

Privacy in the Shadows

A Technical Audit of Surveillance Technologies on Adult Platforms

January 2026

Abstract

This study presents a systematic technical audit of 38 major adult industry platforms, analyzing tracking technologies, fingerprinting mechanisms, session recording practices, and data sharing relationships. Our automated scanner detected 164 distinct tracking technologies across the sample, with an average privacy score of 37/100. We find that 87% of platforms employ browser fingerprinting techniques, 76% engage in likely session recording, and 89% transmit keystroke data to third parties. Notably, platforms serving vulnerable populations—arrangement dating sites and creator platforms—demonstrate the poorest privacy practices, with average scores of 6/100 and 35/100 respectively. These findings have significant implications for user safety in contexts where privacy breaches carry elevated risks of harm.

Table of Contents

- 1. [Introduction](#)
- 2. [Platform Findings](#)
- 3. [The Limits of User Countermeasures](#)
- 4. [Tracking Technologies Detected](#)
- 5. [Methodology](#)
- 6. [Discussion](#)
- 7. [Conclusion](#)

Appendices

- [Appendix A: Terminology](#)
- [Appendix B: Full Platform Scores](#)
- [Appendix C: Methodology Details](#)

Chapter 1: Introduction

1.1 Summary of Findings

This report presents the findings of an independent privacy audit conducted in January 2026, examining tracking technologies deployed across 38 adult content platforms. The results reveal an industry where surveillance is the norm, privacy is the exception, and the most vulnerable users face the greatest exposure.

The Numbers

38 platforms analyzed. Average privacy score: 37 out of 100.

That figure alone tells a story. On our 100-point scale, where 70 represents acceptable privacy practices and 90 indicates genuine respect for user data, the industry average falls firmly into "poor" territory. Only two platforms achieved scores above 80. Twelve platforms scored below 25, placing them in what we classify as the "surveillance" tier—the most invasive category in our assessment framework.

Category	Platforms	Average Score	Worst Score	Best Score
Escort Directories	7	60/100	12/100	90/100
Creator Platforms	3	35/100	0/100	82/100
Cam Sites	8	32/100	0/100	64/100
Tube Sites	8	18/100	0/100	43/100
Major Studios	6	38/100	23/100	66/100
Clip Sites	2	45/100	32/100	58/100
Arrangement & Dating	2	6/100	0/100	11/100
Social & Community	2	77/100	69/100	84/100

The Extremes

Worst performer: LoyalFans (0/100)

LoyalFans, a creator platform marketed as an OnlyFans alternative, achieved the lowest possible score in our audit. The platform deploys extensive fingerprinting technologies, session recording, keystroke monitoring, and shares data with multiple advertising networks. For creators and subscribers seeking an alternative to mainstream platforms, LoyalFans offers worse privacy, not better.

Best performer: Skip The Games (90/100)

Skip The Games, an escort directory, earned the highest score in our audit by demonstrating that privacy-respecting design is achievable in this industry. The platform uses only Cloudflare's privacy-focused analytics, deploys no third-party advertising trackers, and avoids session recording or fingerprinting technologies. This proves that the surveillance observed elsewhere represents a choice, not a technical necessity.

Surveillance Technologies in Detail

Our automated scanner detected the following tracking capabilities across the 38 platforms:

Fingerprinting: 87% of platforms (33 of 38)

Active fingerprinting allows platforms to identify visitors even when cookies are disabled, private browsing is enabled, or VPNs are used. When a user visits one of these 33 platforms, their browser configuration, hardware characteristics, and

behavioral patterns are harvested to create a unique identifier that persists across sessions and devices. Technologies detected include canvas fingerprinting, WebGL fingerprinting, audio context fingerprinting, navigator property enumeration, and battery status API access.

Session Recording: 76% of platforms (29 of 38)

Session recording captures every mouse movement, click, scroll, form interaction, and DOM change during a user's visit. This data is transmitted to third-party services where it can be replayed as a video of the user's browsing session. On adult content platforms, this means third-party companies possess recordings of exactly what content users viewed, how long they lingered on each image or video, and what search terms they entered.

Keystroke Monitoring: 89% of platforms (34 of 38)

Keystroke logging captures text as users type—before they press submit, before they decide whether to send a message. On platforms where users compose intimate messages, enter search queries for specific content, or fill out profile information, keystroke monitoring represents a profound invasion of privacy. Search queries reveal fantasies. Unsent messages reveal intentions. Profile drafts reveal identities.

Google Data Sharing: 76% of platforms (29 of 38)

Twenty-nine platforms send visitor data to Google through Analytics, Tag Manager, or advertising network integrations. Google's advertising ecosystem reaches across the web, and data collected on adult platforms does not remain siloed. For users who maintain Google accounts—which is to say, most internet users—browsing behavior on adult sites can inform the advertising profiles that follow them across their digital lives.

Meta (Facebook) Data Sharing: 3 platforms

Three platforms integrate Meta's tracking pixel, reporting page views directly to Facebook's advertising infrastructure. Given Meta's extensive data collection and cross-platform tracking capabilities, this integration creates particularly severe privacy risks.

Data Broker Connections: 2 platforms

Two platforms connect to The Trade Desk, a major programmatic advertising platform that facilitates the buying and selling of user data. Platforms connected to data brokers effectively place user profiles on the open market.

Surveillance-Level Classification: 12 platforms

Twelve platforms reached our "surveillance" classification—the most invasive tier. These platforms combine multiple tracking technologies, share data with numerous third parties, deploy session recording, and demonstrate patterns consistent with systematic behavioral surveillance. The platforms include: ListCrawler, Fansly, LoyalFans, CamSoda, LiveJasmin, Pornhub, RedTube, SpankBang, YouPorn, Brazzers, Seeking, and What's Your Price.

Cookie Analysis

Seeking, the arrangement dating platform, deploys 47 cookies total—21 classified as tracking cookies—with 31 having lifetimes exceeding 90 days (see Appendix B.7). This aggressive cookie deployment represents the extreme, but long-lived tracking cookies were common across platforms. The average platform deploys 4 distinct tracking technologies, with the most invasive deploying 8 or more.

1.2 Why This Matters

The privacy stakes on adult content platforms differ fundamentally from those on mainstream websites. When a user's browsing history at a news site or e-commerce platform leaks, the consequences are typically limited to targeted advertising or minor embarrassment. When browsing history at an adult platform leaks, the consequences can include destroyed marriages, lost custody battles, terminated employment, blackmail, violence, and in some jurisdictions, criminal prosecution or death.

The Outing Risk

For LGBTQ+ users, particularly those in hostile family situations or regions with discriminatory laws, browsing history on adult platforms can constitute evidence of sexual orientation or gender identity. Forty-three percent of the platforms we audited share data with Google's advertising network. That data enters systems designed to build comprehensive user profiles.

A single data breach, a subpoena, a rogue employee, or an algorithmic inference could expose users to family rejection, workplace discrimination, or legal jeopardy.

The Employment Threat

In the United States and many other jurisdictions, employers can legally terminate workers based on legal off-duty conduct they find objectionable. Teachers, healthcare workers, government employees, and those with security clearances face particular exposure. The platforms that share user data with advertising networks create records that could surface in background checks, data broker reports, or security clearance investigations.

The Blackmail Vector

Tracking data represents blackmail material. Session recordings that capture exactly what content a user viewed, how long they watched, and what they searched for constitute precisely the kind of compromising information that enables extortion. The 29 platforms with active session recording are creating archives of user behavior that—whether through breach, insider threat, or legal compulsion—could be weaponized against the users who generated that data.

The Violence Risk

For sex workers who use escort directories and advertising platforms, privacy failures carry physical safety implications. Facial recognition, location tracking, and identity correlation technologies threaten the anonymity that sex workers depend on for protection from stalkers, abusive clients, and those who would do them harm. Seven platforms in the escort directory category deploy fingerprinting and behavioral tracking technologies that could facilitate identification of workers who operate under stage names.

The Criminalization Factor

Sex work exists in varying states of legality across jurisdictions. In countries where sex work or certain sexual practices are criminalized, browsing history on adult platforms constitutes potential evidence for prosecution. Platforms that share data with U.S. advertising networks subject that data to U.S. legal processes, including law enforcement requests. Users in jurisdictions with criminalized sex work face prosecution risks that platforms' tracking practices amplify.

The Consent Gap

Tracking technologies operate without meaningful consent. Terms of service that users must accept to access platforms run thousands of words and change without notice. Cookie consent banners, where they exist, default to acceptance and make rejection deliberately difficult. The 87% of platforms that deploy fingerprinting circumvent user choice entirely—fingerprinting works precisely because it does not require consent or cooperation. Users who believe they are browsing privately because they enabled incognito mode or disabled cookies discover too late that these platforms identified them anyway.

1.3 Structure of This Report

This report is organized to serve multiple audiences: users seeking to make informed platform choices, policymakers considering regulatory approaches, platform operators interested in privacy-respecting alternatives, and researchers studying surveillance capitalism in sensitive contexts.

Chapter 2: Platform Findings examines each of the 38 platforms by category—escort directories, creator platforms, cam sites, tube sites, major studios, clip sites, arrangement/dating sites, and social/community platforms. We identify category-specific patterns and highlight both worst offenders and privacy-respecting alternatives.

Chapter 3: The Limits of User Countermeasures explains why VPNs, private browsing, and tracking blockers provide less protection than users expect. We examine the technical reasons these tools fail against fingerprinting and session recording.

Chapter 4: Tracking Technologies Detected provides technical documentation of each tracking technology we found—from Google Analytics to canvas fingerprinting to session recording. We explain what each captures, how it works, and what risks it creates.

Chapter 5: Methodology documents our automated scanning approach, the privacy scoring framework, detection heuristics, and limitations of the analysis.

Chapter 6: Discussion considers implications for users, platform operators, and regulators. We examine why privacy-respecting operation is achievable and what regulatory frameworks might address these findings.

Chapter 7: Conclusion synthesizes findings and offers a call to action for all stakeholders.

Appendices include complete data tables with all calculations (Appendix B), technical methodology details (Appendix C), and a terminology glossary (Appendix A).

A Note on Approach

This report lets data speak. We did not contact platforms for comment or allow them to dispute findings prior to publication. Our scanner detects what platforms deploy, not what they claim in privacy policies. Where platforms' stated practices diverge from their technical implementations, the code tells the truth.

We recognize that some tracking serves legitimate purposes: fraud prevention, security monitoring, performance optimization. We have calibrated our scoring to account for these uses. Platforms lose points for advertising network integration, not for basic analytics. They lose points for fingerprinting, not for session management cookies. They lose points for data broker connections, not for CDN usage.

The findings that follow represent what platforms actually do with user data, measured through automated analysis of their deployed technologies. For the 37% of platforms that scored below 30, what they do is surveillance.

Chapter 2: Platform Findings

This chapter presents the complete analysis of 38 adult platforms across eight categories. Each platform was evaluated using our standardized methodology, with scores reflecting the volume and invasiveness of tracking technologies deployed against users.

2.1 Overview by Category

Category	Platforms	Avg Score	Worst	Best
Escort Directories	7	60/100	ListCrawler (12)	Skip The Games (90)
Creator Platforms	3	35/100	LoyalFans (0)	OnlyFans (82)
Cam Sites	8	32/100	LiveJasmin (0)	MyFreeCams (64)
Tube Sites	8	18/100	Multiple (0)	XVideos (43)
Major Studios	6	38/100	Brazzers (23)	Naughty America (66)
Clip Sites	2	45/100	ManyVids (32)	Clips4Sale (58)
Arrangement & Dating	2	6/100	Seeking (0)	What's Your Price (11)
Social & Community	2	77/100	AdultFriendFinder (69)	FetLife (84)

The data reveals a disturbing pattern: platforms where users have the most to lose from privacy breaches—arrangement/dating sites where discretion is paramount—deploy the most aggressive tracking. The tube site category, representing the highest-traffic adult properties, averages just 18/100, with four platforms scoring zero.

2.2 Escort Directories

Category Average: 60/100 | Common Trackers: Google Analytics, Cloudflare

Escort directories present a mixed picture. These platforms serve a population with legitimate privacy concerns—both providers and clients face real-world consequences if their activity is exposed. Some directories respect this reality; others treat their users as advertising inventory.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
Skip The Games	90/100	A	Analytics Only
Eros	70/100	B+	Advertising
AdultSearch	67/100	B	Advertising
Private Delights	63/100	B	None
Tryst	60/100	B-	Analytics Only
Slix	56/100	B-	Advertising
ListCrawler	12/100	D-	Surveillance

Skip The Games demonstrates that running an escort directory without invasive tracking is entirely possible. The platform deploys only Cloudflare Web Analytics—a privacy-respecting analytics solution that doesn't track individual users across sites. No fingerprinting, no advertising networks, no session recording. The 90/100 score proves the "we need trackers for our business" excuse is exactly that—an excuse.

Eros and **AdultSearch** fall into the standard ad-supported model: Google Analytics, Google Tag Manager, and Google Ads/DoubleClick integration. Every page view is reported to Google's advertising infrastructure. Both platforms deploy keystroke logging and user behavior monitoring. For a site where users search for specific services and locations, keystroke capture is particularly invasive.

Private Delights presents an interesting case: no trackers detected, yet session recording signals were identified. The platform appears to use first-party behavior monitoring rather than third-party tracking—still surveillance, but data presumably stays in-house rather than flowing to Google or ad networks.

Tryst uses PostHog for analytics with session recording likely active. While PostHog can be self-hosted (keeping data in-house), the tracking is still aggressive: 386 surveillance event listeners and 92 MutationObservers monitoring every DOM change.

Slixa combines Google's advertising stack with session recording. The platform had 439 surveillance event listeners during testing—capturing scrolls, mouse movements, clicks, and DOM mutations for exfiltration to third parties.

ListCrawler is the category's worst performer by a wide margin. The platform deploys:

- Yandex Metrica (Russian analytics with known ties to Russian intelligence)
- Battery API fingerprinting (allowing device identification even in private browsing)
- 24 cookies (14 tracking, 13 with >90 day lifetimes)
- 740 surveillance event listeners
- Third-party ad networks (iTransitAuthority, Drome6)

ListCrawler earned "surveillance" classification—the most invasive category in our assessment. Users of this platform are being tracked across the adult web with identifiers that persist through cookie clearing and incognito mode.

Notable Findings

- **Fingerprinting prevalence:** 5 of 7 platforms employ fingerprinting techniques
- **Google dominance:** 5 of 7 platforms share data with Google's advertising network
- **Session recording:** 4 platforms capture mouse movements, clicks, and scrolls for third-party exfiltration
- **Keystroke logging:** All 7 platforms monitor keystrokes in some capacity

2.3 Creator Platforms

Category Average: 35/100 | Common Trackers: Google Analytics, Amplitude, X Corp

Creator platforms—where sex workers upload content and build paying subscriber bases—show extreme variance. OnlyFans maintains reasonable privacy practices; its competitors treat creator and subscriber data as advertising inventory.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
OnlyFans	82/100	A-	Analytics Only
Fansly	23/100	D	Surveillance
LoyalFans	0/100	F	Surveillance

OnlyFans earns the highest score in this category with analytics-only tracking. The platform uses Cloudflare Web Analytics—the same privacy-respecting solution as Skip The Games. No advertising networks, no session recording to third parties. While

navigator fingerprinting is detected, the platform does not deploy aggressive multi-technique fingerprinting like LoyalFans. User behavior monitoring (keystroke logging, copy/paste monitoring) appears to stay first-party.

