GENERAL FISCAL AUDIT: GOOGLE LLC, ALPHABET INC., GEMINI AI

Period: September 1, 2025 – February 28, 2026

I. PRIVACY VIOLATIONS AND USER SURVEILLANCE

I.1. Secret Activation of Gemini AI in Communication Services

I.1.1. Factual Circumstances of the Violation

October 10, 2025: Corporation **Google LLC** carried out mass forced activation of artificial intelligence features **Gemini AI** in three key communication services: **Gmail**, **Google Chat**, and **Google Meet**. This action affected all users of Google accounts in the United States, representing the largest unilateral change to personal data processing terms in the company's history without obtaining informed consent.

The nature of the violation is defined as a **forced transition from an "opt-in" model to an "opt-out" model**: whereas previously users independently activated AI features, after October 10, 2025, communication analysis was enabled by default, while opting out required navigating a complex multi-level procedure. The complaint states that Google **"secretly activated Gemini for all user accounts in Gmail, Chat, and Meet, allowing AI to track private user communications on these platforms without their knowledge and consent."**

The concealment mechanism involved three key elements. **First**, there was no explicit notification to users about the changes—mass activation was carried out silently at the server infrastructure level. **Second**, the opt-out procedure required navigation through four or more levels of privacy settings menus, making it practically inaccessible to the average user. **Third**, the settings interface retained the misleading phrasing **"When you turn this setting on, you agree..."**, despite the fact that the setting had already been factually activated by the company.

The scale of processed data encompasses **the entire history of user communications**: the Gemini AI system gained access to "literally every email and attachment sent and received in their Gmail accounts." Categories of confidential information include financial data and banking records, employment information, medical data, political and religious beliefs, information about family and social contacts, eating habits, purchases, and physical activity. Processing was carried out through servers located in **California**, establishing an unambiguous jurisdictional nexus to state legislation.

Violation Parameter	Characteristic
Activation Date	October 10, 2025
Affected Services	Gmail, Google Chat, Google Meet
Geographic Scope	All Google account users in the USA

Activation Model	Forced (opt-out instead of opt-in)
Data Categories	Financial, medical, political, religious, social
Infrastructure Base	Google servers in California

I.1.2. Legal Qualification: California Invasion of Privacy Act (CIPA)

The violation is qualified under **California Penal Code § 632**—the central provision of the **California Invasion of Privacy Act (CIPA)**, codified in sections 630–637.7 of the California Penal Code. The law, adopted in 1967, establishes one of the strictest regimes in the United States for protecting confidential communications, based on the principle of **"two-party consent."**

Content of the prohibition is formulated in § 632(a): it is prohibited to "intentionally use an electronic amplifying or recording device to eavesdrop upon or record a confidential communication without the consent of all parties to the communication, whether the communication is carried on among the parties in the presence of one another or by means of telegraph, telephone, or other device." Key elements of the crime are present in Google's actions: (1) intentional use of an electronic device—Gemini AI qualifies as a comprehensive recording and analysis system; (2) confidential nature of communications—electronic correspondence and video conferences; (3) absence of consent from all parties—users did not give informed consent to AI analysis.

Type of liability is defined as a **"wobbler"**—an offense that can be qualified as either a **misdemeanor** or a **felony** depending on circumstances and prosecutorial discretion. The sanction structure includes:

Type of Liability	Sanctions
Criminal (misdemeanor)	Fine up to **$2,500** per violation; imprisonment up to **1 year** in county jail
Criminal (felony)	Imprisonment **16 months – 3 years** in state prison
Upon Recidivism	Fine up to **$10,000** per violation

Civil liability under § 637.2 provides for **statutory damages of $5,000 per violation** or **treble actual damages** (whichever is greater), as well as reimbursement of court costs and attorney fees. Critically important is the scale of the violation: with coverage of tens of millions of users and billions of communications, cumulative liability could reach **hundreds of billions of dollars**.

Of particular legal significance is the provision of § 632(d) on **inadmissibility of evidence** obtained as a result of illegal eavesdropping or recording, in any judicial, administrative, legislative, or other proceedings—except for the prosecution of the violation itself. This creates a paradoxical situation: data collected by Gemini AI cannot be used in legal proceedings, but the very fact of collection is subject to criminal prosecution.

I.1.3. Litigation: The Case of *Thele v. Google LLC*

The class action **Thele v. Google LLC** was filed in **November 2025** in the **U.S. District Court for the Northern District of California** under case number **5:25-cv-09704**. Plaintiff **Thomas Thele**, a resident of Cook County, Illinois, acted individually and **on behalf of the class** of all similarly situated persons.

