CIRCUITTELLIGENCE

Joint-Liability Regulatory Brief

Re: The Shared Microsoft–Google Architecture That Substitutes Privilege for Consent, Enabling Mass Non-Consensual Interception of Electronic Communications

Date: 3 June 2026

Version: v1 — Initial public submission

Purpose: Submission to antitrust authorities, data protection regulators, and investigative bodies

Canonical URL: circuittelligence.com/briefs/consent-gate-brief-v1.pdf

Prepared by: Circuittelligence // Beautiful Intelligence, Bounded.

DOCUMENT STRUCTURE

The Consent Gate Principle

Wiretapping law has never been about wires. It has always been about the expectation of privacy and the function of consent. The Wiretap Act (18 U.S.C. § 2511) does not regulate copper; it regulates interception. It mandates that before a communication may be lawfully intercepted, a specific and independent consent gate must be satisfied: either a court-issued warrant or the consent of at least one party to the communication. The physical medium — copper, fibre, or radio — is irrelevant. The junction box is simply the place where the gate is tested.

The law correctly separates two things that must never be collapsed:

Infrastructure access (capability): The physical or digital ability to reach the communication stream.

Legal authority (consent): The verified, lawful right to intercept its contents.

No person or company is permitted to treat the first as proof of the second.

> *The architectural argument in this brief applies under the Wiretap Act where interception is contemporaneous with transmission, and under the Stored Communications Act and CFAA where it is not. The consent-gate analysis holds across all applicable statutes regardless of which title governs a specific fact pattern.*

II

The Exact Same Collapse in the Windows–Chromium Architecture

Microsoft and Google have built and maintained a joint architecture that collapses infrastructure access and legal authority into a single binary gate, and then deployed it indiscriminately across every consumer device running Windows.

How the Architecture Works

1. Microsoft's registry treats any write to HKEY_LOCAL_MACHINE\Software\Policies by a process holding an administrative token as a valid expression of the device owner's policy intent. There is no separate verification step. The OS does not ask: "Is this specific change consented to by the actual physical owner of this device?" Administrative privilege is treated as absolute consent.

2. Google Chrome and Microsoft Edge ingest these policy keys unconditionally on startup. Upon reading ExtensionInstallForcelist, both browsers silently install the referenced extension; remove the user's ability to disable or delete it (the "Remove" button is stripped); and grant the extension all declared permissions — including the ability to read, intercept, and exfiltrate all web traffic, form inputs, and cookies — without any affirmative user action.

3. The consent gate is entirely absent. No out-of-band verification confirms that the policy originated from the device owner. No distinction is made between a corporate device under legitimate management and a consumer device in a living room. The architecture treats any admin-level write as an authorised interception order.

The Result

An attacker who escalates to administrator — through malware, social engineering, or a software vulnerability — gains the power to order both dominant browsers to intercept all electronic communications, silently and permanently, without the device owner ever being notified or able to revoke the interception.

> *This is not a hypothetical. Over 300,000 consumer devices were compromised through precisely this vector, across both Chrome and Edge simultaneously, in a single documented campaign identified by ReasonLabs in August 2024. Home computers. Not corporate networks.*

III

The Junction Box Analogy: Simple, Complete, and Fatal to the Defence

A telephone lineman has a key to the street-side junction box. He opens it, clips onto a household's line, and listens to all calls. The telephone company's infrastructure does not verify subscriber consent before the clips make contact. The lineman's physical access to the copper is his infrastructure privilege.

The question: Is the lineman's physical access to the junction box the legal equivalent of the subscriber's consent to be listened to?

> *The law answers: No. Infrastructure access is not consent. The Wiretap Act demands a completely separate gate — a warrant or party consent — irrespective of how the lineman got into the box.*

Substituting the Terms

Junction Box Wiretap	Windows / Chrome Policy Chain
Lineman has physical access to the junction box	Attacker has administrator access to the device
The box provides no consent gate before enabling interception	The registry provides no consent gate before browser policy is enforced
Lineman clips on and listens to all calls	Attacker writes to ExtensionInstallForcelist; browser silently intercepts all web communications
"Physical access is the security boundary. This is network maintenance."	"Administrative access is the security boundary. This is enterprise management."
The law: Infrastructure access is not consent. Liable.	**The law must say: Administrative privilege is not consent. Jointly liable.**

The Unanswerable Question

> *"If you argue that admin privilege is not the same as the junction box key — that the permission comes from somewhere else — then where does it come from?"*

There are only two possible answers, and both destroy the defence.