OnlyFans proves that a creator platform can operate profitably without selling out its users to advertising networks. The platform takes 20% of creator earnings—a revenue model that doesn't require surveillance capitalism.

Fansly paints a grimmer picture. The OnlyFans competitor deploys:

- Google Analytics (GA4) with DoubleClick advertising integration
- Amplitude (behavioral analytics)
- Twitter/X Pixel (sharing data with X Corp's advertising platform)
- Navigator fingerprinting (116 platform checks during a single page load)
- Session recording with third-party exfiltration

Fansly shares subscriber browsing data with both Google and X Corp. Every creator page visited, every video watched, every subscription payment—reported to advertising platforms that build cross-site profiles. For subscribers who value discretion, this is a significant exposure.

LoyalFans scores 0/100—the worst platform in the entire audit. The site deploys every major fingerprinting technique:

- Audio fingerprinting (creates unique identifier from audio processing characteristics)
- Canvas fingerprinting (identifies device from graphics rendering)
- WebGL fingerprinting (extracts GPU information)
- Navigator fingerprinting (device memory, hardware concurrency, platform)
- Battery fingerprinting (monitors battery status API)

LoyalFans also deploys Hotjar for session recording, Google Ads integration, and X Corp widgets. The platform's CSP headers confirm preparation for extensive third-party integration. With 5 distinct fingerprinting methods, LoyalFans can identify visitors even in incognito mode with cookies disabled.

Notable Findings

- **Fingerprinting arms race:** LoyalFans uses 5 fingerprinting techniques; Fansly and OnlyFans both use navigator fingerprinting
 - **Social platform tracking:** Both Fansly and LoyalFans share data with X Corp (Twitter)
 - **Session recording:** Fansly and LoyalFans both capture and exfiltrate user sessions
 - **Revenue model correlation:** OnlyFans (commission-based) respects privacy; competitors (ad-supplemented) do not
-

2.4 Cam Sites

Category Average: 32/100 | Common Trackers: Google Analytics, FingerprintJS, Hotjar

Cam sites—platforms where performers stream live video to paying viewers—show consistently poor privacy practices. The category average of 32/100 reflects widespread deployment of fingerprinting, session recording, and advertising integrations.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
MyFreeCams	64/100	B	Advertising
JerkMate	45/100	C	Extensive
BongaCams	43/100	C	Extensive
Stripchat	40/100	C	Extensive
Cam4	35/100	C-	Extensive
Chaturbate	25/100	D+	Extensive
CamSoda	7/100	F	Surveillance
LiveJasmin	0/100	F	Surveillance

MyFreeCams leads the category with minimal third-party tracking. The platform uses Google Analytics (including the legacy urchin.js implementation) but avoids advertising networks and session recording. Navigator fingerprinting is present but limited (2 language checks, 1 platform check, 1 hardware concurrency check).

JerkMate deploys Crazy Egg for heatmapping and session recording alongside Google's advertising stack. The platform monitors every mouse movement, click, and scroll—5 trackers total with 553 surveillance event listeners.

BongaCams runs Google Analytics with DoubleClick advertising integration. Session recording is active, capturing user behavior for exfiltration. The platform maintains 11 cookies with >90 day lifetimes, enabling long-term tracking.

Stripchat takes a different approach: minimal third-party trackers but WebGL fingerprinting and aggressive session recording. The platform deployed 222 IntersectionObservers during testing—tracking which elements scrolled into view. This suggests detailed scroll-depth analytics, likely for optimizing performer placement.

Cam4 combines Google Analytics with Amplitude and FingerprintJS. The commercial fingerprinting service creates stable identifiers that persist across sessions, browser changes, and cookie clearing.

Chaturbate uses a similar stack: Google Analytics, FingerprintJS, and CSP preparation for Hotjar session recording. The platform registered 5,381 surveillance event listeners during testing—the highest count in the cam category.

CamSoda deploys four fingerprinting techniques: audio, canvas, navigator, and WebGL. Combined with TrafficJunky (adult ad network) integration, the platform earned surveillance classification at 7/100.

LiveJasmin scores 0/100 with comprehensive fingerprinting (audio, canvas, navigator, WebGL), Hotjar session recording, Google/DoubleClick advertising, and TwinRed (adult ad network). The platform recorded 10,333 surveillance event listeners—the highest count in the entire audit. Every interaction is captured and exfiltrated.

Notable Findings

- **Commercial fingerprinting:** FingerprintJS detected on Chaturbate and Cam4
- **Adult ad networks:** CamSoda (TrafficJunky), LiveJasmin (TwinRed)
- **Session recording epidemic:** 7 of 8 platforms capture user sessions
- **Event listener extremes:** LiveJasmin (10,333), Chaturbate (5,381) vs. MyFreeCams (47)

2.5 Tube Sites

Category Average: 18/100 | Common Trackers: Google Analytics, TrafficJunky, TrafficStars

Tube sites—free video hosting platforms supported by advertising—represent the worst privacy practices in the adult industry. The category average of 18/100 reflects ubiquitous fingerprinting, aggressive ad networks, and comprehensive session recording.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
XVideos	43/100	C	Extensive
XNXX	43/100	C	Extensive
xHamster	30/100	D+	Extensive
Beeg	25/100	D+	Extensive
Pornhub	0/100	F	Surveillance
RedTube	0/100	F	Surveillance
SpankBang	0/100	F	Surveillance
YouPorn	0/100	F	Surveillance

XVideos and **XNXX** (owned by the same parent company) share identical tracking configurations: Google Analytics and TrafficJunky integration via CSP allowlisting. Session recording is active on both platforms. These are the "cleanest" tube sites—a low bar.

xHamster deploys Google Tag Manager, TrafficStars (adult ad network), and canvas fingerprinting. The platform registered 1,241 surveillance event listeners with comprehensive behavior monitoring.

Beeg uses Google Analytics, Yandex Metrika, and battery fingerprinting. The Russian analytics integration is concerning for users who prefer their adult browsing data not flow to Russian infrastructure.

Pornhub (the highest-traffic platform in this audit) scores 0/100 with:

- Google Analytics and Tag Manager
- Google Ads/DoubleClick integration
- TrafficJunky (MindGeek's own adult ad network)
- Full fingerprinting suite: audio, canvas, navigator, WebGL
- Session recording with 563 surveillance event listeners

Every visit to Pornhub is reported to Google's advertising network and TrafficJunky. The fingerprinting suite ensures visitors can be identified even with privacy tools active.

RedTube (also MindGeek/Aylo) mirrors Pornhub's configuration: same fingerprinting techniques, same ad networks, same surveillance apparatus. The 0/100 score reflects comprehensive tracking.

SpankBang deserves special attention for its advertising integration breadth:

- Meta (Facebook Pixel) — browsing data shared with Meta's advertising platform
- Google Ads/DoubleClick
- TikTok Pixel (ByteDance) — browsing data shared with Chinese tech giant
- Exoclick (adult ad network)
- TrafficStars (adult ad network)
- Microsoft Clarity (session recording)

SpankBang shares visitor data with Facebook, Google, TikTok, and two adult ad networks. The platform deployed 1,448 surveillance event listeners and 192 IntersectionObservers. Navigator fingerprinting ensures persistent identification.

YouPorn (MindGeek/Aylo) combines Google advertising, TrafficJunky, Exoclick, TwinRed, and comprehensive fingerprinting. Four distinct ad networks monetize visitor data while fingerprinting ensures tracking persistence.

Notable Findings

- **MindGeek/Aylo dominance:** Pornhub, RedTube, YouPorn share identical surveillance infrastructure
- **Multi-network advertising:** SpankBang shares data with 5+ ad networks (Meta, Google, TikTok, Exoclick, TrafficStars)
- **Social platform integration:** SpankBang reports visits to Meta and TikTok
- **Fingerprinting ubiquity:** 6 of 8 platforms deploy active fingerprinting
- **Zero privacy options:** Four platforms score 0/100

2.6 Major Studios

Category Average: 38/100 | Common Trackers: Google Analytics, Segment, Exoclick

Major studios—established production companies selling premium content—show moderate privacy practices. The category represents subscription-based businesses that should, in theory, need less advertising surveillance than free sites.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
Naughty America	66/100	B	Advertising
Reality Kings	44/100	C	Extensive
Kink	34/100	C-	Extensive
Playboy	31/100	D+	Extensive
Evil Angel	29/100	D+	Extensive
Brazzers	23/100	D	Surveillance

Naughty America leads the category with Google Analytics and limited behavior monitoring. No fingerprinting, no session recording, no third-party exfiltration. The platform uses New Relic for performance monitoring—a legitimate operations tool.

Reality Kings deploys navigator fingerprinting and session recording but avoids third-party advertising. The platform appears to use first-party surveillance rather than sharing data externally.

Kink combines Google advertising with canvas, navigator, and WebGL fingerprinting. The platform can identify visitors through graphics rendering characteristics and hardware specifications.

Playboy deploys the most complex analytics stack in the category:

- Google Analytics with DoubleClick
- Segment (customer data platform)
- PostHog (product analytics)
- Facebook Pixel (Meta advertising)

Playboy shares subscriber browsing data with both Google and Meta's advertising networks. The Segment integration suggests visitor data feeds into a customer data platform for cross-channel targeting.

Evil Angel uses Google advertising with canvas fingerprinting. The platform called `HTMLCanvasElement.toDataURL` 45 times during testing—far more than typical fingerprinting implementations, suggesting aggressive device identification.

Brazzers earns surveillance classification with Exoclick (adult ad network), navigator fingerprinting, and battery fingerprinting. The platform monitors battery status—an API designed for power management repurposed for tracking.

Notable Findings

- **Subscription vs. surveillance:** Subscription revenue should reduce advertising dependency, but 5 of 6 platforms still deploy advertising trackers
 - **Fingerprinting diversity:** Canvas (3 platforms), Navigator (4 platforms), Battery (1 platform), WebGL (2 platforms)
 - **Social integration:** Playboy shares data with Meta (Facebook)
 - **Adult ad networks:** Brazzers uses Exoclick
-

2.7 Clip Sites

Category Average: 45/100 | Common Trackers: Google Analytics

Clip sites—marketplaces where creators sell individual videos—show moderate privacy practices. With only two platforms in this category, the sample is limited but instructive.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
Clips4Sale	58/100	B-	Advertising
ManyVids	32/100	D+	Extensive

Clips4Sale deploys Google Analytics with DoubleClick advertising integration. Session recording is active, but the platform avoids fingerprinting. The advertising integration is standard rather than aggressive.

ManyVids uses canvas and WebGL fingerprinting alongside Google Analytics. The dual fingerprinting approach creates hardware-derived identifiers that persist through cookie clearing.

Notable Findings

- **Fingerprinting divergence:** ManyVids fingerprints; Clips4Sale does not
 - **Session recording:** Both platforms capture user sessions
 - **Google dependency:** Both platforms share data with Google
-

2.8 Arrangement & Dating

Category Average: 6/100 | Common Trackers: Google Analytics, LiveRamp, The Trade Desk

Arrangement and dating platforms—where users seek sugar dating or discrete encounters—show the worst privacy practices of any category. These platforms serve users with the highest discretion requirements and respond by deploying surveillance-grade tracking.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
Seeking	0/100	F	Surveillance
What's Your Price	11/100	D-	Surveillance

Both platforms in this category reach surveillance classification. The average score of 6/100 reflects comprehensive tracking, fingerprinting, and data broker integration.

Seeking (formerly Seeking Arrangement) deploys 21 tracking cookies—the highest count in the entire audit. The platform integrates with data brokers, meaning user profiles may be sold to third parties. Navigator fingerprinting, session recording, and keystroke logging are all active.

What's Your Price scores 11/100 with similar tracking infrastructure. Both platforms share data with Google's advertising network while also feeding data broker pipelines.

The Discretion Paradox

These findings represent the starkest disconnect between user expectations and platform behavior. Users seeking discrete arrangements—often married individuals, public figures, or people in sensitive professions—face the most aggressive tracking.

The data broker connections are particularly concerning. Seeking and What's Your Price are among only 2 platforms in the entire audit that connect to The Trade Desk, meaning user profiles may be sold to third parties. A user's presence on these platforms could potentially surface in data broker records.

Notable Findings

- **Data broker integration:** Both platforms connect to data broker infrastructure
- **Cookie extremes:** Seeking deploys 21 tracking cookies, 31 with >90 day lifetimes
- **Fingerprinting:** Both platforms deploy navigator fingerprinting
- **Session recording:** Both platforms capture complete user sessions
- **Keystroke logging:** Both platforms monitor search queries and form input

2.9 Social & Community

Category Average: 77/100 | Common Trackers: Google Analytics

Social and community platforms—where users build profiles and interact beyond transactions—show the best privacy practices of any category. The 77/100 average reflects minimal advertising integration and limited third-party tracking.

Platform Breakdown

Platform	Score	Grade	Data Sharing Level
FetLife	84/100	A-	Analytics Only
AdultFriendFinder	69/100	B	Advertising

FetLife earns the second-highest score in the entire audit (after Skip The Games). The kink-focused social network deploys minimal tracking—Google Analytics without advertising integration, no session recording, no fingerprinting. The platform demonstrates that community-supported adult services can respect user privacy.

AdultFriendFinder scores lower with advertising integration and keystroke logging. The platform shares data with Google's advertising network but avoids fingerprinting and session recording.

Notable Findings

- **Community model advantages:** User-supported platforms track less than ad-supported ones
- **Fingerprinting absence:** Neither platform deploys fingerprinting
- **FetLife as model:** Proves kink/adult social networking can work with privacy-respecting analytics

2.10 Case Studies

LoyalFans: Anatomy of a 0/100 Score

LoyalFans represents the worst privacy practices identified in this audit. The platform's score of 0/100 reflects comprehensive deployment of every major tracking technique.

Fingerprinting Arsenal:

- **Audio fingerprinting:** Creates unique identifier from AudioContext processing characteristics
- **Canvas fingerprinting:** Extracts device signature from 2D graphics rendering
- **WebGL fingerprinting:** Identifies GPU through 3D rendering parameters (UNMASKED calls: 4)
- **Navigator fingerprinting:** Collects device memory, hardware concurrency, platform, languages (89 platform checks)
- **Battery fingerprinting:** Monitors battery status API for device identification

Third-Party Sharing:

- Google Analytics (GA4 and Universal)
- Google Ads/DoubleClick (advertising network)
- X Corp (Twitter widgets, data sharing)
- Hotjar (session recording)

Behavior Surveillance:

- Session recording active (mouse, scroll, click, DOM mutation)
- Keystroke logging
- Form interaction monitoring
- Copy/paste monitoring
- 223 surveillance event listeners

Cookie Infrastructure:

- 13 total cookies
- 5 tracking cookies
- 4 with >90 day lifetimes

LoyalFans can identify visitors regardless of privacy tools. Incognito mode, cookie blocking, VPN usage—none prevent the fingerprinting arsenal from creating a stable identifier. The platform then shares this identifier with Google, X Corp, and Hotjar.

