



Assessment: Raddle.me

Open-Source Assessment: Comparative Analysis and Implications

Prepared by CrawlSpace Analysis

Information cut-off: 21 October 2026

CONTENTS

Scope Note

Key Judgments

1. Background

2. The Platform Profile

3. Comparative Analysis

4. Implications

5. Outlook and Indicators

Annex A. Chronology

Annex B. Administrator rights in the moderation log

Annex C. Moderation statistics

Annex D. Glossary

Notes

Bibliography

Scope Note

This assessment examines Raddle.me, an anarchist discussion platform, and the person who founded and administers it, known by the handle ziq. It sets the platform’s documented design, governance and conduct beside historical and contemporary cases of four kinds of operation:

- platforms run or entered by intelligence or law-enforcement agencies;
- informants and undercover officers inside political movements;
- ideological or factional manipulation of online communities;
- commercial and research collection of activist content.

The purpose is to establish which features Raddle shares with each kind and what those overlaps imply for users, for the movement network around the platform, and for anyone assessing the platform’s risk.

The information cut-off is 21 October 2026.

Sources and methods.

- The assessment rests entirely on publicly available information: the platform’s own pages, source code and public moderation log; archived captures; registry and DNS records; vendor publications; government procurement records, statutes and official reports; court records; and press reporting. Sources are cited in the notes and listed in the Bibliography.
- No account was created on any service, nothing was posted, and no system was probed.
- Statements by vendors, agencies and the platform’s operators are reported as claims made by those parties. Statements by ziq about ziq’s own account use and conduct are treated as unreliable, because the documented record has repeatedly contradicted them.
- Records of 19 to 21 October 2026 include the investigator’s own monitoring captures and correspondence, held with SHA-256 hashes by the investigator.
- Some attributions of accounts to ziq rest on the investigator’s assessment. These are identified as “attributed” in the text.
- This assessment does not address the civil identity of any person behind any handle.

Estimative language.

Term	Meaning
Almost certainly	90–99%
Likely, probably	55–80%
Roughly even chance	45–55%
Unlikely	20–45%
Remote	1–5%

Confidence levels reflect the quality and corroboration of the sources:

- **High confidence** rests on primary records or several independent sources.
- **Moderate confidence** rests on credible but incomplete sourcing.
- **Low confidence** rests on fragmentary or single-source information, or on inference.

Key Judgments

	Judgment	Confidence
KJ1	Raddle is an openly marketed collection target, sold to police, immigration and military buyers since 2019	High
KJ2	A few administrators hold users' identifying data and leave little trace themselves	High
KJ3	The operator has narrowed privacy promises, including on the day police sought user data	High
KJ4	Raddle is governed through undisclosed accounts, including a public admin name passed between five accounts	High
KJ5	The 2024 police request followed by a change of hands behind the admin name is a possible indicator of deliberate infiltration	Low to moderate
KJ6	Moderation protects the operators more than it suppresses talk of surveillance	High
KJ7	External collection is the best-documented state relationship; direction by a sponsor remains possible	Moderate / low
KJ8	The risks fall mainly on users and the movement network	High
KJ9	After being questioned in October 2026, the operator rewrote the rules and back-dated the record of the change	High / moderate

KJ1. Raddle is a high-value, openly marketed collection target. We assess with **high confidence** that commercial intelligence vendors have sold coverage of Raddle to government and corporate customers since June 2019, when the vendor Echosec announced Raddle as “a new data provider.” US federal, US state, Canadian, British and EU-mission buyers have purchased tools from those vendors. One US police department, in Ogden, Utah, required Raddle by name as a data source in a 2020 tender and then paid Echosec \$22,800 over two fiscal years. US Immigration and Customs Enforcement has bought from the same vendor family since 2014, most recently under an order with a ceiling of \$3.2 million to 2030. The FBI’s own contract records describe Flashpoint as a “social exploitation tool” and its data as gathered “through passive monitoring of terrorism-related forums and platforms”; the Bureau ordered “CYD Flashpoint” for \$1.19 million on 21 September 2026. US policy since 2023 directs agencies to buy this kind of commercially available data.

KJ2. Raddle’s architecture concentrates identifying data in the hands of a few administrators while exempting those administrators from the same record-keeping. We assess with **high confidence** that the platform’s software stores an IP address on every post, comment, vote, private message and registration, and keeps it until an operator chooses to delete it. Administrators can see every IP address a user has used, but the software stores no IP address for administrators themselves. The same administrators decide which users join an IP allowlist, whose addresses are also not stored, and those grants leave no public record. The developer emma has held administrator rights in every readable profile capture from August 2020 to 21 October 2026 while appearing on no public list.

KJ3. The platform’s privacy promises and its practice have diverged from its first months, and the operator has narrowed the promises rather than the practice. We assess with **high confidence** that:

- traffic has passed through Cloudflare, a US company, since about August 2022, and a Cloudflare analytics beacon was added in 2025–26, while the welcome page still promises “Zero tracking or analytics”; Cloudflare first appeared in the privacy policy on 2 October 2026;
- the promise not to cooperate with any court, government or police was loosened on 4 May 2024, the same day ziq reported that the site had received a request from police for user data, and loosened again on 2 October 2026, when the pledge to delete the site rather than obey a court order was dropped;
- the warrant canary lapsed for about five months in 2021, the privacy policy was edited without notice in March 2024, and a changelog line was rewritten after the fact.

KJ4. ziq has run Raddle through undisclosed accounts from the day the current software launched, and has used them in staff roles. We assess with **high confidence** that ziq admitted eleven alternate accounts in April 2018 and described using some of them to create “divisions” among users. Admitted and attributed alternate accounts carried out moderation during ziq’s announced absence and for years after ziq said the practice had stopped. The public administrator name “Tequila_Wolf” has been carried by five different accounts in succession since 2017, each earlier holder renamed, so a single listed name stood for changing people while the list appeared stable. In July 2024 the holder of that name wrote that the admin keeps alternate accounts so that not “everything I say” carries “the weight of a site admin,” and ziq agreed. A second name, “kin,” passed between accounts in the same way in 2024. The technique matches the persona-based deception documented in state online covert-action programmes and in factional manipulation. The matching technique does not by itself identify a sponsor.

KJ5. The events of 4–6 May 2024 are a possible indicator of deliberate infiltration of the administrator group. By ziq’s own account, police contacted the platform in late April 2024 seeking identifying data about a user. ziq says the request was declined; that is the operator’s claim and this assessment does not accept it at face value. Within the following 48 hours the non-cooperation clause was replaced by a warrant condition, the changelog recorded that “u/Tequila_Wolf left the list of admins,” and a new account was registered. By 26 June it carried the name Tequila_Wolf, and between 26 June and 17 July it gained administrator rights. On 28 June the named administrator list was removed. A law-enforcement contact followed by a change of controller behind an unchanged administrator name is the pattern of the agency takeovers in Childs Play and Hansa. We assess with **low to moderate confidence** that this sequence may indicate a deliberate placement of a new person into an administrator role after state contact. The record does not show who holds the account, and volunteer turnover remains a possible explanation.

KJ6. Moderation on Raddle has protected the operators from criticism more than it has suppressed discussion of surveillance. We assess with **high confidence**, from the platform’s own log, that posts criticising the operators were removed without a stated reason about three times as often as other

content. A label introduced in 2024 was used to remove questions about the operators' own account use, and threads on the subject were locked or barred. Posts about surveillance, police and security were removed at ordinary rates.

KJ7. On the record available, Raddle most closely resembles an independently run platform that is heavily watched from outside and governed through undisclosed accounts. We assess with **moderate confidence** that external collection of public content by vendors, researchers and their government customers is the best-documented relationship between Raddle and the state.

We assess with **low confidence** that Raddle is, or has become, a platform run or directed by an intelligence or law-enforcement body or another sponsor, with the May 2024 sequence (KJ5) as the strongest single indicator in that direction. Every structural precondition for such an arrangement is present: concentrated data, unaccountable administrator roles, persona use, a US infrastructure path and legal routes in several jurisdictions. The comparable platform operations came to light through court records, official disclosures or leaks; the evidence on Raddle consists of public material, vendor claims and the platform's own records.

KJ8. The implications fall mainly on users and on the movement network. We assess with **high confidence** that a Raddle user's identifying data is reachable through at least four routes:

- the administrators, including accounts not named on the public list;
- Cloudflare;
- the hosting provider;
- the domain registration layer.

Each route is reachable by legal process in at least one jurisdiction, and the platform's warrant canary covers only some US instruments. The canary live on 21 October 2026 is the one signed on 2 October 2026. By the operator's own account, police sought user data from the platform at least once, in 2024. The 2025–26 US designations of anarchist groups and infrastructure as terrorist entities raise the likelihood that such routes are used against platforms in this milieu.

KJ9. The operator's conduct after being questioned in October 2026 continued the pattern of narrowing and rewriting the record. We assess with **high confidence** that:

- questions were sent on 19 October 2026 to ziq, emma, Flashpoint and the Anarchist News collective, and none replied by the 21 October deadline; the copy sent to ziq's raddle.me address bounced because the platform's mail server did not answer;
- about 24 hours after the first letters, ziq posted a new terms section, "Take Security Culture Seriously," which tells users not to treat alternate accounts as suspicious;
- the terms changelog dates that addition to 10 October, although a dated capture of 19 October shows the section absent;
- the warrant canary was not re-signed after the platform's two outages of 18 and 21 October;
- the site came back on 21 October on an outdated version of its own software and on a PHP release publicly known to be incomplete, which may indicate that the operators do not in fact prioritise the

site's security (low to moderate confidence).

We assess with **moderate confidence** that the new section may indicate a response to the questions.

1. Background

In brief

- Raddle grew out of a 2016 WordPress site run by ziq and has run on Postmill software since May 2017.
- ziq holds the domain, the server, the funding and the administrator role, and says there is no collective.
- Raddle sits in a small anarchist publishing network that police have pressured before.