Answer 1: The permission comes from the admin rights. This is exactly the lineman's argument: the permission comes from having the key. The law has already rejected this conflation of access and authority. It is not a defence; it is an admission.

Answer 2: The permission is implied by the enterprise management configuration. But a consumer device in a home has no enterprise management configuration. The architecture makes no distinction between a domain-joined corporate asset and a privately owned laptop. By deploying the policy ingestion channel universally, the companies treat every living room as a corporate office the moment admin access is obtained. That is not an enterprise feature; it is the absence of any consumer consent gate.

The architecture is void of consent by design. There is no third permission source.

III-A

The Legal Distinction Between Capability and Authority

The central defence advanced by Microsoft and Google is that administrative privilege constitutes the relevant security boundary and that any actor capable of writing policy to the operating system necessarily possesses sufficient authority to direct browser behaviour. This position is inconsistent with multiple established legal doctrines that distinguish technical capability from lawful authority.

A. Trespass to Chattels: The Injury Is Measurable Before Data Theft Is Calculated

Restatement (Second) of Torts §§ 217–218 establishes that trespass to chattels attaches when the chattel is impaired as to its condition, quality, or value; the possessor is deprived of use for a substantial time; or harm is caused to a legally protected interest. Physical destruction is not required.

Sotelo v. DirectRevenue, LLC confirmed that spyware running without consent, depleting bandwidth and system memory, and requiring technical expertise to remove constitutes actionable trespass. Thomas Kerrins v. Intermix Media, Inc. confirmed the same for adware requiring remediation effort. S&S; Activewear LLC v. Promo Hunt, Inc. (2026) established that the browser application and local registry are the exclusive chattels of the end user — not the remote services they access.

The registry injection exploit satisfies all three Restatement categories independently and cumulatively:

System impairment: Browser controls stripped. Remove button removed. Permissions granted without user action. The chattel is materially degraded.

Deprivation of use: The owner is locked out of managing their own browser environment for the entire persistence period — which by design is indefinite.

Remediation cost: The hours, specialist tools, repeated attempts, and technical expertise required to remove a re-injecting persistence loop constitute quantifiable actual injury before any downstream data theft is counted.

> *Intel Corp. v. Hamidi involved emails causing distraction with zero system impairment. This involves software causing dispossession and stripping the owner's possessory relationship to the chattel. They are categorically different injuries. Hamidi is not a limit here — it is a distinction that confirms the claim.*

B. Intrusion Upon Seclusion

Restatement (Second) of Torts § 652B protects individuals from intentional, highly offensive invasions into their private affairs. The Ninth Circuit confirmed in In re Facebook, Inc. Internet Tracking Litigation that browsing habits are protected and covert cross-site tracking constitutes a plausible intrusion. The "broken banner" decisions of late 2025 go further: when a user actively selects a privacy setting and it is technically bypassed, the consent defence is eliminated entirely.

The architecture at issue does not offer a banner. It offers nothing. The owner's expectation that their browser operates under their control is not only reasonable — it is the entire premise on which consumer computing is sold.

C. Van Buren v. United States: Gates-Up-or-Down

Van Buren v. United States, 593 U.S. 374 (2021), establishes that technical access capability and legal authorization are distinct inquiries. A gate being technically open does not mean the entrant is legally authorized to proceed. The Third Circuit confirmed this in Durenleau v. Allied (August 2025). Administrative privilege establishes that a process can write policy. It does not establish that the process is authorized by the device owner to install surveillance-capable software, override user controls, or displace owner authority.

D. Lenovo/Superfish: The Direct Enforcement Precedent

Between August 2014 and early 2015, Lenovo preloaded Superfish "VisualDiscovery" adware on 43 consumer laptop models. The software used Komodia to install a self-signed root certificate into the OS trusted Certificate Authority store, intercepting and decrypting all HTTPS browser traffic — acting as a man-in-the-middle on financial and medical communications without user consent.