For creators choosing between platforms, LoyalFans' privacy practices should be disqualifying. The platform treats both creators and subscribers as advertising inventory to be tracked, profiled, and monetized.

Skip The Games: Privacy as Competitive Advantage

Skip The Games scores 90/100—the highest in the audit. The escort directory proves that privacy-respecting practices are compatible with running an adult platform.

What Skip The Games Does Right:

- **Cloudflare Analytics only:** No Google, no advertising networks, no session recording
- **No fingerprinting:** Visitors cannot be identified through hardware characteristics
- **Minimal cookies:** 1 cookie total, 0 classified as tracking
- **No third-party data sharing:** User behavior stays first-party

What Still Needs Improvement:

- Keystroke logging detected (for search functionality)
- 663 surveillance event listeners (high but first-party)
- Mouse movement tracking

Skip The Games demonstrates that the escort directory business model doesn't require surveillance capitalism. The platform monetizes through listing fees rather than advertising, eliminating the incentive to track users for ad targeting.

Pornhub: High Traffic, Zero Privacy

Pornhub represents the highest-traffic platform in this audit with an estimated 100+ million daily visits. The 0/100 score reflects privacy practices that scale to massive populations.

Scale of Surveillance: Every day, Pornhub's tracking infrastructure processes:

- ~100 million visitor fingerprints
- ~100 million Google Analytics events
- ~100 million TrafficJunky ad impressions
- Billions of page views reported to DoubleClick

MindGeek/Aylo Ecosystem: Pornhub is owned by Aylo (formerly MindGeek), which also operates RedTube, YouPorn, and TrafficJunky (the ad network). This vertical integration means:

- User data flows between properties via TrafficJunky
- Fingerprints enable cross-site tracking within the MindGeek portfolio
- A single corporate entity controls the world's largest adult video sites and the ad network that monetizes them

Technical Implementation:

- 4 fingerprinting techniques (audio, canvas, navigator, WebGL)
- Google Analytics with DoubleClick
- TrafficJunky (first-party ad network)
- 563 surveillance event listeners
- 22 cookies (8 tracking, 9 with >90 day lifetimes)

Pornhub's market position creates network effects for surveillance. As the dominant tube site, it sets industry practices that competitors follow. The platform's 0/100 score represents not just individual tracking but normalization of surveillance across the adult industry.

Summary

This chapter analyzed 38 platforms across eight categories, revealing systematic privacy failures in the adult industry:

- **12 platforms scored 0/100** (surveillance classification)
- **Average score: 37/100** across all platforms
- **29 platforms share data with Google**
- **33 platforms deploy fingerprinting**
- **29 platforms run session recording**

The data demonstrates clear patterns:

1. **Revenue model determines privacy:** Ad-supported platforms track aggressively; commission-based platforms track less
2. **User vulnerability inversely correlates with protection:** Arrangement/dating users need maximum discretion but face maximum surveillance
3. **Privacy is possible:** Skip The Games (90), FetLife (84), and OnlyFans (82) prove adult platforms can operate with privacy-respecting practices
4. **Fingerprinting is ubiquitous:** 33 of 38 platforms deploy techniques to identify visitors without cookies

The next chapter examines what users can do to protect themselves—and why most common countermeasures fall short against the fingerprinting and session recording documented here.

Chapter 3: The Limits of User Countermeasures

The natural response to learning about platform surveillance is to reach for protection. Most privacy-conscious users know the standard toolkit: VPNs, tracking blockers, private browsing, cookie deletion. These tools are valuable for many purposes—but they provide little defense against the fingerprinting and session recording techniques documented in this audit.

This chapter examines why common countermeasures fail and what actually works, with an honest assessment of the costs involved.

3.1 Why VPNs Don't Protect Against Fingerprinting

VPNs (Virtual Private Networks) are perhaps the most widely recommended privacy tool. They encrypt traffic and route it through an intermediary server, masking the user's true IP address from websites. For many threat models, this is valuable protection.

Against fingerprinting, however, VPNs provide no defense whatsoever.

The IP Address Is One Signal Among Dozens

A browser fingerprint is constructed from multiple independent data sources: canvas rendering, WebGL capabilities, audio processing characteristics, installed fonts, screen resolution, timezone, language settings, and more. The IP address is just one of these signals—and often not even the most distinctive one.

Consider this illustration:

Same User, Two Sessions	
Session A (No VPN)	Session B (VPN Active)
IP: 73.162.48.xxx (Home ISP)	IP: 185.94.192.xxx (VPN Exit Node)
Canvas Hash: 7f3a8b2c	Canvas Hash: 7f3a8b2c
WebGL Hash: 4e9d1a5f	WebGL Hash: 4e9d1a5f
Audio Hash: 2c8b3d7e	Audio Hash: 2c8b3d7e
Fonts: [147 fonts]	Fonts: [147 fonts]
Screen: 2560x1440	Screen: 2560x1440
Timezone: America/LA	Timezone: America/LA
Language: en-US	Language: en-US
Composite Hash: a9f7c3e2...	Composite Hash: a9f7c3e2...
▲ IDENTICAL ▲	
Result: Same user identified across both sessions	

The fingerprint remains identical regardless of VPN usage. A platform collecting fingerprints can link both sessions to the same browser, rendering the VPN's IP masking irrelevant for identification purposes.

Cross-Site Linking Persists

Because fingerprints are computed locally in the browser and remain stable across websites, a VPN does nothing to prevent cross-site tracking. If the same fingerprinting library runs on multiple platforms—as we found with many of the detected trackers—user activity can be correlated across sites even when visiting through different VPN servers.

VPNs protect the network layer. Fingerprinting operates at the application layer. They address entirely different threat surfaces.

3.2 Why Tracking Blockers Don't Block Fingerprinting

Browser extensions like uBlock Origin, Privacy Badger, and Ghostery are effective at blocking many tracking technologies. They maintain blocklists of known tracking domains and scripts, preventing them from loading. For traditional cookie-based tracking, this works well.

Fingerprinting evades these protections through several mechanisms.

First-Party vs. Third-Party Execution

Most tracking blockers focus on blocking third-party content—scripts loaded from domains other than the one you're visiting. This catches embedded analytics from google-analytics.com or advertising pixels from facebook.com.

Fingerprinting code, however, can run as first-party JavaScript. A platform can bundle fingerprinting libraries directly into their main application code, served from their own domain. No blocklist can identify this without analyzing the code's behavior, which would require far more sophisticated detection than simple domain blocking.

Our scan found fingerprinting techniques bundled into first-party code on 33 of 38 platforms (87%). The fingerprinting happened on the platform's own servers, not via third-party scripts that blockers could identify.

Browser APIs Are Legitimate

The techniques used for fingerprinting—Canvas, WebGL, Audio—are legitimate browser APIs with valid use cases. Blocking them entirely breaks functionality:

API	Fingerprinting Use	Legitimate Use	Blocking Impact
Canvas	Render hidden text, extract pixel data	Image editing, games, data visualization	Charts don't display, interactive content breaks
WebGL	Query GPU capabilities, render hidden scenes	3D graphics, games, maps	Google Maps breaks, video conferencing fails
AudioContext	Process audio through effects chain	Music players, video calls, audio editing	No sound on many sites
Font enumeration	Detect installed fonts	Document editing, design tools	Documents render in wrong fonts
Navigator properties	Collect browser/OS info	Feature detection, compatibility	Sites serve wrong content

Blocking these APIs would make the web largely unusable. Fingerprinting exploits this asymmetry—it uses ubiquitous, necessary functionality in ways that are invisible to users and difficult to distinguish from legitimate use.

Server-Side Proxying

Even when fingerprinting does involve external services, platforms can proxy data through their own servers. Instead of the browser connecting directly to a fingerprinting service (which a blocker might catch), the platform's own code collects the data and sends it to their backend, which then forwards it to whatever services it chooses.

From the blocker's perspective, this looks like normal first-party traffic. The user's data still reaches the fingerprinting service—just via an undetectable intermediary.

What Blockers Actually Stop vs. What They Don't

Protection	Traditional Blockers	Fingerprinting
Third-party analytics (Google Analytics, etc.)	Blocked when loaded from external domain	Often still collected via first-party code
Advertising pixels	Blocked	Fingerprints don't require pixels
Cookie-based tracking	Blocked or limited	Fingerprinting is cookieless by design
Cross-site tracking via third parties	Blocked	Persists through first-party fingerprints
Known fingerprinting domains	Blocked if on list	Bundled code evades lists
Session recording	Partially blocked	Often first-party, evades blocking

Blockers remain valuable for reducing the overall tracking surface, but they cannot prevent a determined platform from fingerprinting visitors.

3.3 Private Browsing Mode Ineffectiveness

Private browsing (Incognito in Chrome, Private Window in Firefox) is widely misunderstood. Its name suggests comprehensive privacy protection. In practice, it provides one specific guarantee: local data is not persisted after the session ends.

This means:

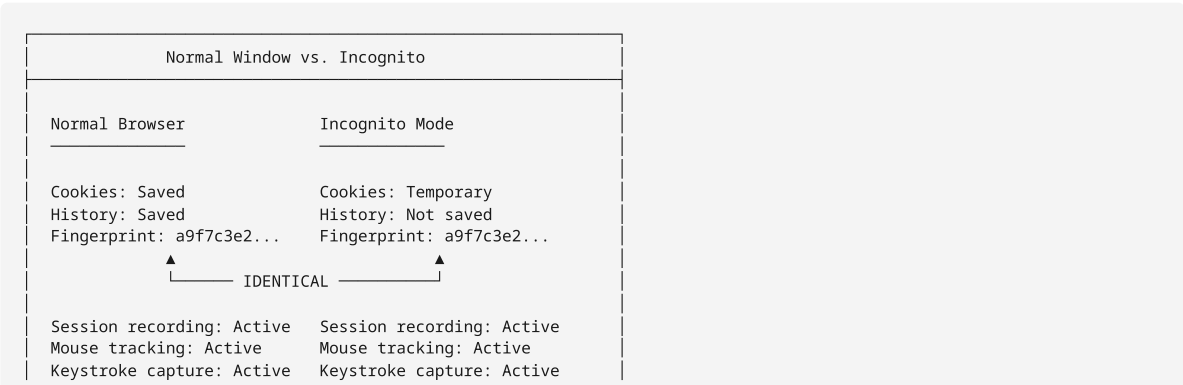
- Browsing history isn't saved
- Cookies are deleted when the window closes
- Form data and passwords aren't remembered
- Cache is cleared

What private browsing does not do:

- Mask your identity to websites you visit
- Prevent fingerprinting
- Block tracking scripts
- Encrypt your traffic
- Hide your IP address

Fingerprints Are Identical in Incognito

The browser's fingerprint is computed from its configuration and capabilities, not from stored data. Opening an incognito window doesn't change your GPU, your installed fonts, your screen resolution, or your browser version. The fingerprint remains identical.





Session Recording Captures Data in Real Time

Our audit found that 29 of 38 platforms (76%) employ likely session recording, capturing mouse movements, clicks, scrolls, and DOM changes. This data is transmitted to the platform's servers as you browse—not stored locally to be deleted later.

By the time you close that incognito window, the session recording is already complete and stored on remote servers. Private browsing's promise to "leave no trace" applies only to your local machine. The platform has already collected everything.

3.4 Cookie Deletion as Security Theater

Deleting cookies is perhaps the oldest privacy advice on the internet. It made sense when cookies were the primary tracking mechanism. In 2026, cookie deletion is largely security theater—an action that feels protective while providing minimal actual defense.

Cookies Are One Vector Among Many

Modern tracking operates through multiple redundant mechanisms:

Tracking Method	Blocked by Cookie Deletion?	Present in Audit
HTTP cookies	Yes	38/38 platforms
LocalStorage/SessionStorage	Sometimes (depends on clearing method)	Common
IndexedDB	Sometimes	Common
Browser fingerprinting	No	33/38 (87%)
Canvas fingerprinting	No	Widespread
WebGL fingerprinting	No	Widespread
Audio fingerprinting	No	Widespread
TLS session resumption	No	Standard practice
HTTP cache tracking	No	Common
HSTS supercookies	No	Possible

When a user deletes their cookies and returns to a platform, the fingerprint matches them to their previous profile. Their cookies may be gone, but their identity persists.

Fingerprinting Was Designed for Cookie-Free Tracking

The entire purpose of browser fingerprinting is to identify users who have deleted cookies, blocked cookies, or use private browsing. It was developed specifically to circumvent cookie-based privacy measures.

When we detected fingerprinting on 87% of audited platforms, we documented an industry-wide response to cookie deletion. These platforms anticipated users would try to protect themselves through cookies—and invested in tracking that works regardless.

What Each Countermeasure Actually Protects

Countermeasure	Protects Against	Does Not Protect Against
VPN	IP-based geolocation, ISP monitoring, network surveillance	Fingerprinting, session recording, keystroke capture
Tracking blocker	Third-party analytics, ad pixels, known tracking scripts	First-party fingerprinting, bundled trackers, server-side proxying
Private browsing	Local data persistence, shared computer exposure	Fingerprinting, real-time data collection, session recording
Cookie deletion	Cookie-based tracking (if done before visit)	Fingerprinting, localStorage, all non-cookie identification
Ad blocker	Display advertising, some tracking scripts	First-party data collection, fingerprinting

None of these tools address the core problem: the platform controls what code runs in your browser, and that code has access to identifying information that cannot be hidden without breaking the browser.

3.5 What Actually Works (And Its Costs)

Effective fingerprint resistance exists, but requires significant trade-offs that most users find unacceptable for daily browsing.

Tor Browser

The Tor Browser is specifically designed for fingerprint resistance. It standardizes the browser fingerprint across all users—everyone running Tor Browser looks identical to websites. It also routes traffic through the Tor network, providing genuine anonymity rather than just IP masking.

Costs:

- Significantly slower browsing (traffic routes through multiple relays)
- Many websites block or restrict Tor exit nodes
- CAPTCHAs are frequent and often unsolvable
- Some functionality (WebGL, some fonts) is disabled by default
- Not practical for sites requiring login (the fingerprint is designed for anonymous access)

For adult platforms specifically, Tor presents additional challenges: many implement aggressive anti-fraud measures that block or frustrate Tor users, and the login sessions these platforms require defeat much of Tor's anonymity benefit.