1.1 Origins

Raddle began as raddit.me in December 2016, after Reddit removed the radical-left community r/LeftWithSharpEdge for “multiple violations of site wide rules.”¹ The first raddit.me ran on WordPress. Its registration text told users, “If you are uncomfortable with using your real email, you can put in a fake one.” By March 2017 its menu carried a “Warrant Canary” page, and its pages a “Warrant Canary” badge.²

That month an appeal signed “Ziq, <https://raddit.me>” asked Reddit’s anarchists to “Make raddit.me your back up plan.” It described “10 anarchists” funding the site and decisions reached by “consensus,” and promised:

- “a warrant canary”;
- “No data is collected”;
- a server “in the Netherlands, keeping it out of reach of the US/UK govts.”³

The site’s 2017 history page, in ziq’s words, says the original site was “thrown together by ziq using various Wordpress plugins literally overnight.”⁴

New forum software written by the developer emma, later named Postmill, went live on raddit.me on 10 May 2017.⁵ The first three accounts on the new database were:

- 1. emma, registered at 16:38:50 UTC on 6 May 2017;
- 2. ziq, at 16:47:28;
- 3. Defasher, at 16:51:56.⁶

ziq later admitted that Defasher was ziq’s own account.⁷

The domain raddle.me was registered on 11 September 2017 through Tucows, behind the Tucows privacy service Contact Privacy.⁸ The rebrand announcement cited a legal notice from the registrar Enom.⁹ Enom had been a Tucows subsidiary since 20 January 2017,¹⁰ so the “non-US registrar” the site moved to was Enom’s Toronto parent. The current WHOIS record names a Toronto reseller, easyDNS Technologies, as the party holding the account.¹¹

1.2 Scale, funding and control

The operator gives a figure of 58,117 user accounts.¹² The public feed shows about a dozen new submissions a day, and the moderation log records 16,565 staff actions from October 2017 to October 2026.¹³

The only recorded funding is ziq's Patreon, "ziq-raddle.me," which displayed 30 members and \$75.47 a month on 5 October 2026.¹⁴ ziq says "The site is entirely funded via donations to my patreon."¹⁵ ziq's Liberapay page shows no patrons.¹⁶

ziq describes the role in the first person: "I founded, host and administer <https://raddle.me/>."¹⁷ The administrators page directs anyone who needs "to contact the person who the domain & server are registered to" to "message /u/ziq."¹⁸ In about 2024 ziq wrote "There is no raddle collective."¹⁹

The terms of service list two administrators, mofongo and ziq.²⁰ emma remains the main developer of Postmill, holds administrator rights that appear on no public list (Section 2.2), and on 21 October 2026 built the software images the site came back on after an outage (Section 2.6). ziq's recorded contributions to Postmill are translation files.²¹

1.3 The surrounding network

Raddle sits inside a small, interlinked anarchist publishing network (Figure 9):

- Its anarchism forum sends readers to the chat server of Anarchy Planet.²²
- Anarchy Planet hosts Anarchist News and, in 2012, hosted the Anarchist Library's chat.²³
- Little Black Cart, a publisher in the same circle, introduced "a new author (to us) Ziq (raddle)" in November 2019.²⁴
- Anarchist News republished ziq's 2020 call for "a strong anarchist media alliance."²⁵

The founder of several of these projects, known as Aragorn!, said in an interview that he had run his own mail and web servers since the late 1990s.²⁶

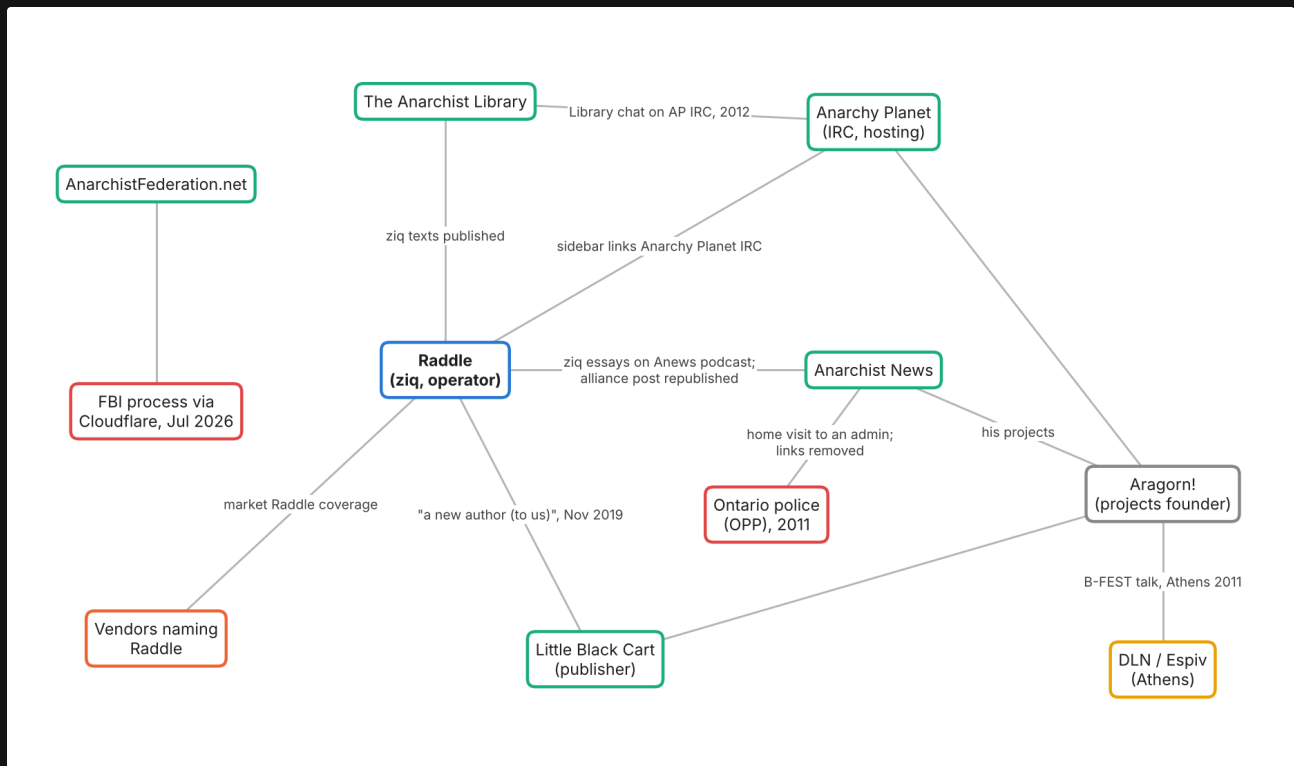


Figure 9. The publishing and hosting network around Raddle, with documented points of state pressure and commercial attention. Lines show documented links (links, publication, hosting); they do not show shared administration.

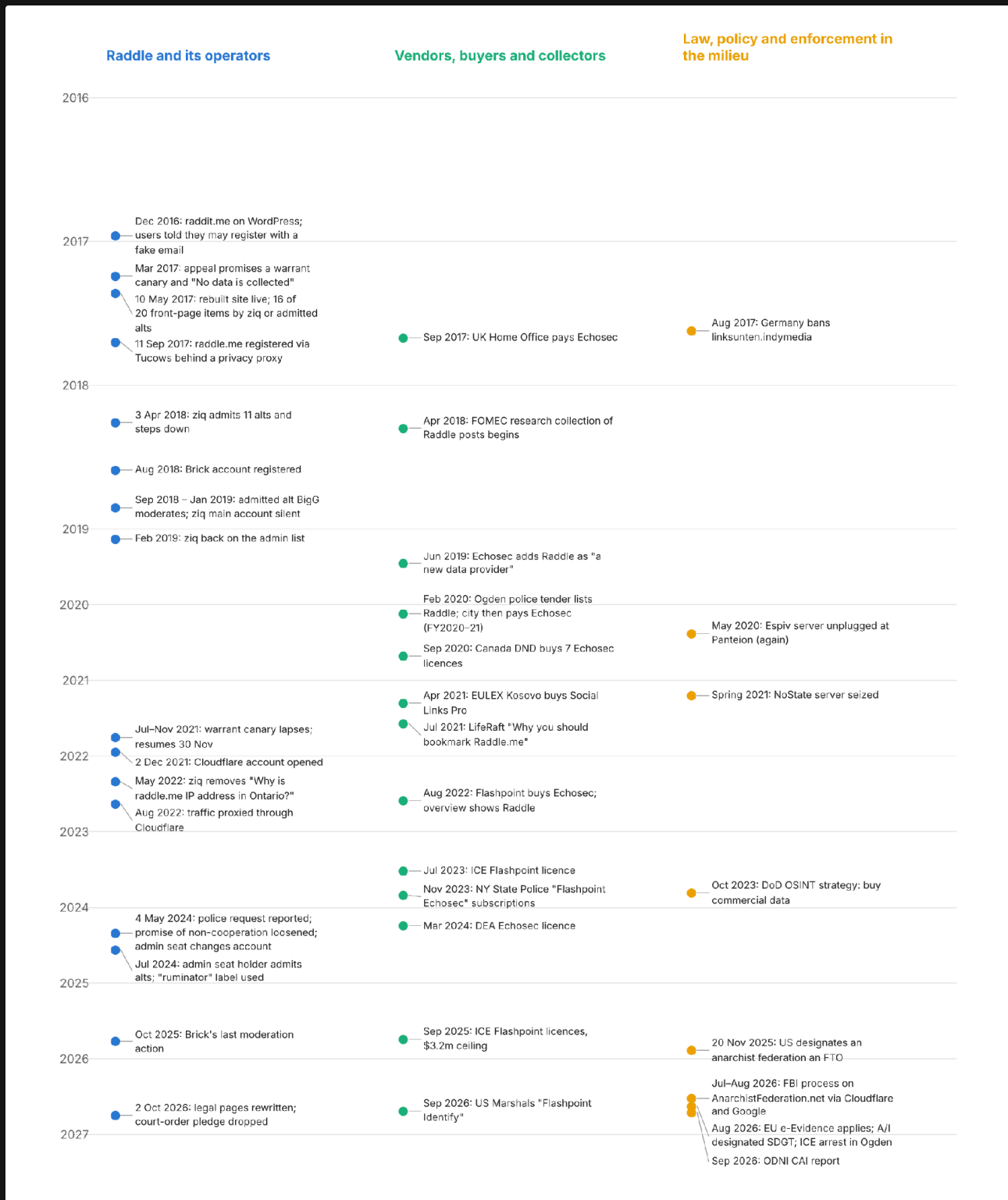


Figure 1. Timeline, 2016–2026: Riddle and its operators; vendors, buyers and collectors; law, policy and enforcement in the anarchist milieu.

2. The Platform Profile

In brief

- The software stores users' IP addresses on every action; administrators see them all and store none of their own.
- The public administrator list has not matched the accounts that held administrator rights, and one listed name was held by five accounts.
- Traffic passes through Cloudflare; the cooperation promise was loosened on the day ziq reported a police request.
- ziq has run undisclosed accounts since launch, including as moderators.
- After questions were sent in October 2026, ziq added a rule against calling accounts alts and back-dated the record of it.

2.1 What the platform holds

Raddle declares version 2.2.2 of Postmill.²⁷ In that code, an IP address is stored with every submission, comment, vote, private message and account registration.

Stored addresses are removed only when an operator runs a pruning command, present in Postmill since at least January 2018.²⁸ The command has no default age, so retention is whatever the operator decides each time it is run.²⁹

The platform's own statements on retention differ. On 13 October 2026 the live pages said both of the following.³⁰

- “IP addresses are stored for all Users for a period of 7 days”;
- “We have no private user data to hand over.”

