The Jurisprudence of Administrative Privilege versus User Consent: Analyzing Wiretap, Digital Trespass, Intrusion upon Seclusion, and Computer Fraud Boundaries in Operating System and Browser Environments

The Wiretap Act, Contemporaneous Interception, and Joint Liability

The interaction between administrative control and user privacy in modern operating systems and web browsers is increasingly governed by federal and state electronic surveillance laws. Under the Federal Wiretap Act, codified as Title I of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2511, it is a criminal offense and a civil liability trigger to intentionally intercept, disclose, or use any wire, oral, or electronic communication. The statute provides a private right of action for any person whose communication is intercepted, allowing them to recover compensatory and punitive damages, along with attorney's fees and costs. Violations can also lead to criminal penalties, including up to five years in prison and civil fines of up to $10,000 per violation.

The application of this statutory framework to browser environments depends on the legal distinction between a contemporaneous "interception" and a subsequent access to "stored communications". Courts have consistently held that Wiretap Act liability attaches only if the acquisition of the electronic communication occurs contemporaneously with its transmission. Once an electronic communication has completed its transfer, it enters "electronic storage" under 18 U.S.C. § 2510(17), placing it outside the scope of the Wiretap Act and under the sole purview of the Stored Communications Act (SCA).

statutory Exception / Legal Boundary	statutory Provision	Standard of Proof / Application	Key Case Law
Contemporaneous Interception	18 U.S.C. § 2511(1)(a)	Requires proof that electronic information was acquired in flight during transfer.	*Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016) ; *Boudreau v. Lussier*, 901 F.3d 65 (1st Cir. 2018).
Consent Exception	18 U.S.C. § 2511(2)(d)	Demands actual, knowing consent; constructive consent or mere service purchase is insufficient.	*In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9 (1st Cir. 2003).
Direct Party Status	18 U.S.C. § 2511(2)(d)	Direct parties are	*Angel Cole v. Quest*

statutory Exception / Legal Boundary	statutory Provision	Standard of Proof / Application	Key Case Law
		generally exempt, but platforms that duplicate and route data to third parties lose this status.	*Diagnostics*, 2025 litigation ; *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).
Secondary Liability Limitation	18 U.S.C. §§ 2511 & 2520	Aiding and abetting is rejected, but developers providing active cloud infrastructure face direct liability.	*Nichols v. PeaceHealth Networks*, 2026 WL 607763 (W.D. Wash. 2026) ; *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016).

This contemporaneity requirement is highly relevant when evaluating third-party tracking tools, such as session replay scripts, chatbots, or pixels embedded on websites. Under the standard articulated by the Ninth Circuit in *Gutierrez v. Converse Inc.*, a plaintiff must present hard evidence of an actual, contemporaneous capture of a live communication rather than the mere technical capability of the tool to access or record messages. If a technology provider merely designs a tool that is capable of tracking but does not actively execute the interception on its own servers, it cannot be held liable under the second clause of California's wiretap statute, California Invasion of Privacy Act (CIPA) § 631(a).

The limits of joint and secondary liability under the Wiretap Act further define this boundary. Most federal jurisdictions reject secondary "aiding and abetting" or "procuring" liability under the Wiretap Act, as seen in *Nichols v. PeaceHealth Networks on Demand LLC*, which held that a website operator cannot be held secondarily liable for using third-party software that captures and transmits user interactions. However, under *Luis v. Zang*, if the software developer of a monitoring tool (such as *WebWatcher*) provides active, cloud-based infrastructure to route, record, and store contemporaneous transmissions on its own servers, the developer is considered to be directly engaged in the act of interception.

The definition of "consent" remains a key battleground under the Wiretap Act, especially given state-level differences, where thirty-eight states and the District of Columbia permit one-party consent, while eleven states (including California, Illinois, Pennsylvania, and Washington) require all-party consent. In *In re Pharmatrak, Inc. Privacy Litigation*, the First Circuit established strict standards for implied consent in digital environments. The court ruled that consent under the ECPA must be actual rather than constructive, and it warned that consent should not casually be inferred.