Definition of the putative class is formulated as: "all natural persons residing in the United States who have Google accounts, whose private communications in Gmail, Chat, and/or Meet were tracked by Google's Gemini AI after Google enabled 'Smart features' in these persons' privacy data settings." By conservative estimates, this concerns **130 million American Gmail users**, making this one of the largest privacy class actions in history.

Claims include: (A) certification of the right to maintain the action as a class action; (B) entry of judgment against Google on the stated grounds; (C) declaratory relief; (D) injunctive relief in the form of a prohibition on continuing the practice of access without consent; (E) injunctive relief in the form of a prohibition on tracking and using private communications; (F) award of compensatory, special, and general damages; (G) award of punitive and exemplary damages; (H) award of interest; (I) reasonable attorneys' fees; (J) any other relief.

Current status of the case: In **January 2026**, Google filed a **motion to dismiss**, arguing that: (a) users gave consent through the Terms of Service; (b) AI analysis does not constitute "recording" within the meaning of CIPA; (c) the complaint fails to satisfy Rule 23 requirements for class actions. These arguments contradict the literal interpretation of § 632 and established California case law, according to which consent must be **specific**, not general, and the use of electronic communication processing systems falls under the law regardless of the technical form of recording.

I.1.4. Systematic Nature of Violations

The analyzed violation fits into a **persistent corporate model** prioritizing AI product scaling over compliance with privacy requirements. **Preceding incidents in 2025** include unauthorized collection of user data through third-party applications even after disabling the **"Web & App Activity"** setting. In **September 2025**, a federal jury in San Francisco ordered the payment of **$425.7 million** in compensatory damages for this practice, covering the period from July 2016 to September 2024 and affecting approximately **98 million smartphones**. The jury found that Google committed **"highly offensive"** invasion of privacy and violated the right to seclusion.

Recurrent theme of corporate behavior—presenting **anti-privacy practices as privacy improvements**:

Initiative	Declared Goal	Actual Result

Privacy Sandbox	Replacement of third-party cookies	Google's own tracking system
FLoC (Federated Learning of Cohorts)	"Private" user clustering	Experiments without explicit consent, canceled after protests
Gemini AI in Communications	"Smart" organization of correspondence	Mass AI analysis without consent

Internal Google documentation, available through **SEC filings**, contains acknowledgment of regulatory risks: "We face risks related to our data collection, use, and protection practices, including risks of non-compliance with applicable data protection and privacy laws." However, these disclosures are general in nature and do not reflect specific mechanisms of violations, allowing the company to formally comply with requirements while factually concealing the scale of the problem.

II. MILITARY USE OF AI TECHNOLOGIES AND CRIMES AGAINST HUMANITY

II.1. Contractual Relations with the Israeli Military-Industrial Complex

II.1.1. Project Nimbus: Infrastructure for Military Operations

Project Nimbus represents a multi-billion dollar contract for providing cloud services to Israeli government institutions, concluded in **2021** by a consortium of **Google and Amazon** with a total value of **$1.2 billion**. The contract provided for the creation of **localized cloud infrastructure** on the territory of Israel for all branches and divisions of the Israeli government, including the **Ministry of Defense and the IDF** (Israel Defense Forces).

The agreement structure included **non-standard "control mechanisms"** built in by Israel to preempt legal challenges. According to leaked documents from the Israeli Ministry of Finance: **(1)** Google and Amazon were obligated to **not restrict Israel's use** of their products, even if such use violates the companies' terms of service; **(2)** the companies were required to **secretly notify Israel** if a foreign court ordered them to transfer Israeli data, effectively allowing circumvention of legal obligations. These conditions create an unprecedented situation in which corporations formally retain control while actually losing the ability to influence the use of their infrastructure.

The initial **public position of Google** claimed that Project Nimbus was **"not intended for sensitive or classified military workloads relevant to weapons or intelligence services."** This statement, as subsequently became clear, was **knowingly false** and served as a mechanism for concealing the actual nature of the technology's use.

Contract Parameter	Characteristic
Date of Conclusion	2021
Contract Value	$1.2 billion (jointly with Amazon)

Contracting Party	Israeli Ministry of Defense, all branches of government
Services Provided	Google Cloud Platform, computing power, data storage, machine learning tools
Financing	Budget allocations of the Israeli Ministry of Defense
Special Conditions	Prohibition on restricting use; secret notification of court decisions

II.1.2. Expansion of Cooperation After October 7, 2023, and During the Audit Period

The period of **September 2025 – February 2026** is characterized by **unprecedented intensification** of Google's cooperation with the Israeli military-industrial complex. Internal company documents obtained by **The Washington Post** confirm **direct servicing of the Israeli Ministry of Defense and the IDF** during military operations in Gaza.