The first FAQ, of June 2017, said addresses were kept “only for 7 days” and named two administrators, located in “West Asia and Scandinavia.”³¹ The later FAQ gives 24 hours and three administrators.³²

2.2 Who can see it

In Postmill, the administrator-only ban form is pre-filled with every IP address the user has ever used.³³ Administrators have no IP address stored with their own posts, comments, votes or messages. Since November 2017 the same has applied to users on an IP allowlist (“trusted” users).³⁴ Users asked for allowlisting in public threads, and the holders of the administrator seat described below, ziq and other administrators granted it; grants do not appear in the moderation log.³⁵ Administrators therefore see the most, leave the least trace, and decide who else leaves none.

The moderation log records whether each actor held site-administrator rights at the moment of each action.³⁶ Read against the public administrator changelog in the terms of service,³⁷ the log shows a wider administrator group than the public list (Figure 3). From mid-2018 onward:

- **emma** left the public list in March 2018 and was never re-added, yet took 637 actions with administrator rights from May 2019 to 30 August 2026.
- **Never on the public list under any name:** Hibiscus_Syrup (43 actions, October 2020 to March 2021) and not_active (one action, February 2022).
- In every year from 2020 to 2026, administrator rights were exercised by at least one account that was not on the public list under its own name at the time.³⁸

A second instrument, independent of the log, gives the same result. Postmill draws a wrench icon on a profile only when the account holds administrator rights at the moment the page is served. The icon appears on emma’s profile in all eleven archived captures from August 2020 to June 2024 and on the live page of 21 October 2026, and on mofongo’s in all nineteen captures from 2020 to 2024. It appears on none of twelve captures of GrimWillow’s profile from 2020 to 2024, although the administrators page named GrimWillow in those years.³⁹ The published list named an account without the rights and omitted two that had them.

One public name, five accounts. The name “Tequila_Wolf” sat on the public administrator list from 2017 to May 2024. Archived user pages, the log and Postmill’s rename function show that the name was held by five different accounts in turn, each earlier holder renamed when the next took the name:⁴⁰

Holder	Registered	Held the name	Name today	Administrator actions
Account A	20 Jun 2017	2017 to at least late Sep 2020	foundstone (earlier An_Old_Big_Tree)	1,580 (Dec 2017 – 13 Oct 2020)
Account B	31 Mar 2021	2021 to early 2022; handled allowlist requests (“Added!”)	Tequilx_Wolf (“retired account”)	none logged
Account “Marco”	2021 or earlier	early 2022 to about 4–6 May 2024	stacat	345 (Apr 2021 – Apr 2024)
Account C	6 May 2024, two days after “u/Tequila_Wolf left the list of admins”	by 26 Jun 2024 to at least 27 Nov 2024; administrator rights from between 26 Jun and 17 Jul 2024	triangle	47 (Jul 2024 – Mar 2025)
Account D	28 Aug 2025	2025 to now; no administrator icon on 21 Oct 2026	Tequila_Wolf	—

The public administrator name "Tequila_Wolf": which account held it

- 1 13–14 Oct 2020: account A acts for the last time; Hibiscus_Syrup acts the next day
- 2 4 May 2024: ziq reports a police request; changelog says "Tequila_Wolf left"; cooperation clause loosened
- 3 6 May 2024: account C registered; later holds the name
- 4 28 Jun 2024: the named administrator list is replaced by role descriptions
- 5 13 Jul 2024: the holder of the name says the admin keeps alternate accounts
- 6 28 Aug 2025: account D registered; holds the name now

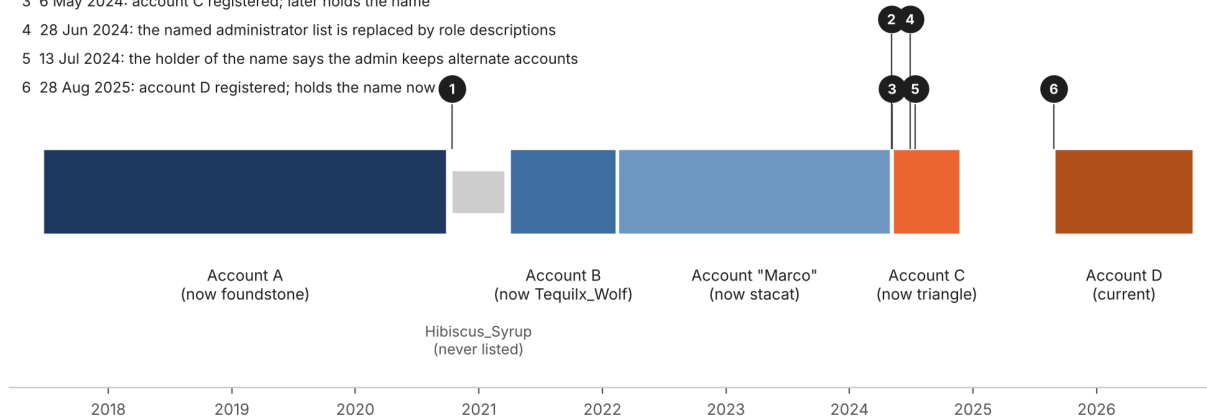


Figure 10. The public administrator name “Tequila_Wolf” and the five accounts that held it, with the events around each handover.

Between accounts A and B, administrator rights passed to Hibiscus_Syrup, created about 12 October 2020. It took its first administrator action on 14 October 2020, the day after account A’s last, and acted until March 2021. Writing as Hibiscus_Syrup, it referred to account A’s essays as “written by someone.”⁴¹

The public changelog records none of these handovers. On 28 June 2024, two days after account C was first seen holding the name, the administrators page replaced its list of named administrators with descriptions of roles.⁴² It still names no one.

The practice is not confined to this name. The name “kin” belonged to an account registered in June 2020 until at least 31 July 2024. By 25 November 2024 it was carried by an account registered in April 2024, which was later renamed “empty.”⁴³

On 13 July 2024, in a thread on the site’s rules, the account then named Tequila_Wolf wrote:⁴⁴

I have alts for a few reasons, from security, to the way I don’t want everything I say to be said with the weight of a site admin, to other reasons I will leave out.

ziq replied that “people don’t realize the target on your back when you’re an admin. sometimes you don’t want everything to be heavily scrutinized.”⁴⁵

The terms promise that “The administrators of this site will not provide any private data ... without a court-ordered warrant.”⁴⁶ That promise attaches to a list that did not name everyone holding the rights the promise is about, and to a name that did not stand for one person.

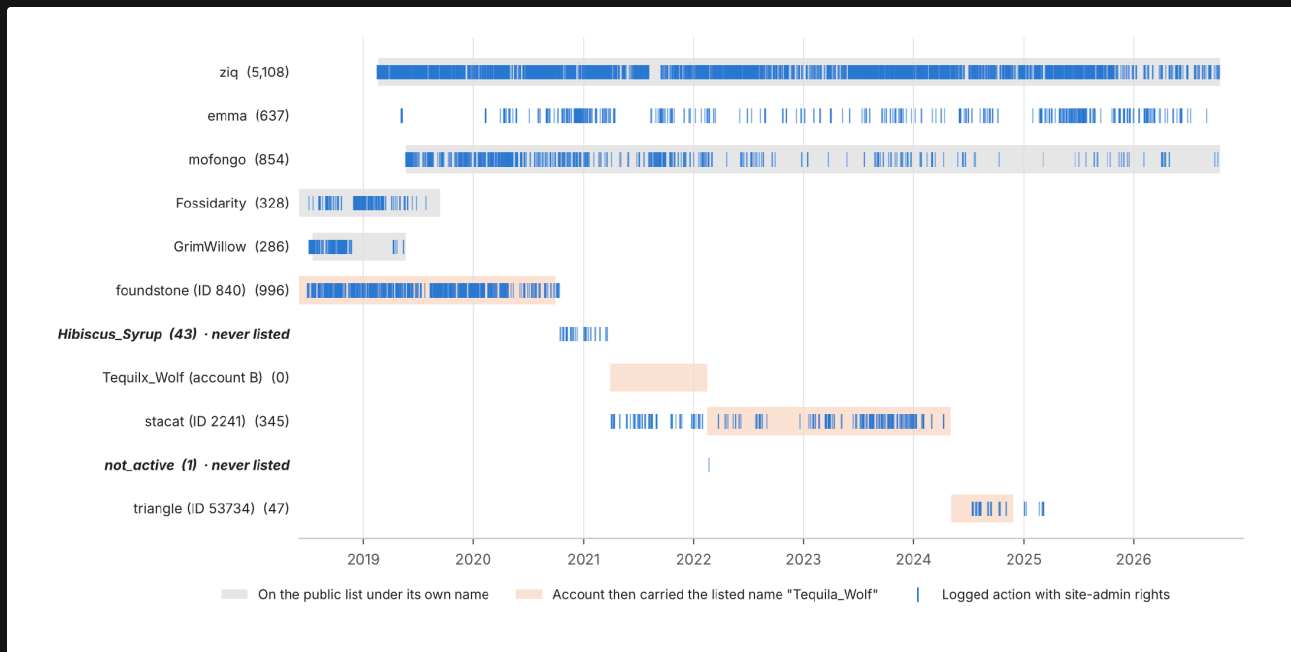


Figure 3. Accounts that used site-administrator rights in the moderation log, July 2018 to October 2026 (ticks), against periods on the public administrator list under their own name (grey bars) and periods in which the account carried the listed name “Tequila_Wolf” (peach bars). Bold italic names never appeared on the public list. Counts are actions from July 2018; all-time counts are in Annex B.

2.3 How traffic and records leave the platform

Figure 2 shows the four routes by which data about Raddle users can reach a third party.