In the absence of explicit notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception. The court emphasized that a user's knowledge of the mere capability of a system to monitor communications cannot be equated with implied consent. Furthermore, the First Circuit rejected the argument that consent can be inferred from the mere purchase of a service, holding that a reviewing court must look at the specific dimensions of the consent to determine whether the interception exceeded those boundaries. Finally, the burden of proving consent in civil ECPA litigation is placed squarely on the party seeking to benefit from the exception.

This standard complicates the "party exception" defense, which shields direct parties to a communication from wiretap liability. In pixel tracking cases like *Angel Cole v. Quest*

Diagnostics, the Third Circuit found that because the user's web browser transmitted communications directly and simultaneously to the pixel provider, the provider was a direct party to the communication, making the party exception applicable. This contrasts with the Ninth Circuit's holding in *In re Facebook, Inc. Internet Tracking Litigation*, where the platform simultaneously duplicated and routed communications to its own servers, stripping it of "party" status because it acted as an independent interceptor rather than an intended recipient.

Digital Trespass to Chattels, Registry Exploits, and the Limits of Platform Control

The common law tort of trespass to chattels has transitioned from protecting tangible personal property against physical intermeddling to shielding digital environments against unauthorized software installations, spyware, and registry modifications. Under Restatement (Second) of Torts § 217, the tort requires proof of an intentional dispossession or unauthorized intermeddling with a chattel in the possession of another.

The Evolution from Server-Side to Client-Side Trespass

The early phase of digital trespass to chattels focused primarily on protecting server resources and database integrity from automated crawlers and high-volume email spam. These cases established that electronic signals could satisfy the common law "physical contact" requirement.

Case Name and Citation	Target Chattel	Nature of Digital Intrusion	Legal Holding and Standard of Harm
CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997)	ISP Mail Servers	High-volume commercial email spam.	Electronic signals constitute physical contact; unauthorized spam that depletes server space and processing power causes actionable harm under § 218(b).
eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000)	E-commerce Database Servers	Automated web "spiders" crawling auction data.	Even without physical damage, automated queries that place a measurable burden on server capacity and bandwith support an injunction.
Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (Cal. 2003)	Corporate Email Servers	Distribution of noncommercial emails to employees.	Narrowed the tort; holding that electronic communication is not trespass to chattels unless it causes actual hardware damage or impairs physical system functioning.

Case Name and Citation	Target Chattel	Nature of Digital Intrusion	Legal Holding and Standard of Harm
Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004)	WHOIS Database Servers	High-volume search queries for data harvesting.	Confirmed that unauthorized queries exceeding the owner's terms of use constitute a digital trespass if they threaten system stability.

As digital distribution models evolved, courts expanded the tort to client-side consumer devices. In *Sotelo v. DirectRevenue, LLC*, a federal court ruled that the surreptitious downloading of spyware onto a user's computer constitutes a trespass to chattels. The court explained that physical destruction of the hardware is not necessary; rather, software that runs without consent, slows down the machine, depletes bandwidth, drains system memory, and floods the screen with pop-up advertisements causes sufficient "interference" to state a claim. Similarly, in *Thomas Kerrins v. Intermix Media, Inc.*, the court held that a trespass claim was viable where adware surreptitiously bundled with free software impaired the system's efficiency and required technical expertise and expense to remove.

Registry Modification and the Abuse of Administrative Policies

The modern equivalent of this client-side trespass is the unauthorized exploitation of enterprise administrative settings to bypass browser and operating system security. Specifically, malware campaigns frequently target the ExtensionInstallForcelist policy utilized by Google Chrome and Microsoft Edge. This policy is designed to let enterprise administrators silently deploy extensions across managed networks without user interaction.

