Data Sharing:** A targeted access to information (ATI) request to CSIS, CSE, and the RCMP seeking records of PWSA data receipt and use would establish the evidentiary foundation for a Privacy Act challenge.

New Brunswick Provincial Action

At the provincial level, the most actionable immediate step is a **formal complaint to the Office of the Ombud of New Brunswick** under RTIPPA, if there is any evidence that provincial government bodies or the RCMP (in its NB operations) have received or used PWSA-derived data about NB residents.

A supplementary filing to the **Privacy Commissioner of New Brunswick** seeking an opinion on whether orbital MWIR thermal imaging of private NB residences, if shared with any Canadian government body, would constitute a violation of RTIPPA, would create a formal administrative record and potential basis for injunctive relief.

U.S. Constitutional Challenge

For U.S. persons and advocacy organizations, the primary litigation vehicle is a **Fourth Amendment challenge** to the commercial data loophole under the logic of *Carpenter v. United States*. Key elements:

- **The *Carpenter* Extension:** Argue that comprehensive orbital thermal tracking is qualitatively equivalent to the cell-site location data in *Carpenter* — it enables comprehensive, retrospective, and continuing surveillance of private activity — and therefore requires a warrant regardless of the commercial intermediary mechanism.
- **The PCLOB Route:** File a formal submission to the Privacy and Civil Liberties Oversight Board's 2026 review of Section 702 reauthorization, arguing that the commercial data fusion pipeline that feeds SHIELD AI is an illegal "backdoor" collection of U.S. persons' data without Section 702 authorization.

Chapter 20 — UN and International Advocacy

UN Special Rapporteur on Privacy

The **UN Special Rapporteur on the Right to Privacy**, whose 2026 report (A/HRC/61/48) has already addressed orbital surveillance, is the most appropriate international advocacy target. A formal written submission to the Special Rapporteur's office, documenting:

- The technical capabilities of the PWSA Custody Layer and HotSat-2 MWIR thermal sensors;
- The lack of consent, notice, or remedy for persons subjected to orbital custody;
- The commercial data loophole that circumvents existing legal protections;
- The specific impact on Canadian and New Brunswick residents under Five Eyes data sharing arrangements;

...would establish this issue as a formal item on the UN human rights agenda and could result in a country-specific recommendation to Canada and the United States.

UN General Assembly Resolution

The UN General Assembly has previously passed resolutions on the right to privacy in the digital age (Resolution 68/167, 2013; and subsequent annual renewals). A draft resolution specifically addressing **orbital surveillance and the right to physical privacy** — establishing that orbital sensors cannot be used to conduct mass surveillance of civilian populations without consent — would provide an international normative framework for decommissioning demands.

UNIDIR Engagement

The **UN Institute for Disarmament Research (UNIDIR)**, which has published extensively on orbital governance and the prevention of an arms race in outer space, is a natural partner for a technical and policy paper specifically addressing the Custody Layer's incompatibility with the peaceful use obligations of the Outer Space Treaty. UNIDIR's credibility with state delegations at the Conference on Disarmament could facilitate treaty-level responses to orbital civilian surveillance.

Chapter 21 — OSINT Counter-Measures and Tactical Responses

This chapter addresses the question of what individuals and organizations can do, within the law, to reduce their exposure to PWSA-derived surveillance while the legal and political campaigns described in the preceding chapters proceed.

IMPORTANT LEGAL AND ETHICAL NOTE:

All counter-measures described in this chapter are legal. They involve no interference with satellite operations, no jamming of government systems, and no classified information. They are the civilian equivalent of closing your curtains — a lawful act of privacy preservation.

Thermal Signature Reduction

- **Thermal Insulation Enhancement:** Improving building insulation (which reduces heat loss and therefore reduces the MWIR thermal signature detectable from orbit) is both environmentally responsible and a form of passive thermal counter-measure. High-R-value roof insulation and exterior thermal barriers reduce the thermal signature that orbital MWIR sensors detect.
- **Thermal Mass Construction:** Buildings with high thermal mass (concrete, stone, earth) attenuate heat signatures more effectively than light-frame construction. This is a long-term architectural consideration.
- **Green Roof Systems:** Planted roof systems provide additional thermal insulation and scatter heat signatures across a wider area, reducing the discrete signature of individual occupants.

Satellite Pass Awareness

PWSA satellites, like all LEO satellites, follow predictable orbital paths that can be tracked using publicly available tools (Heavens-Above.com, N2YO, Celestrak). Knowing when PWSA and HotSat constellation satellites are overhead allows individuals and organizations to be aware of elevated surveillance windows.