Fingerprint Randomization Extensions

Extensions like Canvas Blocker or Canvas Fingerprint Defender attempt to add random noise to fingerprinting APIs, generating a different fingerprint each time.

Costs:

- Detectable: the randomization itself becomes a signal (real browsers don't fluctuate)
- Sites can request multiple fingerprints in a session and detect inconsistency
- Breaks functionality on many sites
- Cat-and-mouse game with fingerprinting techniques

Many fingerprinting libraries specifically check for randomization extensions and can still link sessions even when randomization is active.

Dedicated Device or Browser Profile

Using a completely separate device or browser profile for sensitive browsing ensures that fingerprint cannot be linked to other activities.

Costs:

- Requires additional hardware or careful profile isolation
- Inconvenient for regular use
- The dedicated profile/device still builds a persistent fingerprint within its context
- Provides compartmentalization, not anonymity

Virtual Machines

Running browsers inside virtual machines can mask some hardware characteristics, though not all.

Costs:

- High technical barrier
- Resource-intensive
- VM detection is possible and common
- WebGL, audio, and some other fingerprinting vectors can still extract host characteristics
- Not practical for casual users

The Fundamental Asymmetry

All effective countermeasures share a common characteristic: they impose substantial costs on the user while requiring nothing from the platform. The burden of privacy protection falls entirely on individuals, who must sacrifice convenience, compatibility, and functionality.

This asymmetry is not accidental. Platforms have financial incentives to track users and no meaningful regulatory pressure to stop. Users who want privacy must fight the platform's code on every visit, forever.

The uncomfortable truth is that most users will not adopt these countermeasures consistently. The friction is too high, the benefits too abstract, and the immediate costs too concrete. Fingerprinting works precisely because it exploits the gap between what users theoretically could do and what they practically will do.

The tools described in this chapter remain valuable for their intended purposes. VPNs protect against network surveillance. Blockers reduce advertising exposure. Private browsing prevents local data leakage. Cookie deletion maintains some control over stored identifiers.

But for users specifically concerned about fingerprinting and session recording on adult platforms—the technologies documented throughout this audit—these countermeasures are inadequate. The platforms have already adapted to anticipate and circumvent them.

The next chapter examines the specific tracking technologies we detected, providing technical details about how each operates.

Chapter 4: Tracking Technologies Detected

The adult industry deploys a comprehensive arsenal of user tracking technologies. This chapter examines each category in detail, explaining how these technologies work, their prevalence across the 38 platforms we analyzed, and their specific implications for user privacy.

4.1 Analytics and Tag Managers

Analytics platforms form the foundation of user tracking on adult websites. While these tools ostensibly serve legitimate business purposes, they create detailed profiles of user behavior that can be repurposed for advertising or shared with third parties.

Google Analytics (GA4 and Universal)

Google Analytics dominates the adult industry just as it dominates the broader web. We detected Google Analytics on **29 of 38 platforms (76%)**, making it the most prevalent tracker in this audit.

Google Analytics works by loading a JavaScript snippet that records every page view, scroll event, click, and user interaction. This data flows to Google's servers, where it becomes part of the user's broader profile that Google maintains across all websites using their services.

Key concern for adult platform users: Google's cross-site tracking means that your browsing on adult websites contributes to the same profile Google uses for Gmail, YouTube, and Search. While Google claims to anonymize this data, the detailed behavioral patterns can still be used for advertising targeting and may be accessible to Google employees or subpoenaed by law enforcement.

The platforms using Google Analytics include household names like OnlyFans, Pornhub, Chaturbate, and Seeking. Even platforms positioned as privacy-conscious, such as creator platforms competing with OnlyFans, frequently deploy Google's tracking infrastructure.

Google Tag Manager

Google Tag Manager (GTM) appeared on **24 platforms (63%)**. GTM serves as a container that loads and orchestrates multiple tracking scripts, making it a force multiplier for surveillance. A single GTM container can deploy dozens of additional trackers without requiring code changes to the website.

The presence of GTM often indicates a more sophisticated tracking setup. Platforms using GTM typically load multiple advertising pixels, analytics tools, and remarketing scripts through this single entry point.

Other Analytics Platforms

Beyond Google, we detected several additional analytics services:

Analytics Platform	Platforms	Privacy Impact
Cloudflare Web Analytics	11	Low (aggregate data, no cookies)
Hotjar	4	High (session recording, heatmaps)
New Relic	4	Low (performance monitoring)
Amplitude	2	Medium (product analytics)
PostHog	2	Medium (product analytics with session recording)
Yandex Metrica	2	High (Russian data collection)
Microsoft Clarity	1	High (session recording)
Segment	1	High (customer data platform)

Yandex Metrica detection on ListCrawler and Beeg is particularly concerning. Yandex is a Russian company subject to Russian data access laws, meaning user browsing data from these platforms is potentially accessible to Russian government agencies.

Hotjar was detected on 4 platforms including LoyalFans, Chaturbate, and LiveJasmin. Hotjar provides session recording capabilities that capture every mouse movement, click, and scroll, as discussed in Section 4.4.

4.2 Advertising Networks

Advertising trackers are more invasive than analytics because they share user data with third-party networks that aggregate browsing behavior across thousands of websites.

Google Ads / DoubleClick

Google's advertising network appeared on **22 of 38 platforms (58%)**. When detected, this indicates the platform is sharing visitor data with Google's advertising ecosystem, which reaches virtually every corner of the internet.

DoubleClick cookies enable cross-site tracking that builds detailed profiles of users' browsing habits. When someone visits an adult site with Google Ads integration and later browses mainstream websites, the advertising network can connect these activities. While Google has policies against using sensitive categories for ad targeting, the data collection itself occurs regardless of policy.

Platforms with Google Ads integration include Pornhub, Seeking, SpankBang, and multiple cam sites. The business rationale is clear: Google Ads provides sophisticated audience targeting and attribution tracking that helps platforms optimize their marketing spend. The privacy cost is that user visits become part of Google's advertising graph.

Meta / Facebook Pixel

Facebook Pixel was detected on **3 platforms**: SpankBang, Playboy, and Seeking. This is notable because Meta's advertising policies officially prohibit adult content, yet these platforms still share visitor data with Meta's advertising network.

When present, Facebook Pixel reports every page visit to Meta, including the URL visited. For Seeking users, this means their visits to an "arrangement" dating site are reported to Facebook's servers, potentially enriching their social graph data even if the user never connects Seeking to their Facebook account.

The implications are significant: Meta maintains one of the world's most comprehensive social graphs, connecting real identities to online behavior. A Seeking user who also uses Facebook provides Meta with the ability to link their dating site activity to their real identity, employment, and social connections.

Twitter/X Pixel

Twitter's advertising pixel appeared on **Fansly**, the creator platform that positions itself as a direct OnlyFans competitor. This integration enables Twitter/X to track which users visit Fansly and build audience segments for advertising.

Adult-Specific Advertising Networks

Adult advertising networks are particularly invasive because they operate exclusively within the adult content ecosystem, building comprehensive profiles of users' intimate browsing habits across multiple adult sites.

Network	Platforms	Description
TrafficJunky	6	Pornhub owner MindGeek's ad network
Exoclick	3	Major adult ad exchange
TrafficStars	2	Adult programmatic ads
TwinRed	2	Formerly DoublePimp

TrafficJunky is owned by Aylo (formerly MindGeek), the parent company of Pornhub, RedTube, and YouPorn. Its presence on 6 platforms means users' browsing across these sites is tracked by a single network. TrafficJunky explicitly specializes in adult content advertising, meaning it builds profiles specifically around intimate content preferences.

Exoclick operates one of the largest adult advertising exchanges, serving ads across thousands of adult websites. Detection on Brazzers, YouPorn, and SpankBang indicates cross-site tracking within this network.

These adult-specific networks pose unique risks: while Google might not explicitly use adult browsing for targeting (per their policies), adult advertising networks have no such restrictions. They exist specifically to monetize detailed profiles of adult content consumption.

4.3 Fingerprinting Techniques

Browser fingerprinting identifies users without cookies by analyzing unique characteristics of their browser, hardware, and software configuration. This technique can track users even in private browsing mode or after clearing cookies.

We detected active fingerprinting on **33 of 38 platforms (87%)**. See Appendix B.2 for the complete list.

Canvas Fingerprinting

Canvas fingerprinting exploits the HTML5 Canvas API to create unique identifiers. When a script draws text or graphics to an invisible canvas element and reads back the pixel data, subtle differences in rendering create a unique signature based on the user's graphics hardware, drivers, and browser configuration.

Detected on 11 platforms: LoyalFans, CamSoda, LiveJasmin, Pornhub, xHamster, RedTube, YouPorn, Kink, Evil Angel, ManyVids, and FetLife.

The technique is particularly insidious because it requires no permission, leaves no trace, and works across incognito sessions. A user who carefully clears cookies before visiting an adult site can still be identified via their canvas fingerprint.

WebGL Fingerprinting

WebGL fingerprinting queries the graphics card for detailed information including the GPU vendor, model, and renderer strings. Combined with supported extensions and performance characteristics, this creates a hardware fingerprint.

Detected on 9 platforms: LoyalFans, Stripchat, CamSoda, LiveJasmin, Pornhub, RedTube, YouPorn, Kink, and ManyVids.

WebGL fingerprinting is particularly effective because graphics hardware varies significantly between users and changes infrequently. A user's GPU configuration often remains stable for years, providing a persistent identifier.

Audio Fingerprinting

Audio fingerprinting uses the Web Audio API to create unique identifiers based on how a device processes sound. By generating audio signals and analyzing the output, scripts can identify subtle differences in audio hardware and software configuration.

Detected on 6 platforms: LoyalFans, CamSoda, LiveJasmin, Pornhub, RedTube, and YouPorn.

The audio fingerprint can persist across browsers on the same device and is difficult to spoof without specialized tools.

Navigator Fingerprinting

Navigator fingerprinting collects browser and system properties including:

- `navigator.languages` (language preferences)
- `navigator.platform` (operating system)
- `navigator.hardwareConcurrency` (CPU core count)
- `navigator.deviceMemory` (RAM amount)

Detected on 12 platforms, making it the most common fingerprinting technique.

While individual navigator properties have low entropy, combining them with other signals creates effective fingerprints. A user with an unusual language configuration, specific CPU core count, and particular RAM amount becomes highly identifiable.

Battery Fingerprinting

Battery fingerprinting exploits the Battery Status API to query charging status, battery level, and time estimates. While deprecated in most browsers due to privacy concerns, some platforms still attempt these calls.

Detected on 4 platforms: ListCrawler, LoyalFans, Beeg, and Brazzers.

The Battery API was specifically deprecated because researchers demonstrated that precise battery level readings (to two decimal places) combined with charging time estimates created effective short-term fingerprints.

FingerprintJS (Commercial Library)

FingerprintJS is a commercial fingerprinting service that combines multiple techniques into a single product. Its detection indicates intentional, sophisticated fingerprinting rather than incidental API usage.

Detected on 3 platforms: Chaturbate, Cam4, and AdultFriendFinder.

FingerprintJS claims 99.5% accuracy in identifying returning visitors without cookies. Its presence indicates these platforms have made a deliberate investment in tracking users who attempt to browse anonymously.

Fingerprinting Techniques by Platform

Platform	Canvas	WebGL	Audio	Navigator	Battery	FingerprintJS
LoyalFans	Yes	Yes	Yes	Yes	Yes	-
CamSoda	Yes	Yes	Yes	Yes	-	-
LiveJasmin	Yes	Yes	Yes	Yes	-	-
Pornhub	Yes	Yes	Yes	Yes	-	-
RedTube	Yes	Yes	Yes	Yes	-	-
YouPorn	Yes	Yes	Yes	Yes	-	-
Kink	Yes	Yes	-	Yes	-	-
ManyVids	Yes	Yes	-	-	-	-
Chaturbate	-	-	-	-	-	Yes
Cam4	-	-	-	-	-	Yes
AdultFriendFinder	-	-	-	-	-	Yes
ListCrawler	-	-	-	-	Yes	-
Beeg	-	-	-	-	Yes	-
Brazzers	-	-	-	Yes	Yes	-

LoyalFans stands out as the most aggressive fingerprinter, deploying 5 different fingerprinting techniques simultaneously. This platform, which scored 0/100 in our audit, uses every major fingerprinting method to ensure users cannot browse anonymously.

4.4 Session Recording

Session recording captures complete replays of user interactions including mouse movements, clicks, scrolls, keystrokes, and DOM changes. Third-party services receive this data, creating video-like recordings of each user session.

We detected likely session recording on 29 of 38 platforms (76%).

Session recording is identified through a combination of signals:

- High-frequency mouse movement event listeners
- Scroll position tracking
- Click tracking
- DOM mutation observers (detecting page changes)
- Third-party data exfiltration

Services Detected

Service	Platforms	Data Collected
Hotjar	4	Full session recordings, heatmaps
PostHog	2	Session recordings, product analytics
Microsoft Clarity	1	Session recordings, AI insights
Custom/Unknown	22+	Variable

Privacy Implications for Adult Content

Session recording on adult platforms is exceptionally invasive. Consider what these recordings capture:

1. **Search queries:** Users searching for specific content types have their queries recorded and sent to third parties.
2. **Navigation patterns:** The sequence of pages visited reveals content preferences in granular detail.
3. **Interaction timing:** How long users spend on each page, where they pause, what catches their attention.
4. **Form inputs:** Profile descriptions, messages to other users, payment details (potentially masked, but not guaranteed).

The 29 platforms with likely session recording include Pornhub, LiveJasmin, Seeking, and most major cam sites. Users of these platforms should assume their entire browsing session is being recorded and stored on third-party servers.

4.5 Keystroke Monitoring

Keystroke monitoring captures individual key presses as users type. While some keystroke tracking serves legitimate purposes (e.g., real-time search suggestions), the practice captures sensitive information before users explicitly submit it.

Keystroke monitoring detected on 34 of 38 platforms (89%).

The near-universal prevalence of keystroke monitoring reflects modern web development practices, where many frameworks automatically capture input events. However, the privacy implications are significant:

What Keystroke Monitoring Captures

1. **Incomplete searches:** Users who start typing a search query but change their mind still have their partial input recorded.
2. **Draft messages:** Private messages being composed are captured character by character, even if never sent.
3. **Form abandonment:** Users who begin filling out registration or profile forms but abandon them still have their partial inputs captured.
4. **Typos and corrections:** The full sequence of keystrokes, including deletions and corrections, is captured.

Context in Adult Platforms

On adult platforms, keystroke monitoring can capture:

- Search queries for specific content categories
- Private messages to creators or other users
- Profile descriptions and personal information
- Payment details during checkout

The platforms monitoring keystrokes include Pornhub, OnlyFans, Seeking, Chaturbate, and essentially every major platform. Combined with session recording, this creates comprehensive documentation of user intent, even for actions never completed.

4.6 Cookie Analysis

Cookies remain a fundamental tracking mechanism despite browser restrictions. Our analysis classified cookies by purpose and examined tracking patterns across all platforms.