Malware developers, such as those behind the *SkilledSearchAdvise* Trojan, bypass user consent by obtaining local administrative privileges and writing extension IDs directly into the Windows Registry or macOS configuration files. These malicious entries are typically written to:

```
HKLM\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist
HKLM\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist
```

By hard-coding these registry values, the malware forces the browser to silently install adware or search-redirecting extensions directly from the official web stores. Once installed, these extensions cannot be disabled, turned off, or uninstalled by the user, even if Developer Mode is enabled.

The browser then displays a persistent message indicating that the browser is "managed by your organization," misleading the user and stripping them of possessory control over their own application. This technical hijacking constitutes a clear trespass to the user's local chattel, as it intentionally degrades browser performance, intercepts search queries, and prevents the user from managing their own software environment.

This client-side trespass must be distinguished from actions that occur after data has left the user's device. In *S&S Activewear LLC v. Promo Hunt, Inc.*, a retailer argued that a price comparison browser extension that superimposed overlays on its website committed a trespass to its "digital real estate". The court rejected this argument, holding that once a web page's bits have been transmitted to the consumer's web browser, they are no longer in the retailer's possession.

Because the retailer did not possess the consumer's browser or computer, it had no property right in how those bits were displayed. This ruling establishes that the browser application and local registry are the exclusive chattels of the end user, meaning that any unauthorized administrative intervention inside this local environment is a trespass committed against the user, not the remote web services they access.

Intrusion upon Seclusion, Tracking Technology, and Consent Frameworks

The common law tort of intrusion upon seclusion, codified under Restatement (Second) of Torts § 652B, protects individuals from intentional, highly offensive invasions into their private affairs or concerns. In the digital landscape, this tort has become a primary vehicle for challenging covert tracking and data collection technologies that bypass or override explicit user preferences.

Covert Tracking and the Seclusion Standard

The application of the intrusion tort to online activity was clarified by the Ninth Circuit in *In re Facebook, Inc. Internet Tracking Litigation*. In that multidistrict litigation, plaintiffs alleged that Facebook tracked their post-logout web browsing histories by using persistent cookies (such as datr and c_user cookies) embedded in their browsers. Whenever logged-out users visited third-party websites containing integrated Facebook content, like "Like" or "Share" buttons, the browser was triggered to send a transmission back to Facebook's servers, identifying the specific URL visited.

The Ninth Circuit held that the concept of "seclusion" is flexible enough to encompass a user's web browsing habits. The court ruled that covertly tracking users across third-party websites to build comprehensive personal profiles constitutes an invasion of social norms and a plausible intrusion upon seclusion.

This standard establishes that the nature of the collection, the sensitivity of the data, and the covert means employed must be evaluated to determine whether the tracking would highly offend a reasonable person. Similar principles were tested in *In re DoubleClick Inc. Privacy Litigation*, where the court scrutinized whether tracking cookies placed on user devices to build advertising profiles exceeded the scope of the website's authorization.

Broken Banners and California's Pen Register Laws

The threshold of liability in modern tracking cases often turns on "broken banner" claims. In late 2025, federal courts in California denied motions to dismiss in privacy class actions where plaintiffs argued that website cookie consent banners failed to operate properly. The plaintiffs in these cases carefully studied the disclosures and explicitly opted out of non-essential tracking cookies. Despite this election, the defendants ignored the choice and permitted third-party tracking technologies to be loaded on the users' devices.

The courts held that these allegations stated a viable claim for intrusion upon seclusion. By offering an opt-out mechanism and subsequently ignoring the user's choice, the defendants established a reasonable expectation of privacy that they immediately violated. This broken banner framework effectively vitiates the defense of consent.

Additionally, the courts rejected arguments that pen register and trap and trace statutes apply

only to traditional telephone lines, holding that modern cross-device tracking software that monitors and logs a user's web interactions across multiple platforms operates in a manner analogous to a pen register.