- **TLE Tracking:** Two-Line Element (TLE) orbital data for all catalogued satellites is published by the US Space Force at space-track.org. PWSA satellites can be identified by their SDA launch manifests and tracked using standard satellite tracking software.
- **Pass Prediction Apps:** Apps like Heavens-Above, Stellarium, and ISS Detector provide real-time pass predictions for specific locations. Professional OSINT analysts should develop awareness of which satellites are overhead during sensitive operations.

RF Emissions Reduction

RF geolocation (cell phone, WiFi, radio emissions) is a key method for correlating physical thermal signatures with digital identities. Reducing RF emissions during sensitive activities reduces this correlation vector.

- Use of airplane mode / Faraday cage for devices during sensitive meetings.
- Preference for wired over wireless communications where possible.
- Awareness that even a powered-off cell phone may retain some RF emission; physical removal of the battery is the only reliable solution for devices where this is possible.

Chapter 22 — Legislative Pathways

Canada: Privacy Act Reform Advocacy

The **April 2026 Privacy Act review** is an opportunity as well as a threat. While the current review is oriented toward expanding data sharing, the public consultation process provides a formal channel for civil society to demand:

- **An explicit prohibition on receiving or using orbital thermal imaging data without a judicial warrant**, regardless of whether the data is collected directly or received from a commercial or allied partner.
- **Extraterritorial application**: The Privacy Act should explicitly apply to data collected by any means — including orbital sensors — about individuals physically located in Canada, regardless of where the sensor is located.
- **A "Five Eyes Transparency Report" requirement**: Mandate that CSIS and CSE publish annual reports on the volume and categories of satellite data received from Five Eyes partners about Canadian residents.

New Brunswick: RTIPPA Amendment Proposal

A specific amendment to the **Right to Information and Protection of Privacy Act (RTIPPA)** is proposed:

"Proposed RTIPPA Amendment: "No public body shall collect, use, or disclose personal information derived from remote sensing of any kind — including but not limited to optical, infrared, radar, or radio frequency sensing conducted from an aerial or orbital platform — without the express consent of the individual to whom it relates, or without a warrant issued by a court of competent jurisdiction upon a finding of probable cause.""

United States: The Audit the Pentagon Act

The **Audit the Pentagon Act of 2026**, which targets the commercial data loophole, should be actively supported by civil liberties organizations. Specific advocacy priorities:

- Expand the Act's scope to include **orbital thermal imaging** data specifically — not just traditional signals intelligence.
- Include a **notification requirement**: individuals who have been the subject of SHIELD AI anomaly flags should be notified and given an opportunity to contest the flag.
- Create an **independent technical review board** with security clearances to audit SHIELD AI's anomaly detection parameters and false positive rate.

CONCLUSION

The **Proliferated Warfighter Space Architecture** is real, it is operational, and its most threatening components — the Custody Layer, the thermal intelligence capability, the SHIELD AI — are active now, not in 2028. The satellites are in orbit. The AI is running. The data is flowing. And the legal architecture that should prevent its abuse is being quietly amended to accommodate rather than restrain it.

This dossier has argued — on the basis of publicly available evidence, cited to verifiable open sources — that the PWSA Custody Layer constitutes a systematic violation of the right to privacy as guaranteed by the Universal Declaration of Human Rights, the Canadian Privacy Act, the New Brunswick RTIPPA, and the spirit if not the letter of the U.S. Constitution's Fourth Amendment.

It has documented the financial and industrial interests that drive the architecture's expansion, the narrative mechanisms that have been deployed to insulate it from democratic scrutiny, and the institutional lineage — from PNAC's 2000 blueprint through Michael Griffin's SDA to the Golden Dome's interim operational capability — that connects today's orbital cage to a generation of deliberate strategic planning.

Most fundamentally, it has argued that the PWSA represents something qualitatively new in the history of human civilization: the first architecture capable of providing continuous, persistent, all-weather, through-wall custody of every human being on Earth, processed by an AI that requires no warrant, no human review, and no probable cause to initiate tracking. That this capability has been built, that it is being deployed monthly, and that the legal frameworks that should constrain it are being amended to enable rather than restrict it, is a crisis for human freedom that demands an urgent and sustained response.

"The cage is being built bar by bar, launch by launch, algorithm by algorithm. The only question is whether we notice before the door clicks shut."