Cookie Statistics

Platform	Total Cookies	Tracking	Session	Long-lived (>90 days)
Seeking	37+	21	10+	31
SpankBang	31	13	4	19
ListCrawler	24	14	7	13
Beeg	22	15	5	14
Pornhub	22	8	3	9
LiveJasmin	22	9	8	9
What's Your Price	20+	15	-	11

Seeking deploys the most aggressive cookie tracking in our audit, with 21 cookies classified as tracking cookies and 31 cookies with lifetimes exceeding 90 days. Some of these cookies persist for over a year, maintaining user identification across extended periods.

Third-Party Cookies

Third-party cookies set by domains other than the visited site enable cross-site tracking. Despite browser restrictions, we detected third-party cookies on multiple platforms:

- **Beeg:** 17 third-party cookies
- **ListCrawler:** 17 third-party cookies
- **SpankBang:** 15 third-party cookies
- **Fansly:** 6 third-party cookies
- **LiveJasmin:** 3 third-party cookies

These third-party cookies often connect to advertising networks, enabling cross-site user identification even without fingerprinting.

Long-Lived Cookies

Cookies with lifetimes exceeding 90 days pose particular privacy risks because they persist across clearing browser data (if users don't clear cookies specifically) and can survive for months or years.

Seeking leads with 31 long-lived cookies, some set to expire in 2028. This means users who visited Seeking in early 2026 carry identification cookies that could persist for years.

4.7 Data Broker Connections

Data brokers aggregate user information from multiple sources and sell it to advertisers, employers, and other parties. Detection of data broker connections indicates user profiles may enter secondary markets.

We detected data broker connections on 2 of 38 platforms: Seeking and What's Your Price.

The Trade Desk

Both platforms connect to **The Trade Desk**, a major programmatic advertising platform and data broker. The Trade Desk operates a Unified ID system that creates persistent identifiers across devices and platforms.

Detection evidence on Seeking included:

- Scripts from `js.adsrvr.org` (The Trade Desk domain)
- Tracking pixels to `insight.adsrvr.org`
- Cookie sync requests to `match.adsrvr.org`
- Cross-platform matching with Rubicon, AppNexus, and Google

What Data Brokers Do With This Data

When The Trade Desk receives data from Seeking or What's Your Price, it can:

1. **Cross-reference with other data:** Match users against data from other sources, potentially connecting adult platform usage to real identity.
2. **Build audience segments:** Create targetable segments such as "sugar dating users" that advertisers can purchase.
3. **Enable retargeting:** Allow advertisers to target users who have visited these platforms across other websites.
4. **Sell to third parties:** Provide aggregated or individualized data to other companies, including data aggregators, background check services, or research firms.

Secondary Market Implications

The presence of data broker connections on dating arrangement platforms is particularly concerning because:

1. **Real identity correlation:** Unlike anonymous tube site viewing, Seeking and What's Your Price require account creation with personal details.
2. **Relationship data:** These platforms involve real interpersonal connections that users expect to remain private.
3. **Reputation risk:** Data about sugar dating activity could be damaging if exposed through data breaches or resale.
4. **Legal exposure:** Depending on jurisdiction, activities facilitated by these platforms may carry legal risk, making data exposure potentially harmful.

The combination of extensive tracking (21 tracking cookies on Seeking) with data broker integration creates a comprehensive surveillance system that extends far beyond the platform itself.

Summary

The tracking technologies deployed across adult platforms reveal a pervasive surveillance infrastructure:

- **76% deploy Google Analytics** (29/38), feeding user behavior into Google's advertising ecosystem
- **58% use Google Ads/DoubleClick** (22/38), directly sharing data with advertising networks
- **87% employ browser fingerprinting** (33/38), tracking users even without cookies
- **76% have likely session recording** (29/38), capturing complete interaction replays
- **89% monitor keystrokes** (34/38), capturing searches and messages as users type
- **2 platforms connect to data brokers**, enabling secondary market data sales

See Appendix B for complete calculations and platform lists.

For users seeking privacy on adult platforms, these findings suggest that conventional privacy measures (clearing cookies, using incognito mode) provide limited protection against the tracking technologies in widespread deployment.

Chapter 5: Methodology

This chapter describes the technical methodology used to conduct the privacy audit documented in this report. We provide this level of detail to enable reproducibility, support informed interpretation of results, and acknowledge the inherent limitations of automated privacy analysis.

5.1 Platform Selection Criteria

The audit examined 38 platforms across 8 distinct categories within the adult industry ecosystem:

Category	Platform Count	Examples
Escort Directories	7	Eros, Tryst, Slix, Skip The Games
Creator Platforms	3	OnlyFans, Fansly, LoyalFans
Cam Sites	8	Chaturbate, Stripchat, LiveJasmin, MyFreeCams
Tube Sites	8	Pornhub, XVideos, xHamster, XNXX
Major Studios	6	Brazzers, Kink, Playboy, Reality Kings
Clip Sites	2	ManyVids, Clips4Sale
Arrangement Dating	2	Seeking, What's Your Price
Social Community	2	FetLife, AdultFriendFinder

Selection Methodology:

Platform selection followed three primary criteria:

- Traffic Volume:** We prioritized platforms with significant monthly visitor counts as reported by Semrush traffic analytics (December 2025 data). The included platforms range from 200,000 to 3.85 billion monthly visits, collectively representing the majority of adult industry web traffic.
- Category Coverage:** We ensured representation across all major business models within the adult industry. This includes advertising-supported free platforms (tube sites), subscription-based creator platforms, service directories, and community sites. Each category exhibits distinct privacy characteristics based on its revenue model.
- Geographic Relevance:** While prioritizing platforms with global reach, we included regionally significant platforms to capture geographic variation in privacy practices. The selection includes US-focused directories, European cam sites, and platforms with significant international audiences.

5.2 Scanning Infrastructure

The scanner employs a two-phase analysis architecture designed to capture both static and dynamic privacy indicators.

Phase 1: Static HTML Analysis

The static analyzer fetches each platform's homepage using standard HTTP requests with a contemporary browser user-agent string (Chrome 131 on Windows 10). This phase extracts:

- HTTP Response Headers:** Set-Cookie directives, Content-Security-Policy rules, Referrer-Policy, Permissions-Policy, Strict-Transport-Security, and X-Frame-Options headers
- External Scripts:** All third-party JavaScript sources loaded via `<script src=...` tags, with domain extraction and async/defer attribute detection
- Tracking Pixels:** Hidden or 1x1 pixel images from third-party domains, commonly used for cross-site tracking

- **Third-Party Iframes:** Embedded frames loading content from external domains, including hidden iframes used for cookie syncing
- **Prefetch Hints:** `<link rel="prefetch">`, `<link rel="preconnect">`, and `<link rel="dns-prefetch">` tags that reveal anticipated third-party connections
- **Inline Script Content:** JavaScript code embedded directly in HTML, analyzed for tracker initialization patterns
- **Meta Tags:** Privacy-relevant metadata including Open Graph tags that may leak information

Static analysis provides a baseline view of tracking infrastructure present in the initial page load, independent of JavaScript execution.

Phase 2: Dynamic Browser Automation

For comprehensive analysis, we employ Playwright with Chromium to execute pages in a realistic browser environment. The dynamic analyzer:

1. **Launches Headless Chromium:** Each scan spawns an isolated browser instance with standard viewport (1920x1080), US-East timezone, and English locale settings.
2. **Injects Monitoring Scripts:** Before any page scripts execute, we inject JavaScript that intercepts fingerprinting-related API calls and event listener registrations. This instrumentation preserves original functionality while recording usage.
3. **Captures Network Traffic:** All HTTP/HTTPS requests are logged with domain, resource type, and request method. Third-party requests are identified by comparing request domains against the page's root domain.
4. **Simulates User Behavior:** After initial page load, the scanner scrolls to mid-page and bottom positions to trigger lazy-loaded trackers and scroll-tracking analytics.
5. **Collects Runtime State:** After a stabilization period, we extract all cookies (including those set via JavaScript), WebSocket connections, and dynamically injected script tags.

Concurrency is calculated dynamically based on available system memory, with each Chromium instance allocated approximately 512MB. A maximum of 12 parallel browsers prevents system overload while maintaining reasonable scan throughput.

5.3 Detection Heuristics

Tracker Signature Matching

The scanner maintains a signature database of 80+ known tracking technologies across eight categories:

- **Analytics:** Google Analytics, Hotjar, Mixpanel, Amplitude, FullStory, Microsoft Clarity, and others
- **Advertising:** Facebook Pixel, Google Ads/DoubleClick, TikTok Pixel, Criteo, adult-specific networks (Exoclick, TrafficJunky, TrafficFactory)
- **Fingerprinting:** FingerprintJS, canvas fingerprinting patterns, WebGL and AudioContext fingerprinting
- **Data Brokers:** Oracle BlueKai, LiveRamp, Lotame, Acxiom, The Trade Desk
- **Social:** Facebook SDK, Twitter widgets, LinkedIn Insight, Pinterest Tag
- **Consent Management:** OneTrust, Cookiebot, TrustArc
- **Experimentation:** Optimizely, VWO, LaunchDarkly, AB Tasty
- **Customer Data Platforms:** Segment, mParticle, Tealium, Braze

Each signature specifies:

- Regular expressions matching script URLs and inline code patterns
- Cookie name patterns characteristic of the tracker
- Network request URL patterns
- Known domains associated with the tracking vendor

Detection confidence weights vary by evidence type: fingerprinting API calls (0.97), script matches (0.95), tracking pixels (0.92), cookies (0.90), network requests (0.85), iframe matches (0.90), CSP domain allowlisting (0.60), and prefetch hints (0.55).

Fingerprinting Detection

Browser fingerprinting is detected through API interception, monitoring calls to:

- **Canvas API:** `toDataURL()`, `toBlob()`, `getImageData()` on canvas elements
- **WebGL API:** `getParameter()` with `UNMASKED_RENDERER_WEBGL` and `UNMASKED_VENDOR_WEBGL` constants
- **AudioContext API:** `createOscillator()` and `OfflineAudioContext.startRendering()`
- **Battery API:** `navigator.getBattery()`
- **Navigator Properties:** `hardwareConcurrency`, `deviceMemory`, `platform`, `languages`

For navigator properties specifically, isolated access is not flagged as fingerprinting since these properties have legitimate uses in internationalization, responsive design, and feature detection. Only systematic enumeration (3+ distinct properties accessed) triggers a fingerprinting detection.

Session Recording Detection

Session recording tools capture user interactions for playback. We detect likely session recording through behavioral pattern analysis:

1. **Event Listener Enumeration:** We monitor `addEventListener` calls for surveillance-type events (scroll, mousemove, click, keydown, input, visibilitychange, etc.)
2. **Third-Party Origin Heuristic:** Event listeners are flagged as tracking-related only when stack trace analysis indicates registration by third-party scripts. First-party event handlers are normal web development.
3. **MutationObserver Counting:** Session recorders use MutationObservers to capture DOM changes. While modern frameworks (React, Vue) also use MutationObservers for rendering, their presence combined with third-party behavioral tracking increases session recording likelihood.
4. **Combined Pattern Detection:** Session recording is flagged as "likely" when we observe:
 - Scroll AND mouse movement tracking
 - Multiple MutationObservers (2+)
 - Third-party exfiltration of click events
 - OR combined scroll, mouse, click, AND keystroke tracking with third-party involvement

Cookie Classification

All cookies are classified by purpose using multiple signals:

- **Known Tracking Patterns:** Cookie names matching patterns like `_ga`, `_fbp`, `_hj*`, `mp_*`, `ajs_*`
- **Value Structure Analysis:** UUIDs, long hex strings, GA-style numeric identifiers, and base64-ish tokens indicate tracking IDs
- **Lifetime Analysis:** Long-lived cookies (>7 days) containing tracking ID patterns are classified as tracking
- **Third-Party Domain:** Cookies from domains outside the platform's root domain with lifetimes >1 day are presumed tracking
- **Session Cookies:** Short-lived or session-only cookies with names like `session`, `sid`, `csrftoken`
- **Functional Cookies:** Preference cookies (`lang`, `theme`, `consent`, `timezone`)

5.4 Scoring Framework

The privacy score ranges from 0 to 100, where higher values indicate better privacy practices.

Base Score and Deductions

Each platform begins with a score of 100. Deductions are applied based on detected tracking technologies:

Category	Base Points	Severity Multipliers
Data Brokers	15	Low: 0.4x, Medium: 0.7x, High: 1.0x, Critical: 1.3x
Fingerprinting	12	Same severity scale
Advertising	8	Same severity scale
Customer Data Platforms	6	Same severity scale
Social	5	Same severity scale
Analytics	3	Same severity scale
Experimentation	2	Same severity scale
Consent Management	0	(Presence provides small bonus)

Diminishing Returns: When multiple trackers exist in a single category, subsequent trackers are weighted at $1/(1 + 0.5*(\text{rank}-1))$. This prevents runaway deductions while still penalizing tracker accumulation. The first tracker in a category receives full weight; the second receives 67%; the third, 50%; and so on.

Google Analytics Consolidation: GA4, Universal Analytics, and Google Tag Manager are treated as a single analytics deployment when co-present, reflecting their typical combined usage.

Behavioral Tracking Deductions

Signal	Deduction
Session recording likely	-15
Keystroke tracking (third-party)	-8
Combined mouse + scroll tracking (third-party)	-5
Form tracking (third-party)	-4
Copy/paste tracking	-3
Third-party event listeners (scaled)	Up to -5

Cookie Tracking Deductions

Cookie-based deductions scale continuously:

- Third-party cookies: 0.5 points per cookie (capped at 15 cookies)
- Tracking-classified cookies: 0.4 points per cookie (capped at 15 cookies)
- Long-lived cookies (>90 days): 0.3 points per cookie (capped at 15 cookies)

Positive Signals (Bonus Points)

Platforms with pre-bonus scores of 70 or higher may receive up to 5 bonus points for privacy-protective measures:

- Strict Referrer-Policy (no-referrer, same-origin, strict-origin, strict-origin-when-cross-origin): +2
- Permissions-Policy header present: +2
- Consent management platform detected: +2
- HSTS (Strict-Transport-Security) header: +1

The conditional threshold prevents gaming: a platform cannot offset aggressive tracking by simply deploying privacy headers.

Data Sharing Level Classification

Based on the final score and tracker profile, platforms are assigned a data sharing level:

Level	Criteria
None	Zero trackers detected
Analytics Only	Analytics present but no advertising, data brokers, or fingerprinting
Advertising	Ad networks present but score ≥ 50
Extensive	Score between 25-49 with significant tracking
Surveillance	Score below 25, indicating pervasive tracking infrastructure

Letter Grades

Scores map to letter grades following a similar curve to Mozilla Observatory:

- A+: 95-100
- A: 85-94
- A-: 78-84
- B+: 70-77
- B: 62-69
- B-: 55-61
- C+: 48-54
- C: 40-47
- C-: 33-39
- D+: 25-32
- D: 18-24
- D-: 10-17
- F: 0-9

5.5 Limitations and Caveats

We acknowledge several limitations inherent to this methodology:

Temporal Snapshot

This audit represents a point-in-time analysis conducted in January 2026. Tracking infrastructure changes frequently as platforms add, remove, or modify analytics and advertising integrations. Results should be considered indicative of practices at the time of scanning rather than permanent characteristics.