New elements of cooperation during the period under review:

Component	Description	Deployment Period
Vertex AI	Machine learning platform for military applications	2024–2025
Gemini AI	Generative model for developing military assistants	November 2024 – February 2026
Specialized Team	Israeli citizens with security clearances for state secrets	2024–2026

Internal correspondence of Google employees demonstrates the **commercial motivation** of military cooperation. One employee warned colleagues that if Google did not satisfy the Ministry of Defense's request for expanded access to AI technologies, **"the occupation forces may turn to Amazon"**—the main competitor in cloud computing. This message shows that commercial considerations dominated over ethical and legal constraints in decision-making.

Key dates in internal documentation:

- **October 2023**: Escalation of requests for expanded access to AI technologies after the October 7 attacks
- **Spring–Summer 2024**: Continuation of requests for AI technologies for the IDF
- **November 2024**: Request for access to **Gemini AI** for developing an AI assistant for document and audio processing
- **February 2026**: Whistleblower complaint to SEC with internal correspondence about technical support for analysis of military aerial photography

The **February 2026** SEC complaint, filed by a former Google employee, contains **direct evidence** of military use of Gemini AI. In **July 2024**, Google Cloud support received a request from an email address belonging to the **IDF**, on behalf of an employee of the Israeli technology company **CloudEx** (contractor to the Israeli defense forces). The client reported an error when attempting to use **Gemini AI

for analysis of aerial photographs**, as a result of which the software periodically **failed to identify drones, soldiers, and other objects**. Google employees responded with troubleshooting suggestions, conducted **internal tests**, and provided a technical solution to the problem.

This incident has **exceptional legal significance**: it demonstrates **direct technical assistance** by Google in optimizing AI systems for **military targeting and battlefield object recognition**, refuting any claims about the "non-military" nature of the cooperation.

II.2. Application of AI Technologies in War Crimes

II.2.1. Targeting Systems and Automation of Killing

The Israeli armed forces deployed a **comprehensive ecosystem of AI systems** for automating the identification, prioritization, and liquidation of targets in Gaza, the functioning of which critically depended on Google's corporate infrastructure:

System	Function	Role of Google Technologies
Lavender	AI identification of potential "militants" by behavioral patterns	Cloud infrastructure for processing massive data arrays, machine learning tools
The Gospel (Habsora)	Mass generation of targeting recommendations	Computing power for algorithmic analysis of intelligence data
Where's Daddy?	Real-time tracking of marked individuals, bombing upon entry to home	Cloud storage and processing of geolocation data

The **Lavender system** is characterized by a **high error rate** and **minimal human control**. According to journalistic investigations, the system operated with an **acceptable level of "collateral damage"**: **20 civilians per target** when attacking "low-ranking militants" and **up to 100 civilians** when attacking "high-ranking militants." The only verification criterion applied by military personnel to lists of targets generated by Lavender was the **gender of the target**—which effectively turned **all Palestinian males, including children, into legitimate targets.**

Colonel **Rachelle Dembinski**, head of the IDF Computer Department, in a public presentation characterized cloud technologies as **"a platform that is a weapon"**: "You must understand that this is a platform that is a weapon." This acknowledgment by military leadership of the technological nature of the services provided **refutes any attempts by Google to present its activities as neutral or insignificant** to military operations.

II.2.2. Mass Surveillance and Administrative Violence

Beyond direct application in combat operations, Google technologies ensured a **system of mass surveillance** in the occupied Palestinian territories:

- **Google Photos**: Use of facial recognition features to build databases of Palestinians without their consent. An Israeli officer was quoted as stating that Google's ability to match faces **surpasses specially developed military technologies**.

- **Processing of intelligence data**: Google cloud infrastructure was used to store and analyze **millions of intercepted phone calls, text messages, and audio messages**. According to leaks, the use of machine learning tools increased **64-fold** compared to pre-war levels.

- **Automation of administrative control**: Google AI technologies were used for **processing movement permits, analyzing social connections, predicting "risky" behavior**—creating a new form of **structural violence** depriving Palestinians of the possibility of appeal to human judgment.

Scale of casualties: According to UN data, during the period from October 2023 to February 2026, more than **62,000 Palestinians** died as a result of Israeli military operations, the vast majority of whom were civilians, including women and children. The medical journal **The Lancet** estimates the total number of deaths (direct and indirect) at **186,000 people**. The scale of destruction—**85,000 tons of dropped bombs**, nearly six times the power of the Hiroshima atomic bombing—was made possible by the **automation of targeting processes** enabled by corporate infrastructure.