System Trust and the Lenovo Superfish Vulnerability

The most prominent historical example of administrative privilege substituting for user consent is the Lenovo Superfish "VisualDiscovery" scandal. Between August 2014 and early 2015, Lenovo preloaded "VisualDiscovery" adware on forty-three different models of consumer laptops. Developed by Superfish, Inc., this software injected targeted advertisements into web pages by hovering over similar products.
To inspect and modify encrypted HTTPS traffic, the software utilized a tool called Komodia to install a self-signed root certificate directly into the local trusted Certificate Authority (CA) store of the operating system. This technical implementation had severe security implications:

- **Man-in-the-Middle (MitM) Execution:** The software intercepted and decrypted all browser communications, acting as an unauthorized intermediary between the consumer's browser and secure websites, including financial and medical institutions.
- **System Trust Exploitation:** Because the software bypassed standard browser SSL/TLS certificate verification, secure websites appeared valid even when their traffic was being local-proxied and analyzed.
- **Critical Security Vulnerabilities:** Researchers discovered that the private key for the self-signed root certificate was identical across all affected laptops and could be cracked in less than an hour. This allowed any attacker on a shared local network, such as a public Wi-Fi hotspot, to execute silent MitM attacks, hijack browsers, and steal bank credentials or medical information.

The Federal Trade Commission (FTC) charged that Lenovo preloaded this software without adequate notice or consent, compromising online security protections. The resulting enforcement action led to a 20-year consent decree requiring Lenovo to obtain affirmative consumer consent before pre-installing ad-injecting software, alongside $8.3 million in class action settlements. This case demonstrates how overriding system trust infrastructure without explicit user consent violates reasonable privacy expectations and exposes platform providers to significant joint liability.

The Van Buren "Gates-Up-or-Down" Framework in Platform Environments

The boundary between technical access capability and legal authorization is governed by the Supreme Court's landmark decision in *Van Buren v. United States*. The ruling, along with its subsequent application, is critical to the argument that administrative capability cannot be substituted for actual user consent.

The Facts and Statutory Mechanics of Van Buren

The petitioner, Nathan Van Buren, was a police sergeant who used his valid credentials to search the Georgia Crime Information Center database for license-plate records in exchange for a $6,000 payment from a private individual. Although his search violated explicit departmental policies restricting database use to law enforcement purposes, he was charged and convicted

under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2).
The Supreme Court addressed whether a person authorized to access information on a computer for certain purposes violates the CFAA if they access that same information for an improper purpose. Under 18 U.S.C. § 1030(e)(6), "exceeds authorized access" is defined as accessing a computer with authorization and using such access to obtain or alter information in the computer that the accessor is "not entitled so to obtain or alter".
The government argued that "entitled so" referred to the purpose of the access, meaning that an authorized employee exceeds access when they retrieve information for an unauthorized reason. Van Buren countered that the term "so" refers to the specific manner or technical pathway of access, meaning that he was entitled to obtain the information because his credentials permitted him to access those specific database files.

The Gates-Up-or-Down Rule and Its Progeny

Writing for a 6-3 majority, Justice Barrett adopted Van Buren's narrow interpretation, establishing the "gates-up-or-down" framework. The Court held that liability under both the "without authorization" and "exceeds authorized access" prongs of the CFAA stems from a binary, technical inquiry. Under this framework, a computer system or a specific database within it has a virtual "gate". If a user has valid credentials that permit them to access that specific area (the gate is up), they do not violate the CFAA, regardless of their improper motives or subsequent policy violations.
This gate-based distinction has been strictly applied by federal courts of appeals. In the August 2025 decision *Durenleau v. Allied* (as reported in *Data Matters*), the Third Circuit evaluated whether employees who shared login credentials to retrieve password spreadsheets in violation of corporate computer-use policies violated the CFAA.
The Third Circuit affirmed summary judgment for the employees, holding that because they had legitimate access to the corporate systems, their violations of internal policies did not constitute "unauthorized access" or "exceeding authorized access". The court emphasized that expanding the CFAA to cover internal policy infractions would improperly turn a statute designed to target code-based hacking into a broad tool for policing workplace conduct.