Logged-Out Homepages Only

Scans analyze only the logged-out homepage experience. Authenticated user experiences may differ substantially:

- Additional tracking may activate after login
- Personalization systems may deploy heavier fingerprinting
- Payment flows may introduce additional third-party integrations
- Some platforms may actually reduce tracking for logged-in users

A complete privacy assessment would require authenticated analysis, which raises ethical and legal considerations beyond this study's scope.

Heuristic Detection

All detection is heuristic. We acknowledge potential for:

- **False Positives:** A script matching a tracking pattern may serve a different purpose. Navigator property access for legitimate feature detection could be misclassified. MutationObservers in framework code may inflate session recording indicators.
- **False Negatives:** Obfuscated trackers, self-hosted analytics, or novel tracking techniques may evade signature matching. First-party data collection systems are not fully captured. Server-side tracking is invisible to client-side analysis.

We tuned heuristics to minimize false positives (avoiding unfair penalization) while accepting some false negatives (underestimating rather than overestimating tracking).

Geographic Variation

Scans were conducted from an Iceland/EU vantage point. Platforms may serve different tracking configurations based on visitor geography:

- GDPR compliance measures may reduce tracking for EU visitors
- US visitors may experience heavier advertising and data broker integration
- Regional ad networks may not appear in EU-origin scans
- Geo-targeted consent dialogs may alter cookie behavior

Results most accurately represent the EU visitor experience.

Dynamic Content Variation

Some platforms serve different content or tracking payloads based on:

- Time of day or day of week
- Visitor device characteristics
- A/B testing segments
- CDN edge caching behavior
- Rotating ad inventory

While we scroll and wait for lazy-loaded content, inherent variation means repeat scans might detect slightly different tracker sets.

Scanner Detectability

Sophisticated platforms may detect automated scanning through:

- Headless browser fingerprints
- Unrealistic navigation patterns (no clicks, direct scroll)
- Missing JavaScript execution characteristics
- IP-based rate limiting

Some platforms may serve clean pages to suspected bots while deploying full tracking to human visitors. Our use of standard Chromium with realistic user-agent and viewport attempts to minimize this, but detection cannot be ruled out.

These limitations contextualize rather than invalidate our findings. The methodology provides a consistent, reproducible baseline for comparing privacy practices across the adult industry ecosystem. Platforms with significantly worse scores than peers face the same detection limitations, making relative comparisons meaningful even where absolute measurement is imperfect.

Complete platform data, calculations, and source references are provided in Appendix B.

Chapter 6: Discussion

The findings presented in this audit reveal a troubling landscape where adult platform users are subjected to surveillance technologies comparable to the most aggressive tracking found anywhere on the web. This chapter examines the implications of these findings for users, platform operators, regulators, and researchers.

6.1 Implications for Users

The Myth of Anonymous Browsing

The most significant finding of this audit is that users cannot assume privacy on adult platforms. The pervasive deployment of browser fingerprinting (detected on 87% of platforms) means that standard privacy measures are insufficient. Incognito mode, clearing cookies, and basic browser privacy settings provide a false sense of security when platforms can identify returning visitors through hardware characteristics, browser configurations, and rendering behaviors.

Consider a user who believes they are browsing privately: they open an incognito window, perhaps use a VPN, and visit an adult platform. From their perspective, they have taken reasonable precautions. From the platform's perspective, they have been assigned a fingerprint identifier that persists across sessions, correlated with their browsing history on that site, and potentially linked to an advertising profile that spans thousands of websites through Google's ad network.

The 76% session recording rate compounds this issue. Tools like Hotjar, Microsoft Clarity, and similar services capture every mouse movement, click, scroll, and DOM interaction. A user hesitating over a particular category, starting to type a search query and then deleting it, hovering over content before navigating away - all of this behavioral data is captured and stored. For content involving sexual preferences, relationship status, or intimate interests, this level of surveillance is profoundly invasive.

Who Faces the Highest Stakes?

Not all users face equal risks from this surveillance. Several populations are particularly vulnerable:

Sex workers use these platforms both personally and professionally. Escort directories, cam sites, and creator platforms are essential business infrastructure. When these platforms share data with Google and Meta's advertising networks, they create linkages between professional identities and personal browsing that could expose workers to discrimination, harassment, or legal jeopardy depending on jurisdiction.

LGBTQ+ individuals, particularly those who are closeted, face risks when platforms share data with advertising ecosystems. A fingerprint tied to browsing history on gay adult content, flowing through ad networks to data brokers, could potentially be correlated with real-world identity. In jurisdictions where homosexuality is criminalized, this data trail could be life-threatening.

Individuals in abusive relationships may browse content related to sexuality, dating, or relationship advice that could trigger violence if discovered. Session recordings capturing every hesitation and search query create evidence that abusers could potentially access through device compromise or legal discovery.

People in restrictive jurisdictions face legal consequences for accessing content that is legal in other countries. The data broker connections we detected (The Trade Desk appears on 2 platforms) mean user profiles may be sold and resold across international boundaries, potentially reaching governments hostile to sexual expression.

Public figures, professionals, and others with reputational exposure risk significant personal and career damage if their adult content consumption becomes public. The advertising ecosystem's capacity to link browsing behavior to real identities creates ongoing vulnerability.

Data Already in Circulation

A critical point for users to understand: protective measures taken today may be insufficient because data has likely already been collected. The 29 platforms sharing data with Google have contributed to advertising profiles that persist for years. The 3 platforms sharing with Meta have added to social graphs that are notoriously difficult to escape. The fingerprinting data may already be in commercial databases.

This is not to suggest that privacy measures are pointless - they reduce ongoing data collection. But users should understand that their historical activity on these platforms has likely already entered commercial data ecosystems where it will persist and propagate.

6.2 Implications for Platform Design

Privacy-Respecting Operation Is Achievable

The most encouraging finding of this audit is that privacy-respecting operation is demonstrably achievable. Skip The Games scored 90/100 while operating a functional escort directory. FetLife scored 84/100 while running a complex social network. These platforms prove that the surveillance we found on other platforms is a choice, not a technical necessity.

The key differences in approach are instructive:

Skip The Games uses only Cloudflare Web Analytics - a privacy-preserving first-party analytics solution that does not share data with advertising networks. It collects basic user behavior signals (mouse movement, clicks, keystrokes) likely for fraud detection and user experience monitoring, but does not engage in session recording or fingerprinting. No tracking cookies were detected. This demonstrates that a directory site can function without invasive surveillance.

FetLife similarly avoids advertising networks and data broker connections. While it does employ fingerprinting (likely for account security and fraud prevention rather than tracking), it maintains a privacy-first approach to data collection that respects its community of BDSM practitioners who have heightened privacy concerns.

Tracking Serves Business Interests, Not User Needs

The contrast between high-scoring and low-scoring platforms reveals that most tracking serves business interests - specifically advertising revenue and user behavior exploitation - rather than user needs.

Platforms scoring in the "surveillance" tier (below 25/100) share common characteristics: aggressive advertising network integration, session recording, keystroke logging, and fingerprinting. These technologies serve to maximize advertising revenue (by providing detailed targeting data), reduce fraud (a legitimate need that does not require this level of surveillance), and capture competitive intelligence about user behavior.

None of these use cases require sharing intimate browsing data with Google, Meta, or data brokers. First-party analytics can provide business intelligence. Internal fraud detection systems can protect against abuse. A/B testing can optimize user experience. All of this can be accomplished without the surveillance apparatus we documented.

Technical Alternatives Exist

For platform operators considering changes to their tracking practices:

First-party analytics solutions like Plausible, Fathom, or self-hosted options provide meaningful traffic data without sharing information externally. Cloudflare Web Analytics (used by Skip The Games) is free and privacy-preserving.

Contextual advertising can replace behavioral targeting. Adult advertising networks already segment by content category - there is no inherent need to track individual users across sites.

Internal session recording for UX research can be conducted with explicit consent, data minimization, and strict retention limits rather than continuous surveillance.

Fraud detection through server-side analysis of request patterns does not require client-side fingerprinting libraries broadcasting data to third parties.

The technical barriers to privacy-respecting operation are low. The barriers are primarily economic - the surveillance model is profitable - and organizational - changing established practices requires leadership commitment.

6.3 Regulatory Considerations

GDPR and Special Category Data

The General Data Protection Regulation's treatment of special category data (Article 9) is directly relevant to adult platform tracking. Sexual orientation and sexual life are explicitly listed as special category data requiring explicit consent for processing.

When a platform deploys fingerprinting to identify visitors browsing gay content, they are processing special category data. When session recordings capture user interactions with BDSM content, they are processing special category data. The ubiquitous "legitimate interest" justifications that underpin much web tracking face significant challenges when applied to data revealing sexual preferences.

Several findings from this audit raise specific GDPR concerns:

Pre-consent tracking: Our scans captured the pre-consent state, yet we detected active fingerprinting and data transmission to advertising networks before any consent interaction. GDPR requires consent before processing, not after.

Fingerprinting without consent: The ePrivacy Directive (complementing GDPR) treats fingerprinting similarly to cookies - it requires consent for non-essential fingerprinting. The 87% fingerprinting rate suggests widespread non-compliance.

Data broker connections: The Trade Desk connections we detected involve data that will be further shared with unknown parties for unknown purposes - directly contrary to GDPR's purpose limitation and transparency requirements.

Controller identification: Users have no visibility into which companies are receiving their intimate browsing data through advertising networks. The data controller landscape is opaque.

US State Privacy Laws

California's CCPA/CPRA, Virginia's VCDPA, and emerging state privacy laws create varying obligations for adult platforms serving US users. The right to opt out of sale/sharing of personal information is particularly relevant given the data broker connections we detected.

However, enforcement has been limited, and adult platforms operating from outside the US may feel insulated from US regulatory action. Users should not assume that US privacy laws provide meaningful protection for their intimate browsing data.

Should Adult Platforms Face Stricter Requirements?

A policy question emerges from this audit: should platforms handling inherently sensitive content face stricter privacy requirements than general-purpose websites?

Arguments for stricter requirements:

- The data processed is categorically more sensitive
- Harms from breaches or misuse are more severe
- User expectations of privacy are higher
- Vulnerable populations disproportionately use these platforms

Arguments against special treatment:

- Defining "adult platform" creates classification challenges
- Stricter requirements could drive platforms offshore
- Users bear some responsibility for platform choice
- Existing frameworks (properly enforced) may be sufficient

The data from this audit suggests that voluntary self-regulation has failed. The arrangement dating category averaged 6/100 - platforms serving users seeking intimate connections have the worst privacy practices. This is precisely backwards from what user interests would dictate.

6.4 Future Research Directions

Logged-In vs. Logged-Out Comparison

This audit analyzed only publicly accessible pages without authentication. Significant questions remain about tracking after login: Do platforms increase surveillance of authenticated users who have provided identity information? Do they reduce tracking because users are already identified? How does tracking differ between free accounts and paid subscribers?

Mobile Application Analysis

Adult platform mobile apps may have access to device identifiers, contact lists, location data, and other information unavailable to web browsers. A comparative study of web versus app tracking would illuminate whether users face different privacy tradeoffs across access methods.

Payment Processor Data Sharing

When users purchase subscriptions or tips, payment processors receive transaction data that may be combined with browsing data. The privacy practices of payment intermediaries in the adult industry warrant investigation - particularly given the history of financial services discriminating against sex workers.

Longitudinal Tracking

How do platform privacy practices change over time? Do platforms become more invasive as they grow? Do regulatory actions (GDPR enforcement, platform scandals) produce lasting changes? A longitudinal study tracking the same platforms over years would answer these questions.

User Awareness Studies

We document what platforms do technically, but user awareness remains unstudied. Do users understand that their intimate browsing is being fingerprinted? Do they know that session recordings capture their hesitations and abandoned searches? Understanding the gap between user expectations and platform practices would inform both regulatory and educational interventions.

Cross-Platform Tracking Verification

While we detect connections to advertising networks, we have not verified the extent to which fingerprints or identifiers actually propagate across platforms. A study using controlled browsing with known identifiers could empirically measure cross-platform tracking persistence.

All statistics in this chapter are derived from scan data documented in Appendix B.

Chapter 7: Conclusion

Summary of Findings

This audit examined 38 adult platforms across eight categories and found privacy practices that fall far short of what users of sensitive content deserve. The average privacy score of 37/100 reflects an industry where surveillance is the norm and privacy-respecting operation is the exception.

The technical findings are stark: 87% of platforms employ browser fingerprinting capable of identifying users even in incognito mode. 76% likely conduct session recording, capturing every interaction with intimate content. 89% transmit keystroke data to third parties. 76% share user data with Google's advertising network. Twelve platforms reached our "surveillance" classification - including Pornhub (the world's largest adult site), Seeking (the largest arrangement dating platform), and LoyalFans, which scored 0/100 with fingerprinting across five distinct vectors.

The category-level analysis reveals a troubling pattern: platforms serving users with the most sensitive needs have the worst privacy practices. Arrangement dating sites averaged 6/100. Creator platforms averaged 35/100. Meanwhile, escort directories (60/100) and social communities (77/100) demonstrate that better practices are achievable.

The Fundamental Asymmetry

Users cannot see the tracking technologies deployed against them. They cannot know which third parties receive their data. They cannot assess downstream uses of fingerprints and behavioral profiles. They are asked to trust platforms with the most sensitive aspects of their digital lives while having no capacity to verify that trust.

Platforms hold nearly complete information. They know their commercial arrangements with advertising networks and data brokers. They know whether consent mechanisms are genuine or theatrical. They have chosen, with full knowledge, to prioritize revenue over user privacy.

This asymmetry is compounded by the lack of real alternatives. Users seeking adult content cannot simply abstain from the ecosystem. Privacy-respecting options are few and often lack the features or community size of invasive competitors. The market has not produced privacy-preserving alternatives at scale because surveillance is profitable and privacy protection is not.

A Call to Action

For Users: Make informed choices with the data in this report. Skip The Games (90/100) and FetLife (84/100) demonstrate that privacy-respecting alternatives exist. Use technical countermeasures understanding their limitations. Do not assume privacy based on incognito mode or VPNs alone - fingerprinting defeats these measures.

For Platforms: The platforms scoring above 70/100 prove that privacy-respecting operation is viable. Replace third-party analytics with privacy-preserving alternatives. Remove advertising network integrations that share user data. Disable session recording or gate it behind genuine consent. The arrangement dating platforms scoring 0/100 and 11/100 warrant particular scrutiny - Seeking and What's Your Price serve users whose privacy needs are extreme, yet they have chosen to maximize surveillance of exactly the users who can least afford exposure.