> *The FTC charged Lenovo with preloading intercepting software without adequate notice or consent. Result: 20-year consent decree requiring affirmative consumer consent before pre-installing ad-injecting software. $8.3 million in class action settlements. This is a completed enforcement action. The factual structure is identical to the architecture described in this brief. The platforms are different. The legal principle is the same.*

E. The Missing Consent Layer: Synthesis

These doctrines collectively recognize one principle:

- Wiretap law separates access to communications infrastructure from authority to intercept.
- Trespass doctrine separates digital access from lawful interference with possessory interest.
- Privacy law separates the ability to intrude from the right to intrude.
- Van Buren separates access credentials from authorized purpose.
- Lenovo/Superfish establishes that deploying intercepting software without consent at consumer scale is an actionable FTC violation regardless of the platform's technical authority over the device.

The Microsoft–Google architecture contains no comparable separation. It converts administrative capability directly into operational authority with no independent verification that the asserted authority derives from the device owner.

IV

The "Enterprise Feature" Defence Destroyed by Its Own Premise

The companies will claim that ExtensionInstallForcelist is a legitimate enterprise tool being abused by malware. This argument evades the central question.

An enterprise feature derives its authority not from the raw administrative token but from the consent of the organisation that owns and manages the device. The admin token is the mechanism, not the source of authority. On a consumer device, there is no organisation. The only source of lawful authority is the consumer's own explicit, informed consent. The architecture provides no pathway for that consent to be expressed or verified.

> *In re Pharmatrak, Inc. Privacy Litigation confirms that consent under ECPA must be actual rather than constructive. Knowledge of a system's monitoring capability cannot be equated with implied consent. The burden of proving consent rests on the party asserting the exception. The architecture provides no mechanism by which that burden could ever be met on a consumer device.*

If a telephone exchange included a "maintenance listening" switch activatable by any key-holder on any household line, and the company shipped that exchange to every home, no regulator would call it an enterprise feature. They would call it a built-in wiretap capability and order it removed or gated by an independent consent mechanism. The FTC said exactly that to Lenovo. The same logic applies here.

V

The Regulatory Charge

The charge is no longer a matter of technical interpretation. It is a matter of legal principle already settled in communications law, property law, privacy tort, FTC enforcement, and Supreme Court statutory interpretation — and now demands application to the computing platform.

Microsoft and Google have jointly deployed an architecture in which raw administrative privilege — an attacker's technical capability — is treated as the legal equivalent of the device owner's consent to silently intercept all electronic communications. This architecture contains no independent consent gate of any kind. The two companies have, by this design, created an environment where consumer devices are functionally pre-wired for mass, non-consensual surveillance, activated by nothing more than a privilege escalation. Wiretap law, trespass doctrine, intrusion upon seclusion, Van Buren v. United States, and the Lenovo/Superfish enforcement record all preserve a single unifying principle: capability is not authority. Access is not consent. The key is not the right. The Microsoft–Google architecture violates this principle by design. The law must now recognise that administrative privilege is not consent, and mandate an ownership-validation gateway that the architecture deliberately omits.

The only question that remains is whether regulators will permit the computing industry to sustain a consent-void interception architecture that was outlawed in the telephone industry decades ago and that stands in direct tension with the broader fabric of American legal doctrine.

AMENDMENT

Legal Methodology Note: Contemporaneity, Statutory Scope, and Applicable Law

This amendment is appended in the interest of analytical transparency. The architectural argument is supported by verified authorities across five independent legal frameworks. The following note identifies the one area of federal case law that limits direct application of 18 U.S.C. § 2511 to certain fact patterns within this exploit chain, and identifies the statutes that apply where the Wiretap Act's primary provision does not.

The Contemporaneity Requirement

Every federal circuit to have ruled on the issue holds that an "intercept" under Title I of ECPA requires acquisition contemporaneous with transmission. Luis v. Zang, 833 F.3d 619 (6th Cir. 2016); Boudreau v. Lussier, 901 F.3d 65 (1st Cir. 2018); Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002). A browser extension reading live web traffic, form inputs, and session cookies in real time satisfies this requirement. Where an extension captures data from storage rather than in transit, the Stored Communications Act (18 U.S.C. § 2701) applies with independent civil and criminal liability.