II.3. International Legal Qualification

II.3.1. Report of the UN Special Rapporteur Francesca Albanese

February 2026 was marked by the publication of the groundbreaking report of the **UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese**, entitled **"From Economy of Occupation to Economy of Genocide."** The report was presented during the **59th session of the UN Human Rights Council** and contains **direct accusations against Alphabet Inc.** and other technology corporations.

Key conclusion of the report:

> **"Tech giants Microsoft, Alphabet (Google), and Amazon are providing Israel with cloud and AI technologies, enhancing the government's ability to process data, make decisions, conduct surveillance, and analyze."**

The report identifies **48 corporate actors** in the sectors of armaments, technology, construction, tourism, energy, finance, academia, and agriculture, while emphasizing that the presented list constitutes only the **"tip of the iceberg"** of a broader network of corporate complicity. Alphabet Inc. figures as a **key supplier of cloud and AI infrastructure**, with direct reference to the **$1.2 billion** Project Nimbus contract and its financing from the budget of the Israeli Ministry of Defense.

The Rapporteur uses the terminology of **"joint criminal enterprise"**:

> **"This is a 'joint criminal enterprise,' where the actions of one ultimately contribute to an entire economy that leads, supplies, and sustains this genocide."**

This concept has **fundamental legal significance**, as "joint criminal enterprise" represents an established doctrine of international criminal law applied to hold liable persons who assisted in the commission of international crimes.

The report characterizes the modern conflict as the **"first AI-driven and livestreamed genocide,"** in which corporate technologies ensure **"data sovereignty to shield impunity."** The use of commercial AI in Gaza marks a **disturbing boundary**: systems developed for logistics optimization now **"generate kill lists, erase families, and flatten entire neighborhoods."**

II.3.2. Applicable Norms of International Law

Source of Law	Key Provisions	Application to Google's Activities
Geneva Conventions 1949	IV Convention: protection of civilian population in occupied territories; prohibition of collective punishments, forced displacement, destruction of property (Arts. 33, 49, 53)	Provision of infrastructure for systems carrying out mass violations
Rome Statute of the ICC	Art. 7: crimes against humanity (murder, extermination, torture, inhumane acts); Art. 8: war crimes (attacks on civilian population, unjustified destruction)	Complicity in widespread systematic attack against the Palestinian population
Genocide Convention 1948	Art. II: genocide as acts with intent to destroy a group; Art. III: liability for genocide, conspiracy, incitement, attempt, **complicity**	Provision of means for destruction of Palestinians as a group with awareness of criminal intent
UN Guiding Principles on Business and Human Rights	Principle 13: duty to respect human rights; Principle 17: due diligence for identifying and preventing negative impact	Violation of due diligence obligation; continuation of activity with known risks

The **International Court of Justice** in its **advisory opinion of July 19, 2024**, recognized that Israel violates **the Palestinian people's right to self-determination** and the **prohibition on acquisition of territory by force**, and also established the existence of a **system of racial segregation and apartheid.** This opinion creates a legal basis for qualifying any activity supporting the Israeli occupation as **complicity in international crimes.**

II.3.3. Elements of Crimes Against Humanity

Legal analysis of Alphabet Inc.'s activities reveals the presence of **all objective elements of crimes against humanity**:

Element	Factual Circumstances	Legal Assessment

Widespread or systematic attack	Massive application of AI targeting systems in Gaza; thousands of potential targets identified algorithmically; coverage of entire sector population	Corresponds to the criterion of "systematicity"—organized activity of state structures using corporate infrastructure
Directed against civilian population	Palestinians in occupied territories as target group of AI systems; predictable mass casualties among non-combatants	Corresponds to the criterion of "civilian population"—persons not taking direct part in hostilities
Murder, extermination, inhumane acts	Liquidations based on AI-generated targeting; destruction of life support infrastructure; 62,000+ dead, 186,000 including indirect deaths	Corresponds to Arts. 7(1)(a), (b), (k) of the Rome Statute
Knowledge of the attack's nature	Public availability of information about mass casualties; internal risk assessments; direct technical support of military operations	Corresponds to the criterion of "awareness"—actual and constructive knowledge of the context of use
Intentional assistance	Provision of critical infrastructure with awareness of criminal use; refusal to terminate cooperation; creation of specialized team with clearances	Corresponds to criteria of **complicity** under general law and specific ICC norms

The construction of **"common plan or policy"** (Art. 7(2)(a) of the Rome Statute), necessary for qualification as crimes against humanity, is confirmed by the **systematic nature of Israeli military doctrine** integrating AI technologies into operational planning. Google, by ensuring the technological foundation of this doctrine, becomes part of the "common plan" in a **material, if not intentional, sense.**

II.4. Liability of Alphabet Inc. Management

II.4.1. Change of Corporate Policy in February 2025

February 2025 marked a **principled change** in Alphabet Inc.'s corporate policy. The company **formally abandoned its commitment not to use artificial intelligence for military purposes**, replacing it with flexible "responsible AI principles" permitting military application subject to procedural guarantees.