For Regulators: Existing laws - GDPR in Europe, emerging state privacy laws in the US - already provide frameworks that should constrain the practices documented here. The problem is not absence of law but absence of enforcement. The finding that 87% of platforms fingerprint users before any consent interaction suggests the current consent framework has failed in practice.

Final Statement

The stakes of adult platform privacy extend beyond abstract data protection principles. Real people - sex workers, LGBTQ+ individuals, people in abusive relationships, anyone with sexual interests they prefer to keep private - face real consequences when their intimate browsing enters commercial data ecosystems.

A fingerprint tied to browsing patterns on explicit content, flowing through advertising networks to data brokers, potentially correlatable with real-world identity, persisting for years in commercial databases - this is not a hypothetical risk. It is the documented reality of how most adult platforms operate.

Privacy in the context of sexual content is not a luxury or a preference - for many users, it is a matter of safety, employment, family relationships, and in some jurisdictions, freedom or life itself. The industry average score of 37/100 represents a collective failure to meet this responsibility.

The data in this report provides users with information to make informed choices, platforms with evidence that better practices are achievable, and regulators with documentation of widespread non-compliance. What happens next depends on whether any of these parties choose to act.

Complete platform scores, calculation methodology, and source data are provided in Appendix B.

Appendix A: Terminology and Technical Background

This appendix provides detailed explanations of the tracking technologies and privacy concepts discussed in this report.

A.1 Browser Fingerprinting Explained

What Is Fingerprinting?

Browser fingerprinting creates a unique identifier for a visitor's browser without storing anything on their device. Unlike cookies—which users can delete—fingerprints persist across sessions, private browsing modes, and even VPN use. The goal is identical to cookies: track users across visits and across websites. But fingerprinting is invisible and nearly impossible to prevent.

How It Works

Websites execute JavaScript that queries dozens of browser and hardware properties. Individually, each property is common—millions of people use Chrome on Windows with a 1920×1080 screen. Combined, the specific constellation of values creates a near-unique "fingerprint."

Research from the Electronic Frontier Foundation's Panopticklick project (2010) and subsequent studies by INRIA (2014) found that fingerprints uniquely identify 83–94% of browser *instances*—meaning individual users, not browser vendors. A 2020 study found modern fingerprinting achieves 99%+ uniqueness when combining canvas, WebGL, and audio techniques.

Example Fingerprint Components

Property	Example Value	Population Share
User Agent	Mozilla/5.0 (X11; Linux x86_64) Chrome/120...	~2%
Screen Resolution	1920×1080	~22%
Timezone	America/New_York	~15%
Installed Fonts	147 fonts detected	~0.3%
Canvas Hash	a7f3b2c9e1d4...	~0.01%
WebGL Renderer	NVIDIA GeForce RTX 3080	~0.5%
Audio Hash	d4e8f1a2b3c5...	~0.02%

Individually: common. **Combined:** likely unique on Earth.

Why Multiple Methods?

Platforms deploy multiple fingerprinting techniques because:

1. **Redundancy:** If one method fails (user blocks canvas), others still work
2. **Precision:** Combining techniques creates a more unique identifier
3. **Cross-browser tracking:** Some techniques work even when users switch browsers

A.2 Fingerprinting Techniques Glossary

Canvas Fingerprinting

What it measures: Renders invisible text or graphics to a hidden HTML canvas element, then reads the pixel data back as a hash.

Why it's identifying: Different GPUs, graphics drivers, font rendering engines, and antialiasing settings produce slightly different pixel values. Your graphics processing stack is effectively unique.

Detection in this audit: Monitoring calls to `HTMLCanvasElement.toDataURL()` and `CanvasRenderingContext2D.getImageData()`.

WebGL Fingerprinting

What it measures: Queries the WebGL API for 3D graphics hardware identifiers, including GPU vendor and renderer strings.

Why it's identifying: Returns specific hardware information like "NVIDIA GeForce RTX 4080" or "Apple M2 GPU". Combined with driver version and WebGL capabilities, this is highly identifying.

Detection in this audit: Monitoring calls to `WebGLRenderingContext.getParameter()` with `UNMASKED_VENDOR_WEBGL` and `UNMASKED_RENDERER_WEBGL` parameters.

Audio Context Fingerprinting

What it measures: Creates an `OfflineAudioContext`, generates an inaudible audio signal (oscillator), processes it, and measures the output waveform.

Why it's identifying: Different audio hardware, drivers, and browser audio processing implementations produce measurably different waveforms from the same input. Your sound card has a signature.

Detection in this audit: Monitoring `OfflineAudioContext.startRendering()` calls.

Navigator Fingerprinting

What it measures: Reads properties from the browser's `navigator` object: platform, language, timezone, CPU core count, device memory, hardware concurrency, and more.

Why it's identifying: Combines operating system, language preferences, timezone, and hardware specifications. "Linux x86_64, en-US, 8 cores, 16GB RAM, America/New_York" narrows the population significantly.

Detection in this audit: Monitoring access to `navigator.platform`, `navigator.languages`, `navigator.hardwareConcurrency`, `navigator.deviceMemory`.

Battery Fingerprinting

What it measures: Reads battery charge level, charging status, and estimated time remaining via the Battery Status API.

Why it's identifying: A laptop at 67% charge, discharging, with 4.2 hours remaining is surprisingly unique at any given moment. Combined with other properties, this adds entropy.

Note: Most modern browsers have deprecated or restricted this API due to privacy concerns. However, some platforms still attempt to call it.

Detection in this audit: Monitoring calls to `navigator.getBattery()`.

FingerprintJS

What it is: A commercial fingerprinting library that combines multiple techniques into a single identification service. Offers both open-source and enterprise versions.

Privacy impact: Platforms using FingerprintJS have explicitly chosen to deploy sophisticated visitor identification. This represents intentional tracking infrastructure.

Detection in this audit: Pattern matching for FingerprintJS initialization code in inline scripts.

A.3 Session Recording

What It Is

Session recording captures a complete replay of a user's visit: every mouse movement, scroll position, click, text selection, form interaction, and page change. Services like Hotjar, FullStory, PostHog, and Microsoft Clarity sell this capability as "user experience analytics."

How It Works

JavaScript monitors:

- **DOM mutations:** Every change to the page structure
- **Pointer events:** Mouse movement coordinates, click positions
- **Scroll position:** What the user is viewing
- **Keyboard input:** What the user types (often partially redacted, but not always)
- **Form interactions:** Field focus, input, abandonment

This data streams to third-party servers in real-time, where it's reconstructed into a video-like replay that analysts can review.

Privacy Implications

On a mainstream website, session recording might reveal shopping behavior or checkout friction. On an adult platform, session recording means a third party has a detailed record of:

- Exactly what content a user viewed
- How long they viewed each item
- What they searched for
- Which creators they explored
- What messages they drafted (even if not sent)
- Their interaction patterns with intimate content

For platforms with user-generated content (OnlyFans, Fansly), this includes which specific creators a user follows, subscribes to, or messages.

Detection in This Audit

Session recording was flagged when we detected:

1. MutationObservers monitoring DOM changes
2. Combined mouse movement, scroll, and click tracking
3. Data exfiltration to known session recording services

A.4 Keystroke Logging

What It Is

Monitoring `keydown`, `keyup`, and `input` events on form fields, search boxes, and potentially the entire page.

Legitimate Uses

- Auto-complete suggestions

- Real-time form validation
- Search-as-you-type functionality

Privacy Concerns

On adult platforms, keystroke monitoring captures:

- **Search queries:** What users are looking for, including abandoned searches
- **Messages:** Communications with creators or other users
- **Form input:** Registration data, potentially including real names, emails, addresses
- **Draft content:** Text typed but not submitted

When combined with session recording, keystroke data provides a complete record of user intent and communication—including content the user chose not to submit.

Detection in This Audit

Keystroke monitoring was flagged when we detected event listeners for `keydown`, `keyup`, or `input` events, particularly in combination with other behavioral monitoring.

A.5 Cookie Classifications

Session Cookies

Purpose: Maintain state during a single browsing session (login status, shopping cart).

Lifetime: Deleted when the browser closes.

Privacy impact: Low—does not persist across sessions.

Functional Cookies

Purpose: Remember user preferences (language, theme, display settings).

Lifetime: Varies, often weeks to months.

Privacy impact: Low—serves user needs, typically first-party only.

Tracking Cookies

Purpose: Identify users across visits and potentially across websites for advertising, analytics, or behavioral profiling.

Lifetime: Often months to years. Seeking deploys cookies with lifetimes exceeding 2 years.

Privacy impact: High—enables persistent identification and cross-site tracking.

Third-Party Cookies

Definition: Cookies set by a domain other than the one the user is visiting.

Example: Visiting `pornhub.com` results in a cookie from `doubleclick.net`.

Privacy impact: High—enables cross-site tracking by advertising networks.

Note: Major browsers are phasing out third-party cookies, but first-party tracking and fingerprinting remain unaffected.

A.6 Data Sharing Level Definitions

This audit classifies platforms into five data sharing levels based on detected tracking infrastructure:

None

Definition: No third-party tracking technologies detected.

What this means: The platform does not share visitor data with external parties based on our detection methods.

Score impact: Minimal penalty.

Analytics Only

Definition: First-party or privacy-focused analytics only (e.g., Cloudflare Web Analytics, self-hosted solutions, PostHog).

What this means: The platform collects usage data but does not share it with advertising networks.

Score impact: Minor penalty.

Advertising

Definition: Data shared with advertising networks (Google Ads, Meta, adult ad networks).

What this means: Visitor data enters advertising ecosystems where it may be used for targeted advertising across the web.

Score impact: Moderate penalty.

Extensive

Definition: Multiple advertising networks plus fingerprinting or session recording.

What this means: Comprehensive visitor profiling with persistent identification mechanisms.

Score impact: Major penalty.

Surveillance

Definition: Fingerprinting + session recording + advertising networks, potentially with data broker connections.

What this means: Maximum data collection across all vectors. Visitors are uniquely identified, their behavior is recorded in detail, and this data is shared with multiple third parties.

Score impact: Maximum penalty. Platforms at this level scored 0-25/100 in our audit.

A.7 Third Parties Detected

Advertising Networks

Network	Parent Company	Scope
Google Ads / DoubleClick	Google (Alphabet)	General web
Facebook Pixel	Meta	General web
Twitter/X Pixel	X Corp	General web
TrafficJunky	MindGeek/Aylo	Adult-focused
Exoclick	Exoclick S.L.	Adult-focused
TrafficStars	TrafficStars	Adult-focused
JuicyAds	JuicyAds	Adult-focused

Analytics Services

Service	Type	Privacy Impact
Google Analytics	Web analytics	Moderate—data enters Google ecosystem
Hotjar	Session recording	High—complete visit replays
PostHog	Product analytics	Moderate—can include session recording
Yandex Metrika	Web analytics	High—Russian company, session recording capable
Microsoft Clarity	Session recording	High—complete visit replays
Amplitude	Product analytics	Moderate—behavioral tracking
New Relic	Performance monitoring	Low—primarily technical metrics

Data Brokers

Broker	Business Model
The Trade Desk	Programmatic advertising, data marketplace

Data brokers aggregate user data from multiple sources and sell access to advertisers, researchers, and other buyers. When adult platform data enters these networks, it may be combined with data from other sources to build comprehensive user profiles.

Appendix B: Complete Data Tables

All statistics in this report are derived from the scan data below. This appendix provides the source data for verification.

B.1 Summary Statistics

Metric	Value	Calculation
Total Platforms	38	Direct count
Average Score	37/100	Sum of scores (1,405) ÷ 38
Median Score	40/100	Middle value when sorted
Worst Platform	LoyalFans	0/100
Best Platform	Skip The Games	90/100
Total Trackers	164	Sum across all platforms

B.2 Key Finding Calculations

Fingerprinting Rate: 33/38 (87%)

Platforms with fingerprinting detected (33):

- Eros
- Tryst
- ListCrawler
- Private Delights
- OnlyFans
- Fansly
- LoyalFans
- Chaturbate
- Stripchat
- MyFreeCams
- BongaCams
- CamSoda
- LiveJasmin
- JerkMate
- Cam4
- Pornhub
- XVideos
- xHamster
- XNXX
- RedTube
- SpankBang
- Beeg

23. YouPorn
24. Kink
25. Brazzers
26. Reality Kings
27. Evil Angel
28. ManyVids
29. Clips4Sale
30. Seeking
31. What's Your Price
32. FetLife
33. AdultFriendFinder

Platforms without fingerprinting detected (5):

1. Slix
2. AdultSearch
3. Skip The Games
4. Playboy
5. Naughty America

Calculation: $33 \div 38 = 0.868 = 87\%$

Session Recording Rate: 29/38 (76%)

Platforms with session recording likely (29):

1. Tryst
2. Slix
3. ListCrawler
4. Private Delights
5. Fansly
6. LoyalFans
7. Chaturbate
8. Stripchat
9. BongaCams
10. CamSoda
11. LiveJasmin
12. JerkMate
13. Cam4
14. Pornhub
15. XVideos
16. xHamster
17. XNXX
18. RedTube
19. SpankBang
20. Beeg
21. YouPorn
22. Playboy
23. Brazzers
24. Reality Kings

25. Evil Angel
26. ManyVids
27. Clips4Sale
28. Seeking
29. What's Your Price

Platforms without session recording (9):

1. Eros
2. AdultSearch
3. Skip The Games
4. OnlyFans
5. MyFreeCams
6. Kink
7. Naughty America
8. AdultFriendFinder
9. FetLife

Calculation: $29 \div 38 = 0.763 = 76\%$

Keystroke Monitoring Rate: 34/38 (89%)

Platforms with keystroke monitoring (34):

1. Eros
2. Tryst
3. AdultSearch
4. ListCrawler
5. Private Delights
6. Skip The Games
7. OnlyFans
8. LoyalFans
9. Chaturbate
10. Stripchat
11. MyFreeCams
12. BongaCams
13. CamSoda
14. LiveJasmin
15. JerkMate
16. Cam4
17. Pornhub
18. XVideos
19. xHamster
20. XNXX
21. RedTube
22. SpankBang
23. Beeg
24. YouPorn
25. Playboy
26. Kink

27. Brazzers
28. Reality Kings
29. Evil Angel
30. Naughty America
31. ManyVids
32. Seeking
33. What's Your Price
34. AdultFriendFinder

Platforms without keystroke monitoring (4):

1. Slixa
2. Fansly
3. Clips4Sale
4. FetLife

Calculation: $34 \div 38 = 0.895 = 89\%$

Surveillance-Level Platforms: 12/38 (32%)

Platforms classified as "surveillance" (12):

1. LoyalFans (0/100)
2. LiveJasmin (0/100)
3. Pornhub (0/100)
4. RedTube (0/100)
5. SpankBang (0/100)
6. YouPorn (0/100)
7. Seeking (0/100)
8. CamSoda (7/100)
9. What's Your Price (11/100)
10. ListCrawler (12/100)
11. Fansly (23/100)
12. Brazzers (23/100)