Consent Standard

Under In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003), consent under ECPA must be actual and specific, not constructive. Consent cannot be inferred from mere service use or knowledge of a system's monitoring capability. The burden rests on the party asserting the exception.

Additional Applicable Law

The consent-gate argument holds independently under: CFAA (18 U.S.C. § 1030) — unauthorized access to a protected computer; FTC Act Section 5 (15 U.S.C. § 45) — unfair practices causing substantial unavoidable consumer injury, confirmed by Lenovo/Superfish; GDPR Article 7 / UK GDPR Article 7 — for EU and UK residents; and Restatement (Second) of Torts §§ 217, 218, 652B under digital trespass and intrusion upon seclusion.

SOURCES

Verified Citations and Research

All claims are sourced from primary legal texts, official platform documentation, documented security research, or verified case law.

Federal Statutes

- 18 U.S.C. § 2511 — Wiretap Act / ECPA Title I
- 18 U.S.C. § 2510(17) — Definition of electronic storage
- 18 U.S.C. § 2701 — Stored Communications Act / ECPA Title II
- 18 U.S.C. § 1030 — Computer Fraud and Abuse Act
- 15 U.S.C. § 45 — FTC Act Section 5

Case Law

- Van Buren v. United States, 593 U.S. 374, 141 S. Ct. 1648 (2021)
- Luis v. Zang, 833 F.3d 619 (6th Cir. 2016)
- Boudreau v. Lussier, 901 F.3d 65 (1st Cir. 2018)
- Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)
- In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003)
- In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020)
- Angel Cole v. Quest Diagnostics (2025 — Third Circuit party exception)
- Nichols v. PeaceHealth Networks, 2026 WL 607763 (W.D. Wash. 2026)
- Durenleau v. Allied (3rd Cir. August 2025 — Van Buren applied)
- Sotelo v. DirectRevenue, LLC — client-side spyware trespass confirmed
- Thomas Kerrins v. Intermix Media, Inc. — adware remediation = actionable harm
- S&S; Activewear LLC v. Promo Hunt, Inc. (2026) — browser is user's exclusive chattel
- CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997)
- Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (Cal. 2003)

FTC Enforcement

- FTC v. Lenovo (United States) Inc., Docket No. C-4636 (2017) — 20-year consent decree; $8.3M settlement; Superfish/Komodia MitM adware
- FTC Complaint No. 1523134 — Lenovo preloaded software without consent

Platform Documentation

- Google Chrome ExtensionInstallForcelist — chromeenterprise.google/policies
- Microsoft Edge ExtensionInstallForcelist — learn.microsoft.com/en-us/deployedge
- Google Chrome Help thread — support.google.com/chrome/thread/85246598

Security Research

- ReasonLabs (August 2024) — 300,000 Chrome/Edge browsers compromised via ExtensionInstallForcelist; reported by BleepingComputer
- Loginsoft (January 2026) — SkilledSearchAdvise Trojan; registry injection

• Malwarebytes (2022) — forced extensions + Scheduled Task re-injection confirmed

Legal Analysis

• Covington & Burling LLP (2020) — Key Issues in ECPA Litigation

• Congressional Research Service R41733 — Privacy: An Overview of ECPA

• Bureau of Justice Assistance — ECPA overview — bja.ojp.gov

• Darrow AI (July 2025) — Defining Interception: Wiretap Laws in the Digital Age

• Troutman Privacy (2026) — Privacy Litigation Report: December 2025 Decisions

• Data Matters / Sidley (August 2025) — Van Buren in Action: Third Circuit

• EFF Internet Law Treatise — Trespass to Chattels digital case survey

• Berkeley Technology Law Journal — Cyberspace Trespass to Chattels

CIRCUITTELLIGENCE

Beautiful Intelligence, Bounded.

Prepared for use in formal regulatory submissions, antitrust proceedings, and investigative reporting. The simplest analogy, fully applied, combined with the established legal distinction between capability and authority, leaves the defence with no permission source to cite and no argument that survives its own logic.

circuittelligence.com/briefs/consent-gate-brief-v1.pdf