Submitted by: Marie-Soleil Seshat Landry, Spymaster

Organization: Landry Industries Inc. / Marie Landry's Spy Shop

Date: April 19, 2026

Location: Moncton, New Brunswick, Canada

ORCID: 0009-0008-5027-3337

For Zenodo Archival: This document is submitted for archival under the Landry Industries Zenodo repository.

MASTER REFERENCE LIST

All references are to publicly available sources. URLs are provided as context; for archival access, Zenodo DOIs or institutional repository accession numbers should be obtained where available. All references verified as of April 19, 2026.

- [1] Akin Gump LLP. (2026). *Space Law, Regulation and Policy Update*. AkinGump.com.
- [2] Aerospace America. (2025). *Golden Dome's risks and the math of defense*. AerospaceAmerica.org.
- [3] Canadian Pugwash Group. (March 3, 2026). *Opposition to Golden Dome Space-Based Interceptors*. CanadianPugwash.org.
- [4] Carpenter v. United States. (2018). 585 U.S. 296 — *Fourth Amendment and comprehensive location tracking*. Supreme Court of the United States.
- [5] DefenseScoop. (March 17, 2026). *Golden Dome budget plan gets \$10B plus-up*. DefenseScoop.com.
- [6] Federal News Network. (March 19, 2026). *Pentagon Seeks \$200B Supplemental for Iran Conflict and GDA*. FederalNewsNetwork.com.
- [7] GAO. (2026). *GAO-26-107085: SDA Risks and Capability Delivery*. GAO.gov.
- [8] GNB.ca. (2026). *Right to Information and Protection of Privacy Act — Ten Privacy Principles*. GNB.ca.
- [9] GovDash. (January 2026). *Golden Dome Missile Defense: Complete Guide to Executive Order 14186*. GovDash.io.
- [10] Government of Canada. (2026). *Canada's Defence Industrial Strategy: BOREALIS Overview*. Canada.ca.
- [11] Gowling WLG. (April 2, 2026). *Canada Launches Review of the Privacy Act*. GowlingWLG.com.
- [12] Heritage Foundation. (2026). *Index of U.S. Military Strength: Space Force Assessment*. Heritage.org.
- [13] House Armed Services Committee. (April 15, 2026). *Statement of Marc J. Berkowitz on Golden Dome*. HASC records.
- [14] IAPP. (April 17, 2026). *Notes from IAPP Canada: Privacy Act Reform*. IAPP.org.
- [15] Justice Canada. (2026). *Modernizing Canada's Privacy Act — Policy Approaches*. Justice.gc.ca.
- [16] Kyllo v. United States. (2001). 533 U.S. 27 — *Fourth Amendment and thermal imaging of home*. Supreme Court of the United States.
- [17] L3Harris Technologies. (2025). *Tranche 3 Tracking Layer Contract Award*. L3Harris.com.
- [18] Lockheed Martin. (2026). *Speed and Precision in Space — PWSA systems overview*. LockheedMartin.com.
- [19] Lowy Institute. (March 2, 2026). *The Commercialisation of Space Surveillance*. LowyInstitute.org.
- [20] Majority Whip. (2025). *The One Big Beautiful Bill Act: Legislative Summary*. MajorityWhip.gov.
- [21] Mizzou Engineering. (March 8, 2026). *AI Algorithms for SHIELD and GDA Data Fusion*. Engineering.Missouri.edu.
- [22] Natural Resources Canada. (2025). *Airborne and Spaceborne Radar Systems — SAR and IR overview*. NRCan.gc.ca.
- [23] National Defense Magazine. (2026). *General Guetlein on GDA Cost and Timeline*. NationalDefenseMagazine.org.
- [24] Northrop Grumman. (2026). *March 2026 Contract Awards — PWSA Transport Layer*. War.gov/News.
- [25] OHCHR. (2026). *Report of the Special Rapporteur on the Right to Privacy (A/HRC/61/48)*. OHCHR.org.
- [26] Opinio Juris. (March 16, 2026). *Silent Signals: Electronic Warfare and the Legal Grey Zone of the Outer Space Treaty*. OpinioJuris.org.
- [27] Osler, Hoskin & Harcourt LLP. (2025). *Canada's 2026 Privacy Priorities: Data Sovereignty*. Osler.com.
- [28] PCLOB. (2026). *Unclassified Report on Section 702 and Commercial Data Fusion*. PCLOB.gov.
- [29] PM.gc.ca. (2026). *BOREALIS: Bureau of Research, Engineering and Advanced Leadership in Innovation and Science*. PM.gc.ca.
- [30] Polytechnique Insights. (2025). *Militarisation: The New Frontiers of Space Law*. Polytechnique-Insights.com.
- [31] Potomac Officers Club. (2025). *The One Big Beautiful Bill Act and GDA Mandatory Funding*. PotomacOfficersClub.com.