Applying the Gate Analogy to Browser and OS Environments

The *Van Buren* "gates-up-or-down" model provides a clear conceptual framework for the interaction between administrative privilege and user consent. In operating systems and web browsers, administrative privilege represents a "gate-up" status. Technically, the operating system permits an application running with root or administrative privileges to overwrite local files, modify the Windows Registry, or install self-signed root certificates.
However, *Van Buren* and its progeny establish that technical capability does not define the legal boundaries of authorized purpose. Just as an employee with valid technical credentials violates legal limits when misusing database access, an application with administrative write access does not possess a blanket legal license to alter the user's computing environment.
If a platform provider or developer uses system-level privileges to bypass user consent—for example, by forcing extensions or injecting certificates—the existence of the technical "gate-up" status does not shield them from common law liability. Common law protections, including trespass to chattels and intrusion upon seclusion, remain active to govern this gap, ensuring that technical access cannot legally substitute for actual, informed user consent.

Conclusions and Platform Implications

The synthesis of federal statutory frameworks, state-level privacy variations, and evolving common law doctrines leads to several key conclusions that govern browser and operating system environments:

- **Administrative Power is Not Consent:** Under the First Circuit's *Pharmatrak* precedent, consent must be actual and specific rather than constructive. High-level operating system privileges are administrative utilities designed for system maintenance, not legal substitutes for actual user agreement.
- **Defeating the "Platform Consent" Defense:** In cookie and web tracking environments, courts have firmly rejected the idea that consent can be implied from the mere passive use of a service. The "broken banner" decisions of late 2025 prove that when a user actively selects a privacy setting, any technical bypass of that choice by a tracking tool constitutes an actionable tort.
- **Redefining Platform Joint Liability:** The pre-installation and MitM precedents from *Lenovo/Superfish* , combined with the infrastructure-based liability rules from *Luis v. Zang* , show that companies providing the distribution channels or hosting services for unauthorized monitoring software face severe joint liability. If a platform provider actively cooperates with or hosts services that bypass standard browser protections, they cannot avoid liability by claiming to be a passive distributor.
- **Structural Integrity of the OS and Browser:** Under the *Van Buren* doctrine, technical capability must remain separate from legal authority. Operating systems and browsers must maintain robust code-based barriers to prevent malware from manipulating keys like ExtensionInstallForcelist. A technical configuration that allows a script to write to the registry does not create a defense of consent under the common law of digital trespass.

These legal principles demonstrate why major platform operators seek to defend the boundary between technical capability and legal authorization. By ensuring that system-level privileges cannot be used to bypass user choice, platforms can protect their software environments from unauthorized exploitation and insulate themselves from joint liability under federal and state privacy laws.

Works cited

1. Key Issues in Electronic Communications Privacy Act (ECPA) Litigation - Covington & Burling LLP, https://www.cov.com/-/media/files/corporate/publications/2020/06/key-issues-in-electronic-communications-privacy-act-ecpa-litigation.pdf 2. Litigation Alert: The Sixth Circuit Expands Potential… | Fenwick, https://www.fenwick.com/insights/publications/litigation-alert-the-sixth-circuit-expands-potential-federal-wiretap-act-liability-for-developers-and-sellers-of-cloud-based-monitoring-software 3. Secretly Recording Workplace Conversations Makes for Risky Business - Articles - Tennessee Bar Association, https://www.tba.org/?pg=Articles&blAction=showEntry&blogEntry=109526 4. Use or Disclosure of E-mails Hacked by a Foreign Adversary - Department of Justice, https://www.justice.gov/olc/media/1385376/dl?inline 5. Defining Interception: Wiretap Laws in the Digital Age - Darrow AI, https://www.darrow.ai/resources/wiretap-interceptions-in-the-digital-age 6. Third Circuit Provides Helpful Guidance on the "Party Exception" to Wiretap Liability and What Constitutes "Medical