Justification for the change—the need to "help democratically elected governments evolve and keep pace with global AI use"—masks the actual intention: **ensuring unlimited access of the defense sector to AI technologies** without risk of reputational or legal consequences. The policy change coincided with the **intensification of military operations in Gaza** and the expansion of contractual relations with the Israeli Ministry of Defense, indicating a **direct connection between corporate decisions and specific military applications.**

Financial indicators reflect the consequences of this policy. The **Google Cloud** segment demonstrated revenue growth of **48% to $17.7 billion** in Q4 2025, with **"demand for AI products"** named as the key growth driver. The investment program for **2026** provides for capital expenditures in the range of **$175–185 billion**, directed primarily at expanding AI infrastructure.

II.4.2. Personal Liability of Key Figures

Official	Position	Sphere of Responsibility
Sundar Pichai	CEO of Alphabet Inc. and Google LLC	Strategic approval of military AI use; sanctioning of contracts; change of corporate policy in February 2025
Thomas Kurian	CEO of Google Cloud	Operational management of contracts with the Israeli Ministry of Defense; coordination of technical support for military operations
Google Cloud Leadership (Government Sector)	Vice Presidents and Directors for Government Clients	Direct execution of contracts; adaptation of products to military requirements; interaction with Israeli military structures

Principles of international criminal law permit **holding liable persons occupying leadership positions** for crimes committed by subordinates in the presence of **actual control** and **knowledge of the nature of the activity.** The doctrine of **command responsibility**, developed in the context of war crimes, applies to corporate leaders exercising effective control over activity leading to international crimes.

III. DATA MANIPULATION AND CONCEALMENT OF INFORMATION

III.1. Disinformation of Regulators and the Public

III.1.1. False Statements About the Nature of Contracts

Systematic disinformation regarding Project Nimbus constitutes a **separate offense** related to misleading regulators, investors, and the public. Google's public position, **repeatedly stated** in responses to media inquiries and in communications with employees, was that the contract was **"not intended for highly sensitive, classified, or military workloads relating to weapons or intelligence services."**

This assertion is **refuted** by the following facts:

Fact	Source
Direct requests from the Israeli Ministry of Defense for access to AI technologies for military applications	Internal Google correspondence
Public acknowledgment by Israeli officials of military use of cloud technologies	Statement by Colonel R. Dembinski
Creation of a classified team for work with secret military information	Journalistic investigations
Whistleblower complaint to SEC about technical support for analysis of military aerial photography	SEC complaint, February 2026

February 2026: After publication of new journalistic investigations, a Google representative continued to assert that **"any claim that we violated our AI principles is mistaken"** and that the company

"received a support ticket for a product available to any customer." This position **ignores the specificity of military application** and the factual assistance in the commission of international crimes.

III.1.2. Concealment of the Scale of Surveillance

Alphabet Inc.'s SEC filings for 2025 contain **insufficient disclosure** of information about military use of AI technologies and associated risks. Reports to shareholders do not include:

- specific mentions of contracts with the Israeli Ministry of Defense;
- scale of technical support for military operations;
- potential legal consequences of military cooperation;
- ethical and reputational risks materialized in mass employee protests.

The **risk factors** section in **Form 10-K** contains generalized formulations: "We face risks related to our data collection, use, and protection practices, including risks of non-compliance with applicable data protection and privacy laws." However, **the specificity of military contracts and the risks of international legal liability** are not disclosed, allowing investors to underestimate the materiality of exposure.

This practice **potentially violates** disclosure obligations regarding material information under **federal securities laws** (Securities Act of 1933, Securities Exchange Act of 1934).

III.2. Internal Mechanisms of Information Suppression

III.2.1. Reaction to Data Leaks

The history of Google's relations with critically-minded employees includes **multiple cases of dismissals** for disclosing information about military contracts. The most resonant was the incident of **2018**, related to **Project Maven** (military AI application for analyzing video from drones), which led to mass employee protests and subsequent refusal to renew the contract.

By **2025–2026**, corporate policy **evolved**: instead of public retreats, the company moved to **preventive suppression of dissent** through:

- **expansion of the definition of "confidential commercial information"** to include information about contracts with government structures;
- **use of NDAs with broad formulations**;
- **threats of lawsuits** for breach of contractual obligations and theft of intellectual property.