- [32] Rocket Lab USA. (2024). *Tranche 2 Tracking Layer Selection*. RocketLabUSA.com.
- [33] Rome Statute of the ICC. (2002). *Article 7 — Crimes Against Humanity*. UN.org/law/icc.
- [34] SAM.gov. (2026). *SDA PWSA — Systems, Technologies, and Emerging Capabilities (STEC)*. SAM.gov.
- [35] SatNews. (2026). *Where the Money Is in Space — PWSA Contract Analysis*. SatNews.com.
- [36] SDA.mil. (2026). *Custody Layer and Tranche 2 Tracking Mission Specifications*. SDA.mil.
- [37] SDA.mil. (2026). *News Release: HALO Europa and Tranche 2 Alpha/Beta Awards*. SDA.mil.
- [38] Secure World Foundation. (2026). *Global Counterspace Capabilities Report*. SecureWorldFoundation.org.
- [39] Senate Appropriations Committee. (2026). *FY2026 Defense Appropriations — UAP and GDA testimony*. Senate.gov.
- [40] ShadowDragon. (2024). *OSINT vs. Surveillance: The Democratization of Intelligence*. ShadowDragon.io.
- [41] Shield AI. (February 19, 2026). *Shield AI demonstrates Hivemind autonomy in fleet experimentation*. ShieldAI.com.
- [42] Space Force / Gen. Guetlein. (March 2026). *Senate Armed Services Committee Testimony on GDA Fielding*. SpaceForce.mil.
- [43] Space Systems Command (SSC). (January 9, 2026). *Task Orders Awarded for Tranche 2 Alpha and Beta*. SSC.SpaceForce.mil.
- [44] Space4Peace. (2026). *Orbital Surveillance and the Death of the Castle Doctrine*. Space4Peace.org.
- [45] Startup Reporter. (February 21, 2026). *NATO Innovation Fund Backs SatVu: Thermal Intelligence Inside Buildings*. StartupReporter.com.
- [46] SSTL / SatVu. (March 30, 2026). *HOTSAT-2 Launch Success: 3.5m MWIR Resolution Metrics*. SSTL.co.uk.
- [47] Taxpayers for Common Sense. (April 7, 2026). *Golden Dome Budget Request: The \$4.4 Trillion Reality*. Taxpayer.net.
- [48] Telfer Business Journal. (January 30, 2026). *How Defence Spending Reshapes the Canadian Economy*. Telfer.uOttawa.ca.
- [49] Transcend International. (2019). *Summary of PNAC: Rebuilding America's Defenses (2000)*. Transcend.org.
- [50] Treasury Board of Canada. (April 2, 2026). *Review of the Privacy Act: Policy Approaches for Data Sharing*. Canada.ca.
- [51] UN General Assembly. (2014). *Resolution 68/167: The Right to Privacy in the Digital Age*. UN.org.
- [52] UNIDIR. (2026). *Preventing Orbital Crises with Ethical AI / Impact of Orbital Governance*. UNIDIR.org.
- [53] Universal Declaration of Human Rights. (1948). *Article 12 — Right to Privacy*. UN.org.
- [54] US Department of War. (2026). *Biography: Michael D. Griffin, Former Under Secretary of Defense for R&E*. War.gov.
- [55] Washington Examiner. (April 15, 2026). *Golden Dome operational capability by summer 2028*. WashingtonExaminer.com.
- [56] Western University. (2025). *Analyzing Article II of the Outer Space Treaty*. UWO.ca.
- [57] Wikipedia. (2026). *Space Development Agency — Tranche 2 and Michael Griffin history*. Wikipedia.org.
- [58] Wikipedia. (2026). *Golden Dome (missile defense system) — Overview and funding*. Wikipedia.org.

END OF DOSSIER — UNCLASSIFIED // OSINT // FOR PUBLIC DISSEMINATION
Landry Industries Inc. | Marie-Soleil Seshat Landry | April 19, 2026
ORCID: 0009-0008-5027-3337 | marielandryshop.com | Moncton, NB, Canada