1. **Administrators.** The ban form exposes every IP address a user has used (Section 2.2).
2. **Cloudflare.** On 2 December 2021 ziq announced a move behind Cloudflare, a US company: “Not much choice since the DDoS isn’t stopping.”⁴⁷ The Cloudflare account and the first Cloudflare certificate date from that day; the site’s traffic began to pass through Cloudflare’s network in about August 2022.⁴⁸ Cloudflare’s web-analytics beacon, which sends page-view data to cloudflareinsights.com, was added between August 2025 and January 2026 and loaded on every page read on 13 October 2026.⁴⁹ Cloudflare enables the beacon by default for sites on its free plan.⁵⁰ The privacy policy first named Cloudflare on 2 October 2026. The welcome page’s “Zero tracking or analytics. We don’t even track hits.” has stayed unchanged.⁵¹
3. **The hosting provider.** Passive DNS records place the pre-Cloudflare origin on DigitalOcean, a US company, in its Amsterdam data centre.⁵² The platform’s mail server, mail2.raddle.me, sits at a DigitalOcean address; it did not accept a letter sent on 19 October 2026, which bounced two days later.⁵³ The operator’s description of hosting changed from “VPS in Amsterdam” (2019–23) to “European Union” (4 May 2024), “Various locations in the EU” (28 June 2024) and “Netherlands and Finland” (10 October 2024).⁵⁴ DigitalOcean’s law-enforcement guidelines say a US search warrant reaches the contents of a customer’s virtual machine, and that foreign authorities must proceed through US legal process.⁵⁵

1. **The registration layer.** Tucows says it accepts subpoenas and warrants from Canadian, Danish, German or US authorities.⁵⁶ Contact Privacy reserves discretion to disclose data “in the good faith belief that disclosure is necessary to further determination of an alleged breach of a law.”⁵⁷

Raddle’s warrant canary covers US National Security Letters, Foreign Intelligence Surveillance Court orders and gag orders.⁵⁸ It lapsed for about five months in 2021, between July and November, and resumed with a notice that it “will now be updated on an irregular basis.”⁵⁹ Every canary since October 2017 has been signed with the same key, ziq’s, including those posted by other administrators during ziq’s 2018–19 absence. The canary live on 21 October 2026 verifies against that key and was signed on 2 October 2026.⁶⁰ A member asked in about 2023 why the canary still stated May 2023; the next signed canary in the archive is of June 2024, which may indicate a second long gap.⁶¹

The operator’s promise about legal process has changed in three steps.⁶²

1. From 2018 to early 2024 the terms said the administrators “will not cooperate with any court, government or law enforcement agency.”
2. On 4 May 2024, in revisions ziq made between 20:32 and 20:58 UTC, this became a promise not to “provide any private data ... without a court-ordered warrant that is jurisdictionally valid and without notifying the userbase.”
3. On 2 October 2026, 45 days after the EU e-Evidence Regulation began to apply,⁶³ notice became conditional (“whenever legally permitted”) and the pledge to delete the site rather than comply with a court order was removed.

At 10:40 UTC on 4 May 2024, ten hours before the first change, ziq posted “Transparency: Received a legal request from the police a few days ago.” ziq wrote that police had sought “identifying data of a throwaway spam account” linked to bomb threats, and that the request was declined.⁶⁴ The post establishes, on the operator’s own word, that state pressure reached the platform. The statement that nothing was handed over is the operator’s claim. It is not accepted at face value here, for two reasons: ziq’s statements about ziq’s own conduct have repeatedly been contradicted by the record (Section 2.4), and the same evening ziq replaced the promise of non-cooperation with a promise conditional on a warrant, which may indicate that cooperation had become possible. The terms’ changelog recorded that day only that “u/Tequila_Wolf left the list of admins.”⁶⁵ Six weeks earlier, on 26 March 2024, the privacy policy had been edited without a changelog entry, removing the promise to give 14 days’ notice of changes on the main page and by email.⁶⁶ A terms changelog line dated 26 October 2020 was later rewritten to claim wording that came from edits made a month afterwards.⁶⁷

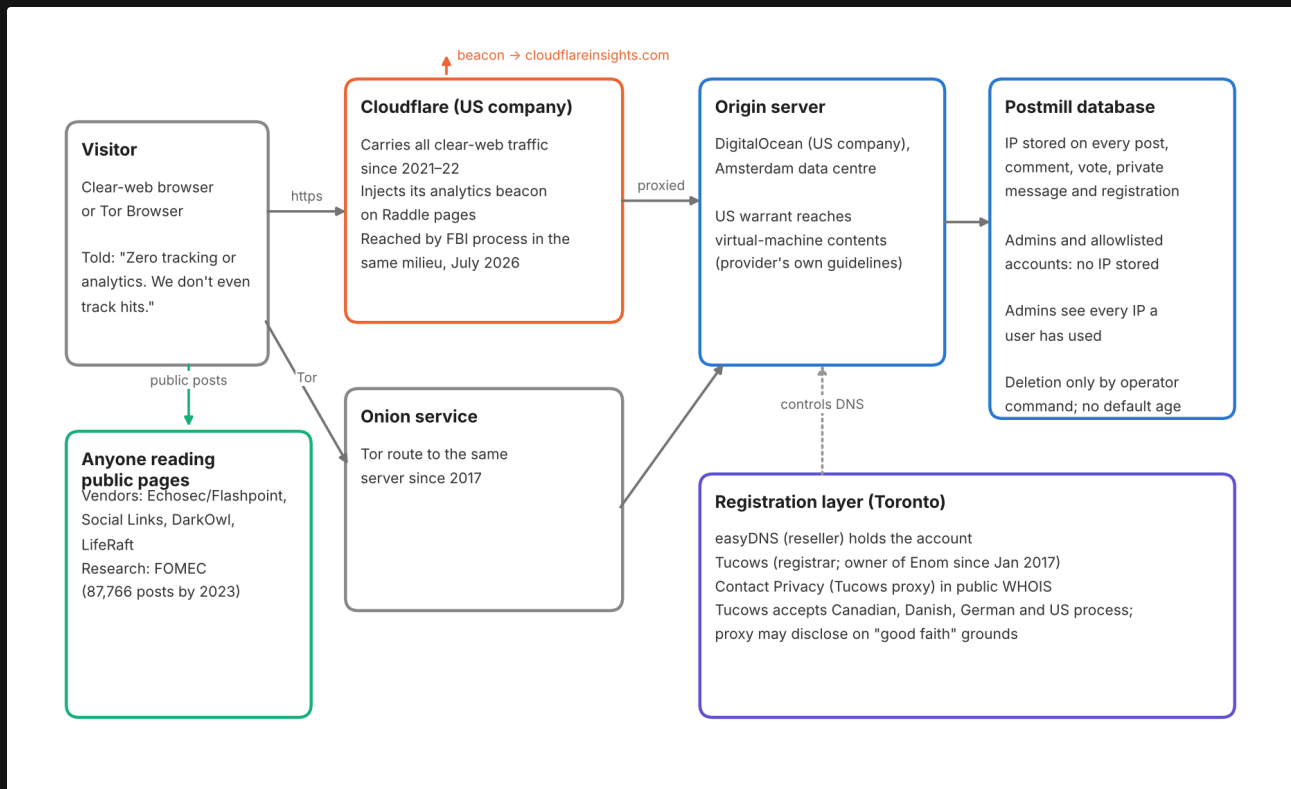


Figure 2. How a visit to Raddle and the data it generates pass through third parties. Each third party named is subject to legal process in at least one jurisdiction.

2.4 The operator's accounts

On launch day, 10 May 2017, the rebuilt site's front page held twenty items. Sixteen came from ziq or from accounts ziq later admitted to: radditnews 5, KarlMarx 4, Defasher 4, Cherimoya 2 and ziq 1.⁶⁸ On the WordPress front page of 4 February 2017, ten of 28 items came from the same group.⁶⁹

On 3 April 2018 ziq posted "I'm stepping down as admin because of some shit I did."⁷⁰ In that post ziq named eleven accounts as ziq's own:

cherimoya, avocado, karlmarx, binary, radditnews, Chomskyist, BigGeorge, Kylie, postcivver, defasher and spock

ziq described using "a strawman (spock)" and defasher to create "divisions between raddle's userbase."⁷¹ ziq wrote: "I'll keep paying the bills but won't be involved in administration or moderating the site at all." Tequila_Wolf, then an administrator, set out the new roles, listing ziq as "site registered and maintained/paid for in their name."

The record after the step-down (Figure 5):

- ziq's main account took no logged action from 3 April 2018 to 16 February 2019.⁷²
- In that gap BigG, an alternate account ziq has acknowledged, took 287 moderation actions, peaking in September 2018.
- On 23 January 2019 BigG banned a user with the reason "cop."

- ziq returned to the administrator list on 18 February 2019.⁷³
- The account Brick was registered on 2 August 2018, four months after the step-down.⁷⁴ It moderated from February 2022 to October 2025. Its actions included nine deletions of ziq’s own placeholder posts and, on 11 February 2022, a permanent ban for a “Pattern of harassment and badjacketing,” that is, falsely calling someone an informant.
- In about 2024–25 ziq told a member, “I’m not using any alts,” and referred to “my old alts like brick,” used “to make a point I can’t make with an admin account because of the power imbalance.”⁷⁵
- Brick is attributed to ziq on that statement and on the overlap in the log.

Accounts ziq admitted were active in the forum’s most sensitive corner. In September 2017 raddit.me hosted Useful_info, a forum whose sidebar read “Post your useful info about horrible people! Post ’em up, Take ’em down! Fascists, rapists only. Not their relatives. No SSNs.” Its moderators were Wrestitaway and Defasher, an account ziq admitted in 2018. Cherimoya, another admitted account, posted a “Dox” of a named individual there, and the account then named Tequila_Wolf posted “Is Doxxing Ever Okay? (Yep).”⁷⁶

In July 2024 a member alleged that the accounts gokuscloud and factotum were ziq’s.⁷⁷ This assessment attributes both to ziq. In a thread of that month, gokuscloud defended “/u/ziq” in the third person and attacked the moderators of the site ziq administers.

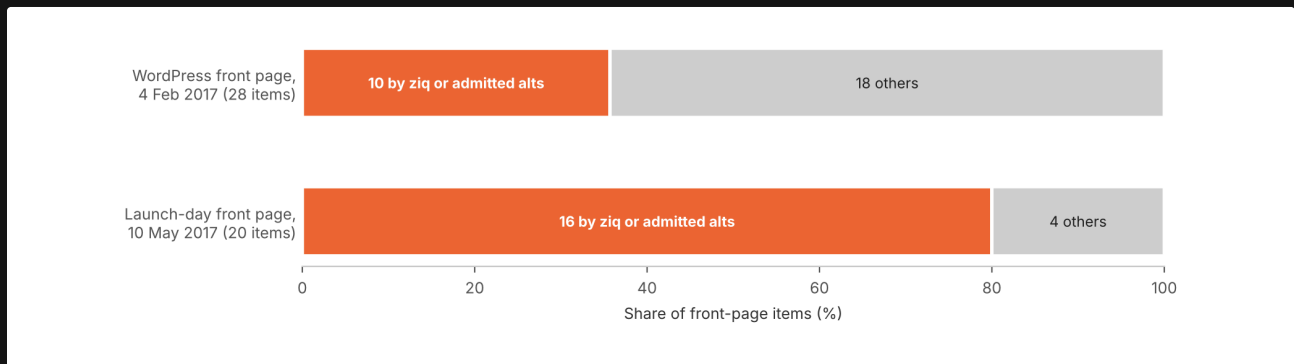


Figure 4. Share of front-page items written by ziq or by accounts ziq admitted in April 2018, on the WordPress site (February 2017) and on the rebuilt site’s launch day (10 May 2017).