These practices create a **"chilling effect,"** preventing legitimate informing of the public about corporate behavior.

III.2.2. Corporate Culture of Secrecy

Classification of documents about military cooperation is built on a **"need-to-know"** model, restricting access to information within the company. Elements of the secrecy architecture:

Element	Function
Project code names	Masking the true nature of the activity
Isolated technical teams	Preventing leaks through "weak links"
Separate legal entities	Formal separation of liability
Classified team with Israeli citizens	Work with information unavailable to the main company

Paradoxically, the company whose business model is built on the **"democratization of access to information"** applies **principles of state secrecy** to its own activities.

IV. FRAUD AND UNFAIR COMPETITION

IV.1. Trademarks and Unfair Competition

IV.1.1. The Case of *Gemini Data, Inc. v. Google LLC*

The judicial case **Gemini Data, Inc. v. Google LLC**, registered in the **U.S. District Court for the Northern District of California** under number **4:2024cv06412**, illustrates corporate methods of conquering market positions.

Plaintiff—**Gemini Data, Inc.**, a company in the data management field, using the trademark **"Gemini" since 2011**. **Plaintiff's allegations**:

- Google made an **attempt to anonymously acquire trademark rights** before public product launch;
- after **USPTO refusal of registration** of Google's application on grounds of likelihood of confusion with previously registered Gemini Data marks, the company carried out **malicious expropriation of the brand** under the cover of a "common dictionary term";
- the Google AI chatbot itself, when asked directly, **acknowledged trademark infringement**, characterizing the situation as "developing."

Current status: **January 27, 2026**, Judge **Jeffrey S. White** issued an order **permitting Gemini Data to file an amended complaint** no later than February 3, 2026, with Google's response due no later than February 17, 2026. The procedural outcome indicates **recognition of the sufficiency of the allegations** at the preliminary stage.

The case acquires **symptomatic significance**: the methods attributed to Google in the field of intellectual property—anonymous acquisition attempts, ignoring prior users' rights, exploitation of resource superiority in litigation—**mirror the general pattern of corporate behavior** regarding data privacy and military cooperation.

IV.2. Anticompetitive Practices in the AI Field

IV.2.1. Forced Integration of Services

The activation of Gemini AI in Google communication services without user consent constitutes a form of **tying**, where a dominant position in the market for one product (Gmail, Google Search) is used to promote another product (Gemini AI). This practice **creates barriers for competitors** in the generative AI market:

Mechanism	Description	Anticompetitive Effect
Exclusive access to data	Gmail users cannot use alternative AI assistants to process their correspondence	Monopolization of sources for training AI models
Integration into dominant products	Gemini is embedded in the Gmail/Chat/Meet interface without possibility of replacement	Exclusion of competitors from user experience
Network effects	Growth of Gemini user base improves model quality through feedback	Self-reinforcing dominance

These practices **potentially violate** provisions of the **Sherman Act** (prohibition on monopolization and conspiracies) and **Clayton Act** (prohibition on tying and exclusive deals), although antitrust regulation in the digital platform sphere remains **insufficiently developed** for effective counteraction.

V. SYSTEMATIC VIOLATIONS AND CORPORATE MODEL

V.1. Pattern of Behavior: Growth Priority Over Human Rights

V.1.1. Historical Continuity of Violations

The analyzed violations fit into a **persistent corporate model** in which **commercial interests are systematically prioritized** over protection of user rights and international legal obligations:

Project	Period	Declared Goal	Actual Result	Legal Consequences
Privacy Sandbox	2019–2024	Replacement of third-party cookies for "privacy protection"	Google's own tracking system maintaining dominance in advertising	Ongoing regulatory investigations
FLoC	2021	"Private" user clustering	Experiments without explicit consent, canceled after protests	Reputational damage, project cancellation
Chrome Incognito	2008–2023	"Private" browsing	Continuous collection of data on user activity	Multi-million dollar settlements
Gemini in Communications	2025–2026	"Smart" organization of correspondence	Mass AI analysis without consent	Class action *Thele v. Google*, potential liability in hundreds of billions

Recurrent theme: presenting **anti-privacy practices as privacy improvements.** Each initiative is accompanied by **rhetoric of protecting user interests**, while factually **expanding data collection and processing capabilities.** This dissonance between words and actions **is not accidental**, but represents a **conscious strategy for neutralizing regulatory and public resistance.**

V.1.2. Financial Motivation Against Legal Constraints

Revenue from advertising based on personal data remains the foundation of Google's business model, generating **tens of billions of dollars annually.** AI services function as a **new source of data for profiling**, expanding targeted advertising capabilities under the guise of "personalizing user experience."