Information" Under the CMIA | Privacy + Cyber + AI, https://www.troutmanprivacy.com/2025/11/third-circuit-provides-helpful-guidance-on-the-party-exception-to-wiretap-liability-and-what-constitutes-medical-information-under-the-cmia/ 7. Court Dismisses Federal Wiretap Claim Premised on Crime-Tort Exception, Rejects Aiding-and-Abetting Liability | Inside Class Actions, https://www.insideclassactions.com/2026/03/16/court-dismisses-federal-wiretap-claim-premised-on-crime-tort-exception-rejects-aiding-and-abetting-liability/ 8. Internet Privacy Litigation Continues to Create Uncertainty for Websites Using Third-Party Technology while Expanding to More States | Insights & Resources | Goodwin, https://www.goodwinlaw.com/en/insights/publications/2023/10/alerts-otherindustries-dpc-internet-privacy-litigation-create-uncertainty 9. Federal Appeals Court Hands Out Win in Website Chat Wiretap Case: What It Means for Your Business | Fisher Phillips LLP, https://www.fisherphillips.com/en/insights/insights/federal-appeals-court-hands-out-win-in-website-chat-wiretap-case 10. Phone Call Recording Laws: What You Need to Know | Rev, https://www.rev.com/blog/phone-call-recording-laws-state 11. Telephone and electronic communications Archives | The Reporters Committee for Freedom of the Press, https://www.rcfp.org/reporters-recording-sections/telephone-and-electronic-communications/ 12. In Re Pharmatrak, Inc. Privacy Litigation, Noah Blumofe, on Behalf of ..., https://law.justia.com/cases/federal/appellate-courts/F3/329/9/576444/ 13. Trespass to chattels - Wikipedia, https://en.wikipedia.org/wiki/Trespass_to_chattels 14. Beware of Internet trespass - Duane Morris LLP, https://www.duanemorris.com/articles/article2093.html 15. Spyware can constitute illegal trespass on home computers - Duane Morris, https://www.duanemorris.com/articles/article1988.html 16. Trespass to Chattels in the Age of the Internet - Washington University in St. Louis Scholarly Repository, https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1337&context=law_lawreview 17. Zissu et al v. IH2 Property Illinois LP, No. 1:2015cv02394 - Document 51 (N.D. Ill. 2016), https://law.justia.com/cases/federal/district-courts/illinois/ilndce/1:2015cv02394/307969/51/ 18. "Internet Property Rights: E-Trespass." by John D. Saba Jr., https://commons.stmarytx.edu/thestmaryslawjournal/vol33/iss2/4/ 19. Looking for Line Where Web Use Crosses into Trespassing - Duane Morris, https://www.duanemorris.com/news/news3940.html 20. THE CONTINUING EXPANSION OF CYBERSPACE TRESPASS TO CHATTELS - Berkeley Technology Law Journal, https://btlj.org/data/articles2015/vol17/17_1_AR/17-berkeley-tech-l-j-0421-0444.pdf 21. Should the English Legal System Adopt the US Law of Cyber-trespass? - SCRIPTed, https://script-ed.org/article/english-legal-system-adopt-law-cyber-trespass/ 22. Sotelo v. Directrevenue, LLC: Paving the Way for Spyware-Free Internet - Santa Clara Law Digital Commons, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1418&context=chtlj 23. Beware of Internet Trespass - Supreme Court - FindLaw, https://supreme.findlaw.com/legal-commentary/beware-of-internet-trespass.html 24. Remove ExtensionInstallForcelist in Chrome on Mac - MacSecurity, https://macsecurity.net/view/492-extensioninstallforcelist-chrome-policy-mac 25. New Trojan Malware Exploits Users with Rogue Chrome and Edge Extensions - Loginsoft, https://www.loginsoft.com/post/new-trojan-malware-exploits-users-with-rogue-chrome-and-edge-extensions 26. Microsoft Edge Browser Policy Documentation ExtensionInstallForcelist, https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies/extensioninstallforcelist 27. How can I remove the ExtensionInstallForcelist policy installed by malware - Google Help, https://support.google.com/chrome/thread/85246598/how-can-i-remove-the-extensioninstallforcelist-policy-installed-by-malware?hl=en 28. Plaintiffs Are Still Litigating-and Losing-Website