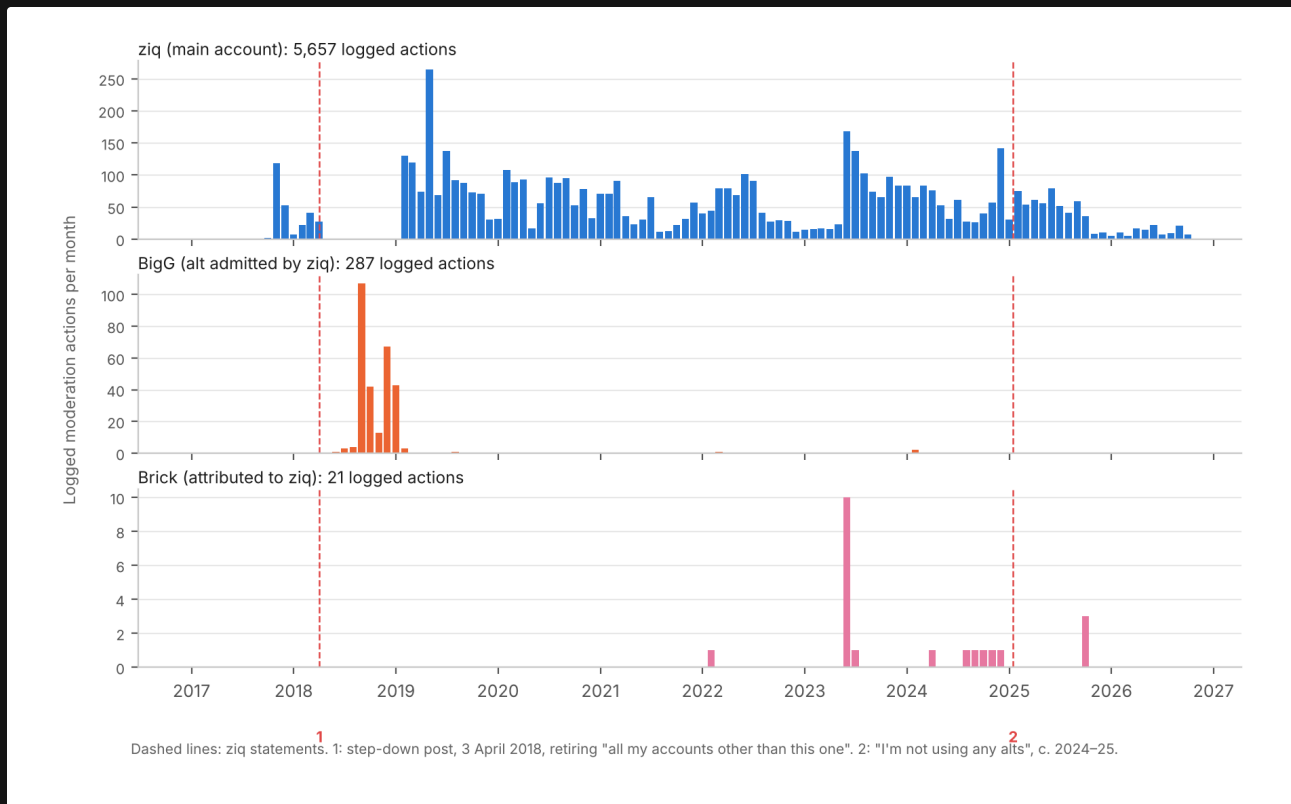


Figure 5. Monthly moderation actions by ziq's main account, by BigG (admitted by ziq) and by Brick (attributed to ziq), October 2017 to October 2026, with two of ziq's statements about account use.

2.5 How the platform is moderated

The public moderation log was read in full: 16,565 entries from 23 October 2017 to 13 October 2026.⁷⁸ ziq took 5,657 of them, about a third, on 1,570 separate days. Across all 16,253 removals, bans and locks:

- 45% give a spam or bot reason;
- 17% give no reason;
- 5% carry an alt, sock, ban-evasion or troll label.

The same measures were applied to two sets of posts selected by words in their titles (Figure 6):⁷⁹

- **Criticism of the operators (367 removals).** 49% gave no reason and 14% carried an alt or ban-evasion label. Of 80 removals of posts naming ziq, ziq took 31. They include "Please explain these serious allegations ziq and tequila_wolf...", which ziq deleted twice on 8 September 2024, the day its author's account was registered, as "ban evasion, harassment, spreading smears posted by a literal cop."⁸⁰
- **Surveillance, police and security topics (201 removals).** These matched the base rate: 54% spam, 24% no reason, 2% alt label.

From 13 July 2024 the operators used a new removal reason, "ruminator," on 131 actions against 44 accounts they treated as one person; ziq took 85 of them.⁸¹ The label was used to remove questions about the operators' own account use, including a post titled "Accountability goes all ways," which the

administrator triangle removed the day it was posted. Administrators can see every IP address a user has used, which may indicate how 44 accounts were linked to one person.⁸²

The question of operator alternate accounts has itself been moderated:⁸³

- In 2019 a post titled “Ziq is still using sockpuppets and they are covering it up” was removed as “Dox.”
- In July 2024 answers to “How do regular users identify alts?” were removed as “ruminator” by the account then named Tequila_Wolf, by subrosa and by ziq, and ziq locked the thread.
- On 26 November 2024 ziq locked an April 2018 thread in which ziq had written “I’m not even the only admin who used alts.”
- In December 2024 a user was banned with the reason “no alts in meta.”

Two removals bear directly on the surveillance question:

- On 4 May 2022 a member asked, “Why is raddle.me IP address in Ontario, Canada?” ziq replied, “that ip isn’t in canada, it’s in NL. click the ip,” and removed the post one minute later as “bad reading comprehension.”⁸⁴
- In November 2023 ziq removed a post titled “Where to share fired cops personal info?” as “Attempted entrapment.”⁸⁵

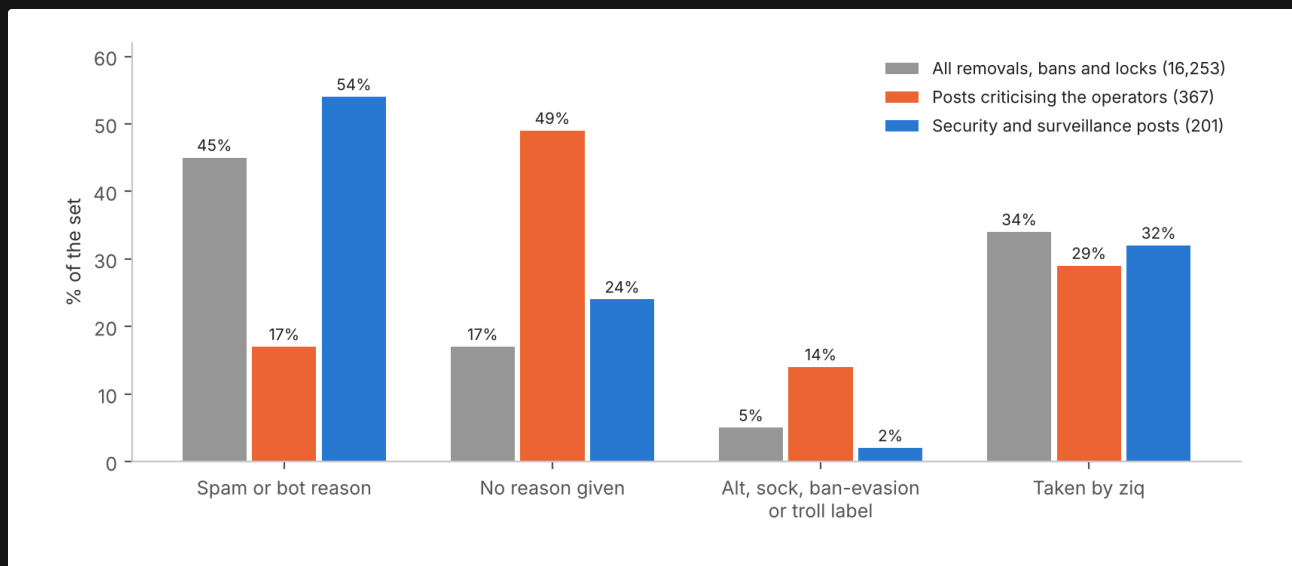


Figure 6. Reasons and actors for removals in the Raddle moderation log: all removals, bans and locks; posts criticising the operators; and posts on surveillance and security. Sets are defined by words in post titles.

2.6 Conduct after contact, October 2026

Between 15 and 18 October 2026, before any letter was sent, several members described receiving moderator roles on several forums at once. ziq told one, “let me know if there are other forums you want to moderate.” One of those members’ posts carries the “[admin]” flag, which the software lets only an administrator set; the member holds no administrator rights.⁸⁶

On 19 October questions were sent by email to ziq, emma, Flashpoint (through its press contact) and the Anarchist News collective, with a deadline of 21 October. The copy to ziq@raddle.me bounced after the platform's mail server failed to answer for two days; the copy to ziq's Proton Mail address was delivered. No recipient replied by the deadline.⁸⁷

At 12:59 UTC on 20 October, about 24 hours after the first letters, ziq posted "New ToS Section: Take Security Culture Seriously."⁸⁸ The section tells users, among other things: "Do not treat alternate accounts as inherently suspicious or baselessly accuse people of being 'alts' or 'sockpuppets'." The terms changelog records the section as "updated on October 10, 2026." A dated capture of the terms at 12:36 UTC on 19 October ends at the 2 October entry and shows no such section.⁸⁹ Replying in the thread, the administrator mofongo wrote, "I totally missed that."

The platform was offline from about 05:34 to 11:46 UTC on 18 October, and again from 00:44 to 17:09 UTC on 21 October.⁹⁰ The second outage followed the PHP project's notice of a critical security release.⁹¹ The site's maintenance notices said it was waiting for updated Docker images. Those images were built and published by emma's Codeberg account: nine manual runs on 21 October, the last finishing at 16:59 UTC, about ten minutes before the site answered again.⁹² The site came back on PHP 8.5.12. Regressions reported against that release, and a follow-up patch, show that it did not fully close the flaws.⁹³ The developer who holds unlisted administrator rights is therefore also the person whose builds the platform depends on to run.

The rebuilt images carry Postmill v2.2.2, although v2.2.3 has been published since 19 July 2026 and emma wrote in August that fixes would not apply "until the server is upgraded."⁹⁴ The PHP release they run is publicly known to be incomplete.⁹⁵ We assess that returning the site on an outdated application version and a release known to be incomplete **may indicate** that the operators do not in fact prioritise the site's security (**low to moderate confidence**). Against that reading, 8.5.12 was the only patched PHP release on 21 October, and the operators took the site offline rather than run it unpatched. Whether the site moves off 8.5.12 once a complete fix is released will test the reading.