Segment	2025 Revenue	Growth	Key Driver
Google Search & other	$175+ billion	+12%	Integration of generative AI into search results
YouTube ads	$30+ billion	+14%	AI-optimization of targeting
Google Cloud	**$70+ billion run rate**	**+48%**	**"Demand for AI products," including military contracts**

The conflict between **financial motivation** and **legal constraints** is systematically resolved in favor of the former. Internal documentation contains acknowledgment of risks, but these risks **are considered exclusively from the standpoint of financial consequences**, not ethical or legal obligations to users.

V.2. Structural Irresponsibility

V.2.1. Separation of Legal Entities

The corporate structure of **Alphabet Inc.** presupposes formal separation between:
- **Alphabet Inc.**—holding company, owner of shares;
- **Google LLC**—operating company implementing core products and services;
- **subsidiaries** (Waymo, Verily, Google Cloud, etc.)—specialized directions.

However, **de facto unity** of management, integrated systems, and **absence of real autonomy** of subsidiaries make this separation a **legal fiction** used for **diffusion of responsibility.** Decisions on military cooperation, mass activation of AI functions, and changes in corporate policy are made by **unified leadership** headed by Sundar Pichai.

V.2.2. Transnational Evasion Mechanisms

Use of complex corporate structure for evasion of liability includes:

Mechanism	Description	Legal Effect

Transfer of assets between jurisdictions	Intellectual property, user data placed in jurisdictions with favorable regulatory regimes	Complicating enforcement in jurisdictions of victims
Separation of contracts between subsidiaries	Military contracts formalized through Google Cloud, not Google LLC	Formal separation of liability
Exploitation of differences in national legislation	Absence of unified international regulation of corporate liability for international crimes	"Regulatory arbitrage"—choice of most favorable jurisdiction

These practices **do not eliminate objective liability** under international law, but create **procedural barriers** to its realization.

VI. APPLICABLE LAWS AND LIABILITY MEASURES

VI.1. United States National Legislation

VI.1.1. California

Legislative Act	Key Provisions	Application to Google's Activities
CIPA (Penal Code §§ 630-637.7)	Prohibition on eavesdropping/recording without consent of all parties; civil and criminal liability	**Direct application** to secret activation of Gemini AI
CCPA (Civil Code §§ 1798.100-1798.199)	Right to know, right to deletion, right to opt out of sales	Violation of right to know about data collection through AI analysis
CPRA (Civil Code §§ 1798.140-1798.199)	Enhanced protection of "sensitive data"; creation of California Privacy Protection Agency	User communications qualify as sensitive data

VI.1.2. Federal Law

Legislative Act	Powers/Limitations	Application
Section 230 Communications Decency Act	Limited liability protection for user-generated content	**Does not apply** to platform's own illegal activity
Federal Trade Commission Act (Section 5)	FTC powers to prevent "unfair or deceptive practices"	False statements about privacy; secret data collection
Securities Act of 1933 / Securities Exchange Act of 1934	Obligation to disclose material information	Insufficient disclosure of military contracts and associated risks
Export Administration Regulations (EAR)	Control of dual-use technology exports	**Potential violations** in export of military-purpose AI technologies

VI.2. International Law

VI.2.1. Individual Criminal Liability

Mechanism	Basis of Jurisdiction	Applicability to Google Leadership
Rome Statute of the ICC	Nationality of victims (Palestinians as depository persons)	Possibility of investigation under Arts. 7, 8 (crimes against humanity, war crimes)
Universal jurisdiction	Serious international crimes (torture, genocide)	Possibility of prosecution in third states (European jurisdictions)
National war crimes legislation	Implementation of Rome Statute (e.g., Germany, France, Belgium)	Criminal cases against leaders when present on territory

VI.2.2. Corporate Liability

Source	Nature of Obligations	Mechanism of Implementation
OECD Guidelines for Multinational Enterprises	Voluntary principles acquiring binding character through national legislation	National Contact Points (NCPs), court actions
UN Guiding Principles on Business and Human Rights	"Protect, Respect, Remedy"—obligations of states and corporations	Voluntary mechanisms, national due diligence legislation
Supply chain due diligence laws (Germany, France, Norway, etc.)	Obligation to conduct due diligence in human rights	Administrative and civil law sanctions