Framing Cases (S&S v. Promo Hunt), https://blog.ericgoldman.org/archives/2026/04/plaintiffs-are-still-litigating-and-losing-website-framing-cases-ss-v-promo-hunt.htm 29. No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion - The Fordham Law Archive of Scholarship and History, https://ir.lawnet.fordham.edu/flr/vol83/iss6/18/ 30. Liking the Intrusion Analysis in In Re Facebook - UF Law Scholarship Repository - University of Florida, https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=2282&context=facultypub 31. Privacy Litigation Report: Takeaways From December 2025 Decisions, https://www.troutmanprivacy.com/2026/01/privacy-litigation-report-takeaways-from-december-2025-decisions/ 32. Order re: Motion to Dismiss, Dkt. 45 , by Magistrate Judge Alex G. Tse. (agtlc2, COURT STAFF) (Filed on 12/22/2025) - U.S. Case Law - Justia, https://cases.justia.com/federal/district-courts/california/candce/3:2025cv03645/448581/50/0.pdf 33. Facebook Hit With $15B Complaint In User Tracking MDL (Law360) - Cooley, https://www.cooley.com/news/coverage/2012/facebook-hit-with-15b-complaint-in-user-tracking-mdl-ilaw360i 34. In re Facebook Internet Tracking Litigation - Santa Clara Law Digital Commons, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2079&context=historical 35. Does the Use of "cookies" Give Rise to a Private Cause of Action for Invasion of Privacy in Minnesota - Mitchell Hamline Open Access, https://open.mitchellhamline.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1807&context=wmlr 36. In Re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4 (D. Mass. 2002) - Justia Law, https://law.justia.com/cases/federal/district-courts/FSupp2/220/4/2533670/ 37. 152 3134 UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION Commissioners: Maureen K. Ohlhausen, Acting Chairman Terre, https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_complaint.pdf 38. Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security | Federal Trade Commission, https://www.ftc.gov/news-events/news/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled-software-its-laptops-compromised-online 39. Lenovo Spyware - Joseph Saveri Law Firm, https://www.saverilawfirm.com/settlement/test/ 40. Superfish Adware Poses High Security Threat to Lenovo Users, https://www.classlawgroup.com/lenovo-superfish-lawsuit 41. SuperFish Vulnerability - Lenovo Support US, https://support.lenovo.com/us/en/product_security/ps500035-superfish-vulnerability 42. The U.S. Supreme Court issued its opinion in Van Buren v. United States, https://www.langleybanack.com/lb-client-alert-the-united-states-supreme-court-issued-its-opinion-in-van-buren-v-united-states-defining-what-activity-falls-under-the-exceeds-authorized-access-of-the-federal-co/ 43. 19-783 Van Buren v. United States (06/03/2021) - Supreme Court, https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf 44. November | 2020 - Patently-O, https://patentlyo.com/2020/11 45. Van Buren v. United States | Supreme Court Bulletin - Law.Cornell.Edu, https://www.law.cornell.edu/supct/cert/19-783 46. Supreme Court Narrows Scope Of Computer Fraud and Abuse Act, Holding It Does Not Prohibit Accessing Otherwise Available Information For An Improper Purpose - Gibson Dunn, https://www.gibsondunn.com/supreme-court-narrows-scope-of-computer-fraud-and-abuse-act-holding-it-does-not-prohibit-accessing-otherwise-available-information-for-an-improper-purpose/ 47. Van Buren in Action: Third Circuit Rejects Application of the Computer Fraud and Abuse Act (CFAA) to Violations of Workplace Policies | Data Matters Privacy Blog, https://datamatters.sidley.com/2025/08/29/van-buren-in-action-third-circuit-rejects-application-of-the-computer-fraud-and-abuse-act-cfaa-to-violations-of-workplace-policies/