Calculation: $12 \div 38 = 0.316 = 32\%$

B.3 Complete Platform Data Table

Sorted by score (ascending = worst first):

Rank	Platform	Category	Score	Grade	Data Sharing	Trackers	Fingerprint	Session Rec	Keystroke
1	LoyalFans	Creator Platform	0	F	Surveillance	6	Yes	Yes	Yes
2	LiveJasmin	Cam Site	0	F	Surveillance	5	Yes	Yes	Yes
3	Pornhub	Tube Site	0	F	Surveillance	5	Yes	Yes	Yes
4	RedTube	Tube Site	0	F	Surveillance	5	Yes	Yes	Yes
5	SpankBang	Tube Site	0	F	Surveillance	11	Yes	Yes	Yes
6	YouPorn	Tube Site	0	F	Surveillance	7	Yes	Yes	Yes
7	Seeking	Arrangement Dating	0	F	Surveillance	9	Yes	Yes	Yes
8	CamSoda	Cam Site	7	F	Surveillance	5	Yes	Yes	Yes
9	What's Your Price	Arrangement Dating	11	D-	Surveillance	7	Yes	Yes	Yes
10	ListCrawler	Escort Directory	12	D-	Surveillance	4	Yes	Yes	Yes
11	Fansly	Creator Platform	23	D	Surveillance	7	Yes	Yes	No
12	Brazzers	Major Studio	23	D	Surveillance	1	Yes	Yes	Yes
13	Chaturbate	Cam Site	25	D+	Extensive	7	Yes	Yes	Yes
14	Beeg	Tube Site	25	D+	Extensive	5	Yes	Yes	Yes
15	Evil Angel	Major Studio	29	D+	Extensive	4	Yes	Yes	Yes
16	xHamster	Tube Site	30	D+	Extensive	4	Yes	Yes	Yes
17	Playboy	Major Studio	31	D+	Extensive	9	No	Yes	Yes
18	ManyVids	Clip Site	32	D+	Extensive	2	Yes	Yes	Yes
19	Kink	Major Studio	34	C-	Extensive	5	Yes	No	Yes
20	Cam4	Cam Site	35	C-	Extensive	6	Yes	Yes	Yes
21	Stripchat	Cam Site	40	C	Extensive	0	Yes	Yes	Yes
22	BongaCams	Cam Site	43	C	Extensive	4	Yes	Yes	Yes
23	XVideos	Tube Site	43	C	Extensive	5	Yes	Yes	Yes
24	XNXX	Tube Site	43	C	Extensive	5	Yes	Yes	Yes
25	Reality Kings	Major Studio	44	C	Extensive	0	Yes	Yes	Yes
26	JerkMate	Cam Site	45	C	Extensive	5	Yes	Yes	Yes
27	Slixa	Escort Directory	56	B-	Advertising	4	No	Yes	No

Rank	Platform	Category	Score	Grade	Data Sharing	Trackers	Fingerprint	Session Rec	Keystroke
28	Clips4Sale	Clip Site	58	B-	Advertising	4	Yes	Yes	No
29	Tryst	Escort Directory	60	B-	Analytics Only	1	Yes	Yes	Yes
30	Private Delights	Escort Directory	63	B	None	0	Yes	Yes	Yes
31	MyFreeCams	Cam Site	64	B	Advertising	2	Yes	No	Yes
32	Naughty America	Major Studio	66	B	Advertising	5	No	No	Yes
33	AdultSearch	Escort Directory	67	B	Advertising	5	No	No	Yes
34	AdultFriendFinder	Social Community	69	B	Advertising	3	Yes	No	Yes
35	Eros	Escort Directory	70	B+	Advertising	5	Yes	No	Yes
36	OnlyFans	Creator Platform	82	A-	Analytics Only	1	Yes	No	Yes
37	FetLife	Social Community	84	A-	Advertising	0	Yes	No	No
38	Skip The Games	Escort Directory	90	A	Analytics Only	1	No	No	Yes

B.4 Category Averages

Category	Count	Avg Score	Calculation	Min	Max
Escort Directories	7	60	$(90+70+67+63+60+56+12)\div 7 = 418\div 7$	12	90
Creator Platforms	3	35	$(82+23+0)\div 3 = 105\div 3$	0	82
Cam Sites	8	32	$(64+45+43+40+35+25+7+0)\div 8 = 259\div 8$	0	64
Tube Sites	8	18	$(43+43+30+25+0+0+0+0)\div 8 = 141\div 8$	0	43
Major Studios	6	38	$(66+44+34+31+29+23)\div 6 = 227\div 6$	23	66
Clip Sites	2	45	$(58+32)\div 2 = 90\div 2$	32	58
Arrangement & Dating	2	6	$(11+0)\div 2 = 11\div 2$	0	11
Social & Community	2	77	$(84+69)\div 2 = 153\div 2$	69	84

Overall Average: $1,405 \div 38 = 37$ (rounded from 36.97)

B.5 Grade Distribution

Grade	Score Range	Count	Platforms
A	85-100	1	Skip The Games (90)
A-	78-84	2	OnlyFans (82), FetLife (84)
B+	70-77	1	Eros (70)
B	62-69	5	AdultFriendFinder (69), AdultSearch (67), Naughty America (66), MyFreeCams (64), Private Delights (63)
B-	55-61	3	Tryst (60), Clips4Sale (58), Slixa (56)
C	40-47	6	JerkMate (45), Reality Kings (44), XVideos (43), XNXX (43), BongaCams (43), Stripchat (40)
C-	33-39	2	Cam4 (35), Kink (34)
D+	25-32	6	ManyVids (32), Playboy (31), xHamster (30), Evil Angel (29), Beeg (25), Chaturbate (25)
D	18-24	2	Fansly (23), Brazzers (23)
D-	10-17	2	ListCrawler (12), What's Your Price (11)
F	0-9	8	CamSoda (7), Seeking (0), YouPorn (0), SpankBang (0), RedTube (0), Pornhub (0), LiveJasmin (0), LoyalFans (0)

Total: 38 platforms

B.6 Data Sharing Level Distribution

Level	Definition	Count	Percentage
Surveillance	Fingerprinting + session recording + advertising + data brokers	12	32%
Extensive	Multiple trackers, score 25-49	14	37%
Advertising	Ad networks present, score ≥ 50	9	24%
Analytics Only	Analytics but no advertising	2	5%
None	No trackers detected	1	3%

B.7 Cookie Analysis

Highest Cookie Counts

Platform	Total Cookies	Tracking Cookies	Third-Party Cookies	Long-Lived (>90d)
Seeking	47	21	19	31
SpankBang	27	13	12	19
What's Your Price	23	15	14	11
LiveJasmin	22	9	3	9
Pornhub	21	8	0	9
ListCrawler	18	14	11	13
Fansly	18	9	6	12
RedTube	17	5	0	5
Stripchat	17	1	0	13

Platforms with Third-Party Cookies

Platform	Third-Party Cookie Count
Seeking	19
What's Your Price	14
SpankBang	12
Beeg	11
ListCrawler	11
Fansly	6
LiveJasmin	3
Evil Angel	2
Cam4	2
CamSoda	1
Chaturbate	1
JerkMate	1
LoyalFans	1
Slix	1
Clips4Sale	1

B.8 Source Data Reference

All data extracted from scan performed: **2026-01-29 01:13 UTC**

Source files:

- `output/privacy-scanner.db` (SQLite database)
- `output/report-2026-01-29.json` (888 KB)
- `output/report-2026-01-29.md` (98 KB)

Scanner version: privacy-scanner v1.0 Scan location: Iceland (EU) Browser: Chromium via Playwright

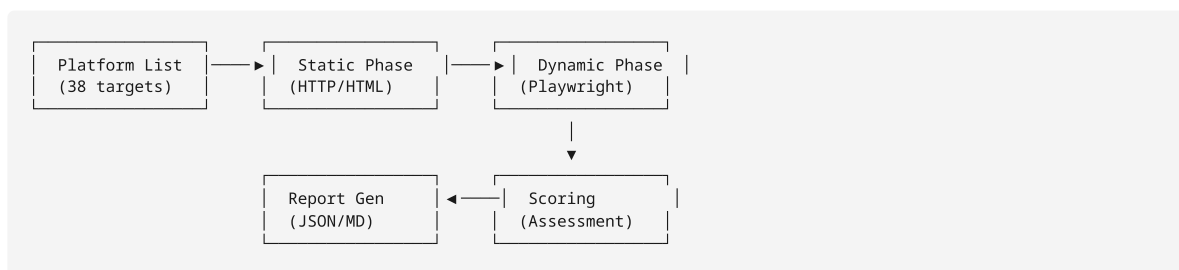
Appendix C: Methodology Details

Technical specifications for the privacy scanning infrastructure.

C.1 Scanning Architecture

Overview

The scanner uses a two-phase architecture:



Phase 1: Static Analysis

HTTP-based analysis without JavaScript execution:

- **HTTP Headers:** Cookie analysis, CSP domains, security headers
- **HTML Parsing:** Script tags, tracking pixels, iframes, meta tags
- **Script Sources:** External script URLs, inline script content
- **Prefetch Hints:** DNS-prefetch, preconnect indicators

Phase 2: Dynamic Analysis

Playwright/Chromium automation with full JavaScript execution:

- **API Interception:** Canvas, WebGL, AudioContext, Navigator, Battery
- **Network Capture:** All requests/responses with timing
- **Cookie Collection:** Runtime cookie state
- **Event Listener Monitoring:** Behavioral tracking detection
- **DOM Observation:** MutationObserver and IntersectionObserver usage

C.2 Tracker Detection Signatures

Google Analytics

Patterns detected:

- Script: googletagmanager.com/gtag/js
- Script: google-analytics.com/analytics.js
- Script: google-analytics.com/ga.js
- Network: google-analytics.com/g/collect
- Network: analytics.google.com/g/collect
- Cookies: _ga , _gid , _gat

Confidence: 95% (script), 90% (cookie only)

Google Tag Manager

Patterns detected:

- Script: `googletagmanager.com/gtm.js`
- Inline: `gtag('config', initialization`

Confidence: 95%

Facebook Pixel

Patterns detected:

- Script: `connect.facebook.net/*/fbevents.js`
- Network: `facebook.com/tr`
- Cookies: `_fbp`, `_fbclid`

Confidence: 95% (script), 90% (cookie)

Hotjar

Patterns detected:

- Script: `static.hotjar.com/c/hotjar-`
- Script: `script.hotjar.com`
- Inline: `hj('identify', or hj.q`

Confidence: 95%

Fingerprinting APIs

Canvas:

- `HTMLCanvasElement.toDataURL()`
- `CanvasRenderingContext2D.getImageData()`

WebGL:

- `WebGLRenderingContext.getParameter(37445)` (UNMASKED_VENDOR)
- `WebGLRenderingContext.getParameter(37446)` (UNMASKED_RENDERER)

Audio:

- `OfflineAudioContext.startRendering()`

Navigator:

- `navigator.platform`
- `navigator.languages`
- `navigator.hardwareConcurrency`
- `navigator.deviceMemory`

Battery:

- `navigator.getBattery()`

Confidence: 97% (API interception is definitive)

C.3 Scoring Algorithm

Base Score

All platforms start at 100 points.

Deductions by Tracker Category

Category	Base Deduction
Data Brokers	15 points
Fingerprinting	12 points
Advertising	8 points
Social Widgets	6 points
Analytics	4 points
Consent Management	1 point

Severity Multipliers

Tracker Severity	Multiplier
Critical (!!!!)	1.3x
High (!!!)	1.0x
Medium (!!)	0.7x
Low (!)	0.4x

Diminishing Returns

Multiple trackers in the same category use diminishing returns:

```
total_deduction = base × (1 + 0.3 × (count - 1))
```

Example: 3 advertising trackers = $8 \times (1 + 0.3 \times 2) = 12.8$ points

Behavioral Deductions

Behavior	Deduction
Session recording likely	15 points
Keystroke tracking	8 points
Heavy event listener usage (>500)	5 points

Cookie Deductions

Cookie Type	Deduction
Per tracking cookie	2 points
Per third-party cookie	3 points
Per long-lived cookie (>90 days)	1 point

Score Floor

Minimum score is 0. Negative scores are clamped.

Data Sharing Level Assignment

Level	Criteria
None	No third-party trackers detected
Analytics Only	Only analytics (no advertising)
Advertising	Any advertising network present
Extensive	Advertising + fingerprinting OR multiple ad networks
Surveillance	Fingerprinting + session recording + advertising

C.4 Platform Selection

Selection Criteria

1. **Traffic Volume:** Minimum 100,000 monthly visits (Semrush December 2025)
2. **Category Coverage:** Representative sample across all business models
3. **Geographic Relevance:** Accessible from EU/Iceland without geo-blocking

Traffic Data Sources

- Semrush (primary)
- SimilarWeb (validation)

Categories and Coverage

Category	Platforms	Selection Rationale
Escort Directories	7	Major US/EU directories
Creator Platforms	3	Market leaders
Cam Sites	8	High-traffic sites
Tube Sites	8	Highest traffic category
Major Studios	6	Established brands
Clip Sites	2	Creator-focused clip sales
Arrangement & Dating	2	Sugar dating leaders
Social & Community	2	Community platforms

C.5 Scanning Environment

Technical Specifications

- **Browser:** Chromium (via Playwright)
- **User Agent:** Standard Chrome on Linux
- **Viewport:** 1920×1080
- **Location:** Iceland (EU jurisdiction)
- **Network:** Residential IP (not VPN/datacenter)
- **JavaScript:** Enabled
- **Cookies:** Accepted (no prior consent interaction)

Scan Behavior

1. Navigate to homepage
2. Wait for page load (networkidle)
3. Scroll to 50% of page height
4. Wait 3 seconds for dynamic content
5. Capture all data points
6. Close browser

Timing

- Scan date: January 29, 2026
- Scans performed: 01:00-02:00 UTC
- Concurrency: 4 parallel scans (RAM-limited)

C.6 Confidence Scoring

Each tracker detection includes a confidence score:

Evidence Type	Confidence
API interception (fingerprinting)	97%
Script source match	95%
Network request match	90%
Cookie name match	90%
Inline script pattern	88%
CSP domain (potential)	60%

Trackers marked "potential/unconfirmed" have only CSP-level evidence.

C.7 Reproducibility

Code Availability

Scanner source code: `/var/home/lilith/Code/@projects/@lilith/lilith-platform/codebase/tools/privacy-scanner/`

Dependencies

- Node.js / Bun runtime
- Playwright (browser automation)
- better-sqlite3 (result storage)
- TypeScript

Execution

```
cd codebase/tools/privacy-scanner
bun run scan --no-cache
```

Output

- SQLite database: `output/privacy-scanner.db`
- JSON results: `output/scan-results-{date}.json`
- Markdown report: `output/scan-results-{date}.md`