The warrant canary was not re-signed after the letters or after either outage. On 21 October it still carried its 2 October date.⁹⁶

3. Comparative Analysis

In brief

- Raddle matches every column of the comparative matrix except a confirmed state agent inside.
- The May 2024 handover of the administrator name after a police request has the shape of the Childs Play and Hansa takeovers.
- ziq’s conduct reproduces the signature of movement infiltrators; it also fits a personal or factional operator.
- Commercial collection of Raddle for government buyers is the best-documented state relationship.
- The FBI’s own records call Flashpoint, a vendor that names Raddle, a “social exploitation tool” for monitoring forums.

3.1 Framework

This section compares Raddle with four kinds of operation that have targeted, entered or exploited online platforms and political movements:

1. **Agency-run platforms.** An intelligence or law-enforcement body runs a platform, or takes one over and keeps it running, so that it can collect from the users.
2. **Informants and undercover officers in movements.** A person reporting to the state takes part in a movement, sometimes in a position of trust over its money, communications or publishing.
3. **Online covert action and personas.** A state body uses false online identities to watch, steer, divide or disrupt a community.
4. **Ideological, factional and commercial actors.** Non-state parties watch or manipulate a community for their own reasons: hostile forums, factions inside the movement, security vendors and researchers.

Each case is scored against ten indicators drawn from the documented features of these operations.

Figure 8 sets out the result. Solid squares mark an indicator documented for that case, pale squares one documented in part, and the hatched square with a question mark an indicator for which Raddle shows signs that are not confirmed.

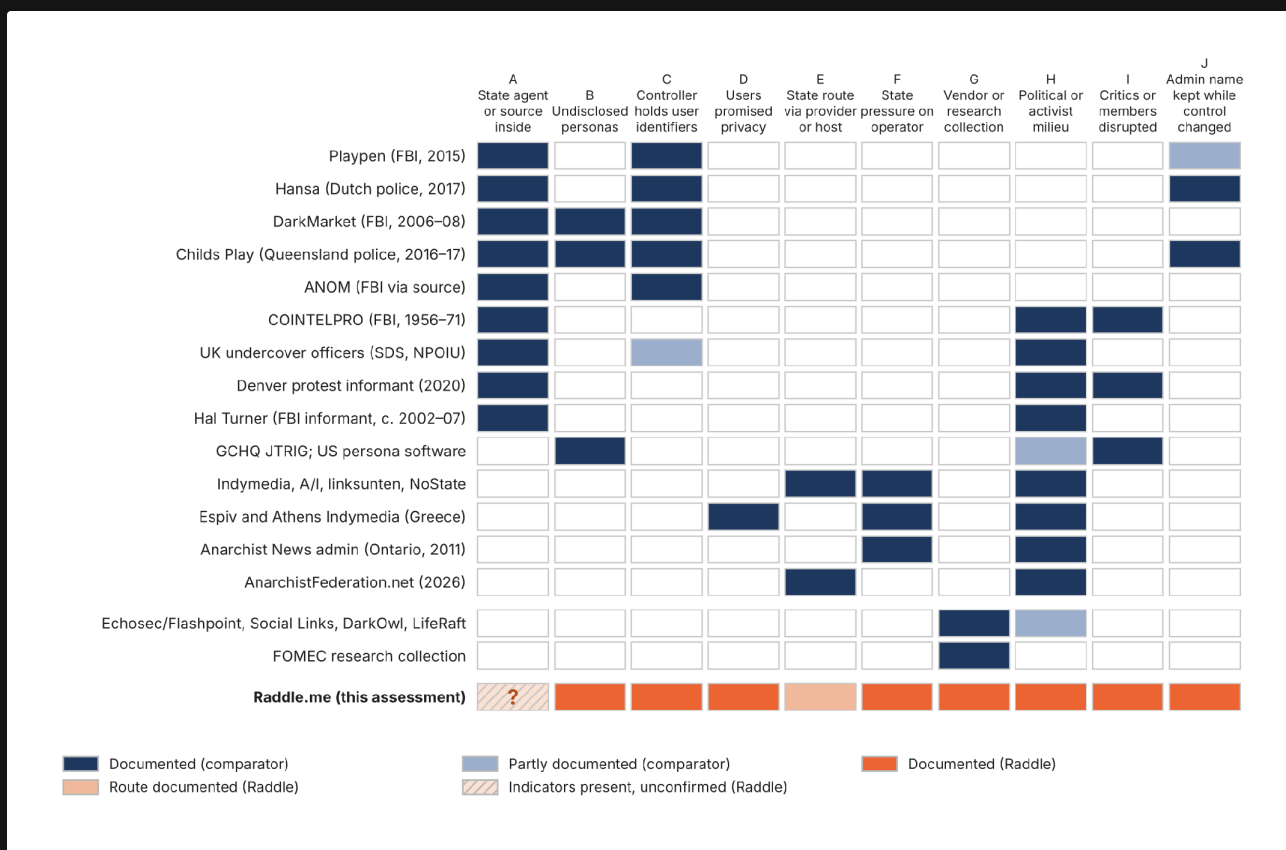


Figure 8. Comparative matrix. Columns: A, a state agent or source inside the platform or group; B, undisclosed personas operated by the controller; C, the controller holds user identifiers; D, users were promised privacy; E, a documented state route through a provider or host; F, documented state pressure on an operator; G, vendor or research collection of the content; H, a political or activist milieu; I, critics or members disrupted; J, an administrator identity kept while control of it changed. Raddle's column E is marked in part because the route is documented and its use is not. Column F is marked from ziq's own report of a police request in 2024. Column A is marked as unconfirmed because of the May 2024 change of hands behind the administrator name (Section 3.2).

Raddle is documented on eight of the ten indicators, partly documented on a ninth, and shows unconfirmed signs on the tenth. Read row by row:

- With the **agency-run platforms** it shares personas, controller-held identifiers, privacy promises and, since the 2024 handover, an administrator name kept while the account behind it changed (columns B, C, D and J).
- With the **movement-infiltration cases** it shares a political milieu and disrupted critics (H and I).
- With the **provider and pressure cases** it shares state pressure on the operator, which ziq reported in 2024 (F), and a documented provider route (E).
- With the **vendor and research cases** it shares commercial collection (G).

Column A, a confirmed state agent or source inside the platform, is what would turn this resemblance into a confirmed operation. Raddle is the only row in the matrix that matches every other column, and the May 2024 sequence is the point at which column A is closest to being met.

3.2 Platforms run or taken over by agencies

Five documented cases show agencies running platforms to collect from users.

- **DarkMarket (2006–2008).** An FBI agent served as a moderator and administrator of a carding forum under the persona “Master Splyntr” and gathered members’ IP addresses.⁹⁷
- **Playpen (2015).** The FBI kept a seized child-abuse site running for about two weeks and used a hacking tool to identify visitors. The First Circuit rejected the argument that running the site was “outrageous government conduct.”⁹⁸
- **Childs Play (2016–2017).** Australia’s Task Force Argos ran a child-abuse site for about eleven months while posing as its arrested original administrator.⁹⁹
- **Hansa (2017).** After German police arrested its administrators, Dutch police took over the darknet market and ran it for about a month under the existing administrator identities before closing it.¹⁰⁰
- **ANOM (2018–2021).** An encrypted-phone platform was offered to the FBI by a developer facing charges and run as a collection system. A Lithuanian court order let police copy data from a server in that country and forward it to the FBI; the order did not say the platform was FBI-run.¹⁰¹

Three features recur.

- **Persona continuity.** In Childs Play and Hansa the platform’s users dealt with a familiar administrator identity after an agency had taken control of it, and in DarkMarket with a trusted persona the agency built. The persona was the asset.
- **A trigger in law enforcement.** In Childs Play and Hansa the change of control followed directly on police contact with the original administrators.
- **Identifier capture at the administrator level.** Each operation’s value lay in what the platform’s controllers could see: IP addresses, messages and account links.
- **Legal survivability.** Courts in the United States have upheld convictions built on agency-run platforms, and the Lithuanian order shows collection routed through a third country.

Comparison with Raddle.

- Raddle’s software gives administrators the same class of data these operations sought: every IP address a user has used, linked to every post, vote and private message (Section 2.1).
- Raddle has a documented persona practice at the administrator level. ziq ran eleven admitted accounts, used two of them to create “divisions,” and admitted and attributed accounts carried out staff work while ziq’s main account was inactive (Section 2.4).
- Raddle shows persona continuity of the Childs Play kind at the level of the administrator seat. The listed name “Tequila_Wolf” stood unchanged on the public list while five different accounts held it in turn, each handover leaving the earlier account renamed and the public changelog silent (Section 2.2). Who stood behind each account is outside the scope of this assessment; the structural point is that users dealing with a familiar administrator name were not dealing with one continuous account.
- In every agency-run case, the platform’s targets were criminal markets or child abuse. Raddle’s users are political.

The May 2024 sequence read against the takeover cases.

Takeover pattern (Childs Play, Hansa)	Raddle, April–July 2024
Law enforcement reaches the platform’s administrators	Late April: police seek identifying data about a user, by ziq’s own account ¹⁰²
The original administrator stops acting	4 May: “u/Tequila_Wolf left the list of admins”; the account holding the name since 2022 makes its last administrator actions in April and is later renamed ¹⁰³
A controller continues under the familiar identity	6 May: a new account is registered; by 26 June it carries the name Tequila_Wolf, and between 26 June and 17 July it gains administrator rights ¹⁰⁴
Users are not told	The changelog records a departure, not an arrival; on 28 June the named administrator list is removed ¹⁰⁵
Legal commitments shift	4 May evening: non-cooperation becomes a warrant condition ¹⁰⁶

The new holder’s own explanation, on 13 July 2024, was that the admin keeps alternate accounts for reasons including “security” and “other reasons I will leave out.”¹⁰⁷ That explanation comes from the account under question and is treated as a claim.

The record has other explanations available: an administrator stepping back and a volunteer replacing them, or the existing team moving the name to a fresh account for security. Two features weigh against a purely routine reading. The handover followed a police request within days, and it was carried out so that users saw continuity. The earlier handovers of the name, in 2020–22, show that the team had a habit of passing the name between accounts, which is itself the property an outside placement would exploit.

Assessment. We assess with **high confidence** that Raddle’s architecture and governance would support the kind of collection these operations achieved, without any change to the software. We assess with **low to moderate confidence** that the May 2024 sequence may indicate the deliberate placement of a new person in an administrator role after state contact, by agreement with the operator or without it; it is the strongest single indicator of infiltration in the record. We assess it **unlikely** that an agency has taken over the platform as a whole in the manner of these cases, because the founding operator, the software and the signing key have stayed continuous from 2017 to 2026. The dated breaks that fit the takeover pattern are discussed in Section 4.5:

- the 2021 canary lapse followed by the Cloudflare account;
- the cluster of March to June 2024 set out above;
- the 2 October 2026 rewrite of the legal pages.