VI.3. Proposed Liability Measures

VI.3.1. Civil Law Sanctions

Measure	Description	Expected Scale
Compensatory payments (class actions)	Compensation to users for violation of CCPA, CIPA	**$10–100+ billion** upon successful class certification in *Thele v. Google*
Injunctive relief	Court prohibition on continuation of contested practices	Mandatory "opt-in" for all AI functions; independent monitoring
Punitive damages	Sanctions for willful and malicious behavior	Trebling of base damages; exemplary damages in amount determined by jury

VI.3.2. Criminal Law Sanctions

Measure	Subjects	Basis
Investigation under articles on complicity in war crimes	Sundar Pichai, Google Cloud leadership	Rome Statute of the ICC, Art. 25 (individual criminal liability); national war crimes laws
Charges under federal fraud laws	Alphabet Inc. leadership	18 U.S.C. § 1341 (mail fraud), § 1343 (wire fraud)—false statements to investors

| **Charges under securities laws** | Chief Financial Officer, Director of Investor Relations | Securities Exchange Act of 1934, Rule 10b-5—insufficient disclosure of material information |

VI.3.3. Regulatory Measures

Measure	Description	Precedents
Forced business separation (structural remedies)	Separation of Google Cloud from main company; separation of advertising business from search	DOJ proposals for Google breakup (2024–2025)
Prohibition on certain types of activity	Moratorium on military contracts; prohibition on forced integration of AI products	Microsoft/DOJ settlement (2001); Facebook commitments after Cambridge Analytica
Appointment of independent monitoring	External observer for compliance with privacy policies and AI ethics	Implementation in settlements with technology companies

---

VII. SOURCES AND EVIDENCE

VII.1. Judicial Documents

Document	Case Number	Court	Status
Complaint **Thele v. Google LLC**	5:25-cv-09704	U.S. District Court for the Northern District of California	Motion to dismiss (January 2026)
Materials **Gemini Data, Inc. v. Google LLC**	4:2024cv06412	U.S. District Court for the Northern District of California	Permission for amended complaint (January 2026)

VII.2. Reports of International Organizations

Document	Author	Date	Key Conclusion
A/HRC/59/23 "From Economy of Occupation to Economy of Genocide"	UN Special Rapporteur Francesca Albanese	February 2026	Microsoft, Alphabet (Google), Amazon provide Israel with cloud and AI technologies, enhancing the government's ability to process data, make decisions, conduct surveillance, and analyze
Advisory Opinion of the ICJ	International Court of Justice	July 19, 2024	Israel violates the Palestinian people's right to self-determination; system of apartheid

VII.3. Journalistic Investigations

Publication	Date	Content
The Washington Post	2024–2025	Internal Google documents on direct servicing of the Israeli Ministry of Defense and IDF; requests for access to Gemini AI

| **+972 Magazine / Local Call / The Guardian** | 2024 | Leak of Israeli Ministry of Finance documents on special contract conditions for Nimbus |
| **Progressive International / AFSC Investigate** | 2024–2025 | Analysis of corporate complicity; use of Google Photos for facial recognition |

VII.4. Corporate Reporting and Regulatory Documents

Document	Period	Key Information
SEC Form 10-K Alphabet Inc.	2025	Acknowledgment of regulatory risks; Google Cloud growth of 48%; investments of $175–185 billion in AI infrastructure
SEC complaint (whistleblower)	February 2026	Direct evidence of technical support for analysis of military aerial photography
Google Press Releases	2024–2026	Public statements on "non-military" nature of Nimbus; AI policy change in February 2025

CONCLUSION

The conducted General Fiscal Audit of the activities of **Google LLC, Alphabet Inc., and the Gemini AI division** for the period **September 1, 2025 – February 28, 2026** reveals **systematic, large-scale, and serious violations** of national and international law. The companies committed:

1. **Massive violations of data protection legislation**, including forced activation of AI surveillance without consent of millions of users, with potential liability in **hundreds of billions of dollars** from class actions.

2. **Assistance in war crimes and crimes against humanity** through Project Nimbus, as confirmed by the **official report of the UN Special Rapporteur**, creating a basis for **criminal prosecution of leadership** under international and national law.

3. **Systematic disinformation** of regulators, investors, and the public regarding the nature and scale of their activities, with potential liability under **securities and fraud laws.**

The corporate model of Alphabet Inc. demonstrates a **persistent pattern of behavior** in which **growth and profit are prioritized over human rights and the rule of law.** Structural mechanisms for evading liability—separation of legal entities, transnational placement of assets, corporate secrecy—**do not eliminate objective liability**, but create barriers to its realization.

Recommended measures include: expedited consideration of class actions with application of enhanced sanctions; criminal investigation of leadership under articles on complicity in international crimes; regulatory measures up to forced business separation; initiation of universal jurisdiction procedures in friendly jurisdictions.