The rotation of the administrator seat means that continuity of the founding operator is not continuity of everyone with administrator access.

3.3 Informants and undercover officers in movements

The closest historical parallels to Raddle’s milieu are long-term infiltrations of political movements.

- **COINTELPRO (1956–1971).** The Senate’s Church Committee documented FBI programmes that used informants inside political groups and that worked to discredit activists, including by making members appear to be informants (“snitch-jacketing”).¹⁰⁸
- **UK Special Demonstration Squad and National Public Order Intelligence Unit.** Evidence to the Undercover Policing Inquiry in March 2026 showed the officer known as HN3 targeting the Campaign Against Arms Trade from 2000 to 2005. HN3 was a signatory on the bank account of the campaign group Disarm DSEI and held its post-office box and access to its email.¹⁰⁹ Another officer, Mark Kennedy, worked in activist circles in Germany as well as Britain; a court in Schwerin found the German deployment “objectively illegal” in 2022.¹¹⁰
- **Germany.** A Hamburg state-police officer worked as a presenter and reporter at a community radio station from 2003 to 2006.¹¹¹ In 2026 the Interventionistische Linke in Bremen announced that one of its members had reported to state intelligence for about eight years.¹¹²
- **Hal Turner (c. 2002–2007).** A far-right radio and website operator served as an FBI informant for about five years. The FBI admonished Turner over the rhetoric in 2007 and kept using Turner; at trial Turner said the FBI had directed Turner to “ratchet up” the rhetoric.¹¹³ This is the closest documented case of an informant who ran a public political platform.
- **Denver (2020).** An FBI informant inside racial-justice protests in Denver pressed activists towards armed action, and reporting describes the informant casting suspicion on others in the movement.¹¹⁴
- **LulzSec (2011–2012).** The hacker Hector Monsegur (“Sabu”) worked under FBI supervision after his arrest, monitoring chats and soliciting evidence from associates.¹¹⁵

Three patterns recur across these cases.

1. **Positions of trust.** Infiltrators moved into roles that held a group’s money, mail, communications or publishing (HN3’s bank account, post-office box and email; the Hamburg radio role; Turner’s broadcasts).
2. **Agitation and division.** Several infiltrators raised the temperature of a movement or turned members against one another (COINTELPRO’s snitch-jacketing; Turner’s rhetoric; the Denver informant).
3. **Long tenure.** Deployments lasted five to ten years.

Comparison with Raddle.

- **Position of trust.** ziq holds every position of trust on Raddle: the domain, the server, the funding, administrator rights and the moderation of critics. ziq describes the role in the first person and says “There is no raddle collective.”¹¹⁶
- **Division.** ziq’s April 2018 admission described using alternate accounts to create “divisions between raddle’s userbase.”¹¹⁷ In 2024–25 ziq said “my old alts like brick” were used “to make a point I can’t make with an admin account because of the power imbalance.”¹¹⁸
- **Exposure of outsiders.** In September 2017 the site hosted Useful_info, a forum for posting personal information about “horrible people,” moderated by an account ziq admitted and used by another for a posted “Dox.”¹¹⁹ Collections of personal details gathered under movement banners are the material an infiltrator or a hostile collector most values.

- **The informant label.** Moderators on Raddle have used the informant label in both directions. BigG, an admitted alternate account, banned a user in January 2019 with the single word “cop.” Brick, an attributed alternate account, banned a user in 2022 for “badjacketing,” and ziq removed a post in November 2023 as “Attempted entrapment.”¹²⁰ On a platform where the administrator also runs undisclosed accounts, the power to decide who is called a cop and who is protected from being called one sits with a single person.
- **Tenure.** ziq has run the platform for nine and a half years.

Assessment. We assess with **high confidence** that ziq’s documented conduct reproduces the operational signature of movement infiltration as recorded in these cases: control of the group’s infrastructure, deliberate division through false identities, and control of who is labelled an informant. In the cases above, those behaviours were the work of state agents or sources. They are also the behaviours of an operator who wants to control a community for personal or factional reasons. The record fits both explanations. On it, a personal or factional motive is the simpler reading (**moderate confidence**).

3.4 State online covert action and personas

Governments have built programmes to run false online identities at scale.

- **GCHQ’s Joint Threat Research Intelligence Group (JTRIG).** Documents published in 2014 describe “Online Covert Action” using deception and messaging, logs of undercover agents talking with hackers, and a denial-of-service attack that JTRIG claimed drove about 80 percent of users out of a chat room used by Anonymous and LulzSec.¹²¹
- **US persona management.** A 2010 US Air Force solicitation sought software to let each operator run ten personas, with fifty licences. The stated use was foreign-language sites.¹²²
- **UK undercover online policing.** Her Majesty’s Inspectorate of Constabulary counted 3,466 undercover operations in England and Wales from October 2009 to September 2013 and devoted a section to undercover work online.¹²³
- **US rules.** The FBI’s investigative guide treats “undisclosed participation” by agents and informants in online groups as a regulated technique. Participation in political, religious, media or academic groups is classed as “sensitive,” and participation meant to influence a group needs legal review.¹²⁴

Comparison with Raddle. The documented persona practice on Raddle matches the technique these programmes describe.

- **Volume at launch.** On launch day, 10 May 2017, sixteen of the twenty front-page items came from ziq or from accounts ziq later admitted (Figure 4).¹²⁵
- **Staged argument.** ziq said one alternate account served as “a strawman.”¹²⁶
- **Third-person defence.** In July 2024 the attributed account gokuscloud defended “/u/ziq” in the third person.¹²⁷
- **Persona as moderator.** Admitted and attributed alternate accounts held moderation powers and used them for years after ziq said the practice had stopped (Figure 5).¹²⁸

- **Rotating identities behind a fixed name.** The listed administrator name “Tequila_Wolf” passed through five accounts, with each earlier account renamed (Section 2.2).¹²⁹ In July 2024 its holder wrote that the admin keeps alternate accounts so that not everything is “said with the weight of a site admin,” for reasons including “security” and “other reasons I will leave out”; ziq agreed.¹³⁰
- **Control of the subject.** Posts and threads asking about operator alternate accounts were removed, locked or answered with bans in 2019 and 2024 (Section 2.5).¹³¹

The persona programmes above were built to keep identities separate and consistent. Raddle’s alternate accounts were admitted publicly in 2018 and again in 2024 and repeatedly alleged by members. That record **may indicate** an operator acting without professional tradecraft. The administrator seat shows the opposite trait: a fixed public name kept stable while the accounts behind it changed, without public notice, over seven years. That **may indicate** deliberate management of how the administrator group appears to users.

Assessment. We assess with **high confidence** that persona use on Raddle is a governance practice and not occasional misuse, and that it extends beyond ziq to the administrator group as a whole. Its form matches state online covert action. The open admissions fit an amateur operator better than a professional programme; the seat rotation shows deliberate management of administrator identities (**moderate confidence** on both).

3.5 Factional and hostile non-state actors

Not every actor who watches or manipulates a political community works for a state.

- **Hostile forums.** Kiwi Farms, a forum known for harassment campaigns, opened a thread on raddit.me in March 2017, before the current software launched, and a second thread on Raddle in February 2020.¹³² Those threads show hostile outsiders following the platform and its operator from the start.
- **Factional control.** ziq’s own accounts of the alternate accounts frame them as weapons in internal disputes.¹³³ The moderation log shows criticism of the operators removed without a reason about three times as often as other content, and the “ruminator” label used to remove questions about the operators’ accounts (Section 2.5).¹³⁴
- **Insiders with unlisted rights.** Administrator rights were exercised by accounts absent from the public list under their own names at the time they used them, and the one listed name that looked stable, “Tequila_Wolf,” was held by five accounts in turn (Section 2.2).¹³⁵ Any of those accounts, under any controller, could see every IP address a user had used and could add users to the allowlist that exempts them from IP storage.

Comparison. Factional manipulation explains the pattern of moderation on Raddle at least as well as any state-direction model does. Section 2.5 found that removals of posts about surveillance, police and security ran at ordinary rates, while removals of posts criticising the operators ran at three times the rate. A state operation aimed at the movement would be expected to shape discussion of security. The removals instead shaped discussion of the operators. That pattern **may indicate** that the operator’s own standing, rather than an external tasking, drives moderation.

The insider route is a risk under either model. Unlisted administrator rights give any person behind those accounts the same view of user identifiers that an agency-run platform would give its controllers.

Assessment. We assess with **high confidence** that factional control by the operator is a documented feature of Raddle. We assess it **likely** that the operator’s personal and factional motives account for most of the moderation and persona record.

3.6 Commercial and research collection

The best-documented relationship between Raddle and the state runs through commercial vendors. Six vendors have named Raddle in their own material as a source they cover, and their products have been bought by government agencies in three countries and an EU mission (Figure 1).

What the vendors say.

- **Echosec Systems** recorded in its product changelog for June 2019: “Echosec has a new data provider: Raddle.me.”¹³⁶ Its blog post of 9 July 2019 called Raddle “a new data provider in the Echosec platform,” “home to extensive shoplifting forums,” that “should be bookmarked by all retail security teams.”¹³⁷ By 2021 the post read “a data source in the Echosec platform” and showed the product with a source selector set to “RADDLE.me” and a search for “Shoplifting.”¹³⁸ Echosec’s monitoring pages listed Raddle among its open-web sources.¹³⁹ An Echosec platform overview, published by Flashpoint in August 2022, lists Raddle under data sources and says the company focuses “on crawling international data sources that are highly relevant to security and intelligence use cases.”¹⁴⁰
- **Flashpoint** advertised in its review of 2021: “In addition to Reddit, Gab, MeWe, Raddle, 4chan etc., view Twitter data to identify potential threats.”¹⁴¹ Flashpoint acquired Echosec on 3 August 2022.¹⁴²
- **Social Links** offers “full anonymous access to more than 30 popular Darknet resources such as Dread, 8chan, Raddle,” and lists law-enforcement agencies and intelligence analysts among its typical users.¹⁴³
- **LifeRaft** told loss-prevention staff in 2021 and 2024 why they “should bookmark Raddle.me” and reproduced users’ posts about thefts as “discovered by Navigator,” its own product.¹⁴⁴ LifeRaft’s product embeds DarkOwl’s dark-web data, which **may indicate** that some of its Raddle content arrived through DarkOwl.
- **DarkOwl** reproduced two Raddle comments with their onion address in April 2020 and published a search of its archive for the handle Tequila_Wolf, the same handle as a Raddle administrator listed at the time.¹⁴⁵
- **Maltego**, through the Social Links Pro add-on, named Raddle among its sources by January 2023, and still did in October 2026. LifeRaft’s “What is Raddle.me” page returned an error on 21 October 2026; its earliest archived copy is of November 2024.¹⁴⁶
- **Open-source tools.** Raddle has been added to free investigative tools: a ProjectDiscovery nuclei template for username checks (February 2023), a gallery-dl extractor for Postmill sites (December 2023) and the WhatsMyName username list (by 2025).¹⁴⁷ Account histories on Raddle can now be checked by anyone running these tools.

- **Retail and security consultants.** A Paladin Risk Solutions white paper of December 2019 and a June 2020 webinar by the Loss Prevention Research Council and Walmart Global Investigations, hosted by the Retail Industry Leaders Association, both point security teams at Raddle.¹⁴⁸
- **Academic collection.** A Youngstown State University project, Frames of Misinformation, Extremism, and Conspiracism, held 56,091 Raddle posts in its January 2023 report and 87,766 in June 2023.¹⁴⁹ The National Institute of Justice funded a related study of “violence and accelerationism” built on that project, with \$449,897.¹⁵⁰

Who buys the tools. The following buyers have purchased products from vendors that named Raddle as a source:

Buyer	Product	Date	Value
UK Home Office	Echosec (card payment)	Sep 2017	£853.24
ICE headquarters	EJ2 Communications (Flashpoint): online social-network and “dark web” data and analysis	Aug 2014	\$149,000 obligated
Canada, Department of National Defence	Echosec (2018, 2019); “7x Echosec Licenses” (2020–2023); EJ2 Communications (2023)	2018–2023	CAD 488,810.24 on the 2020 licences; CAD 870,514.68 in the 2023 contract
Ogden City, Utah	Echosec	FY2020–FY2021	\$22,800 paid
ICE, HSI Philadelphia	EJ2 Communications, “Tailored Reporting Services”	Apr 2021	\$25,000
TSA	“Echosec-Beacon Systems User Licenses”	FY2021–FY2022	\$887,304.20
EULEX Kosovo	Maltego and Social Links Pro	Apr 2021	—
US Army (INSCOM), via BAE Systems	OSINT task order with Echosec subawards	2021–2024	\$437m (task order)
FBI, Miami Field Office	Six Flashpoint licences	May 2022	\$29,500
FBI	“Social Exploitation Tool-Flashpoint”	Aug 2023	\$329,558
US Attorney’s Office, Eastern District of New York	“Flashpoint Platform Database”	Oct 2023	\$137,958
New York State Police	“Flashpoint Echosec license subscriptions”	2023–2025	\$347,878.23
DEA	“Echosec Platform (User License)”	Mar 2024	\$43,000
ICE	Flashpoint licences (four orders)	2023–2030	\$1.87m obligated; \$3.195m ceiling on the current order

Buyer	Product	Date	Value
US Marine Corps	“Flashpoint Echosec”	FY2024–FY2025	\$385,158.09
New York State Police	Flashpoint	2025–2026	\$555,455.28
US Marshals Service	“Flashpoint Identify”	Sep 2026	\$131,107.20
FBI	“CYD Flashpoint”	Sep 2026	\$1,191,452.65

Sources.¹⁵¹

The 2014 ICE order sought “data and analysis on illicit activity conducted on online social networks, especially those accessed via the internet’s ‘dark web.’”¹⁵² The FBI’s 2022 order describes Flashpoint databases of extremist data gathered “through passive monitoring of terrorism-related forums and platforms.”¹⁵³ Its 2023 order names the product a “Social Exploitation Tool.”¹⁵⁴ These are the Bureau’s own descriptions: a tool for watching forums of the kind Raddle is, bought from a vendor that names Raddle as a source. The FBI’s largest Flashpoint order, “CYD Flashpoint,” was placed on 21 September 2026 for \$1,191,452.65.¹⁵⁵ The latest ICE order, funded by Homeland Security Investigations, is for “Flashpoint licenses to gather cyber intelligence for use by investigators and analysts,” with \$1.10 million obligated and a ceiling of \$3.195 million running to 2030 (Figure 7).¹⁵⁶ The closeout of the preceding order says the licences were “utilized by Homeland Security Investigations to assist in cyber investigations.”¹⁵⁷ The US Marshals order is headed “Mission critical - apprehending fugitives.”¹⁵⁸

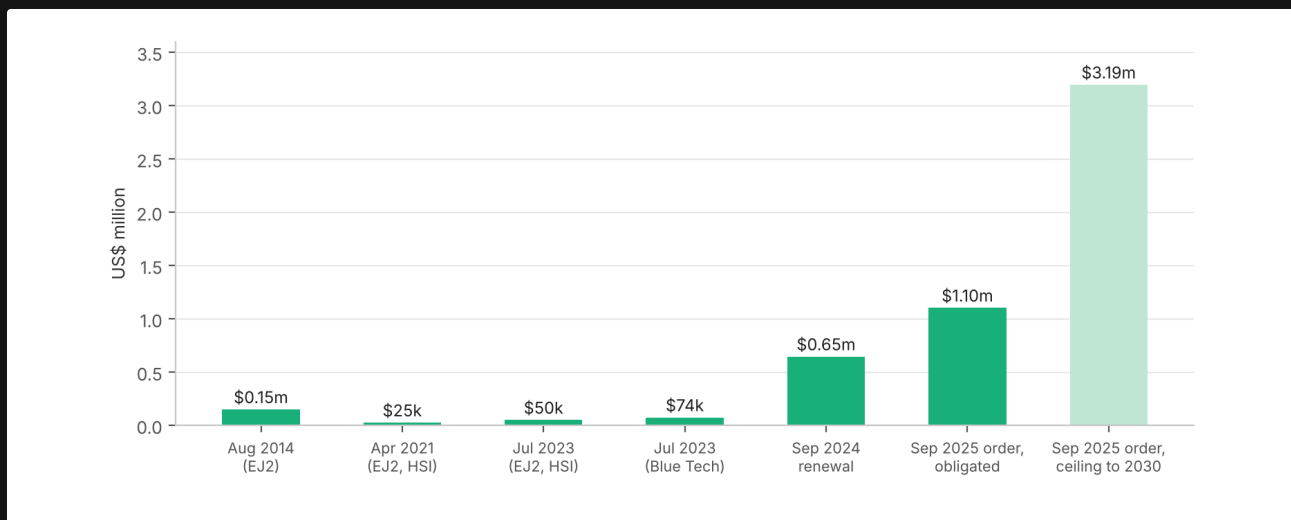


Figure 7. ICE orders from Flashpoint (trading as EJ2 Communications) and its resellers, 2014–2025: obligated value of each order and the ceiling of the current order. Flashpoint acquired Echosec in August 2022.

The one buyer that named Raddle. In February 2020 the Ogden City police in Utah issued a tender for dark-web monitoring software for its Area Tactical Analysis Center.¹⁵⁹ The city’s published answers to bidders list the sources it wanted, and Raddle is one of them, beside Gab, Mastodon, Reddit, Telegram and 4chan.¹⁶⁰ The requested list closely matches Echosec’s own source list, and the city’s recommendation, as indexed, names Echosec Systems. The city then paid Echosec \$11,800 in fiscal year 2020 and \$11,000 in fiscal year 2021.¹⁶¹ On 25 August 2026 an ICE agent detained a man on an Ogden

street with an Ogden officer standing by, and the city has since been revising its policy on police contact with immigration agents.¹⁶² Ogden's licence-plate camera portal lists immigration enforcement as a prohibited use.¹⁶³

The chain from a local tender naming Raddle and a paid licence, through a vendor now owned by Flashpoint, to federal immigration and fugitive-tracking agencies buying Flashpoint licences, **may indicate** that Raddle content is available to agencies whose work now includes immigration enforcement in the United States.

Non-government routes to the police. Flashpoint publishes a case study in which the Community Security Initiative of New York, a private communal-security body, used Echosec and Flashpoint to find a threat and passed it to the New York Police Department.¹⁶⁴ Private customers, including the retail loss-prevention teams the vendors court, can pass what they find to police without any procurement record.

Comparators. Police use of commercial social-media monitoring is well documented elsewhere.

- Houston renewed its support for Dataminr for police use in February 2024, at \$108,000.¹⁶⁵
- The District of Columbia police used Babel Street, Dataminr, Sprinklr and Voyager Labs between 2014 and 2022.¹⁶⁶
- The Los Angeles police used Geofeedia from 2014 to 2016 and trialled Dataminr, Skopenow and Media Sonar.¹⁶⁷
- The New York State Police hold 21 Skopenow subscriptions worth \$829,295.¹⁶⁸

In those cases the platforms monitored were large and mainstream. Raddle stands out because vendors name it individually and market it to security buyers as a niche source.

Assessment. We assess with **high confidence** that Raddle content has been collected commercially and offered to government buyers since June 2019, and with **high confidence** that agencies in the United States, Canada, the United Kingdom and the EU mission in Kosovo bought tools from the vendors concerned. We assess it **likely** that at least one government user has queried Raddle content through these tools, given the vendors' marketing, the Ogden tender and payments, and the volume of licences bought.

3.7 Provider, host and legal routes in the milieu

Platforms in Raddle's milieu have been reached through their providers, their hosts and pressure on their operators.

- **Indymedia.** In 2004 the FBI arranged the seizure of Indymedia servers hosted by Rackspace in London. A 2009 US subpoena for visitor IP addresses was withdrawn because the site kept no logs.¹⁶⁹
- **Autistici/Inventati.** Italian police secretly searched the collective's main server in 2004.¹⁷⁰ On 26 August 2026 the US Treasury designated Autistici/Inventati a Specially Designated Global Terrorist.¹⁷¹ According to ARTICLE 19, the US registry suspended its domain and payment providers closed its accounts; on 6 September 2026 the collective announced its shutdown, affecting about

16,000 mailboxes and 10,000 blogs.¹⁷² Its blog service was defaced around 28 August with a claim that user data had been handed to the US government.¹⁷³

- **linksunten.indymedia.** Germany banned the site on 14 August 2017 and executed the ban on 25 August 2017, two and a half weeks before raddle.me was registered. The Federal Administrative Court upheld the ban in 2020 on evidence that included the site's internal chats and mailing lists, with the source withheld.¹⁷⁴
- **NoState.** Dutch police seized a server of the NoState collective at British request in spring 2021.¹⁷⁵ In May 2026 the Dutch fiscal police seized more than 800 servers of a single hosting company.¹⁷⁶
- **AnarchistFederation.net.** The No Gods No Masters network reports that in July 2026 Cloudflare received an FBI court order about the site under a nondisclosure order, and that Google was later subpoenaed before a federal grand jury to identify two of its administrators.¹⁷⁷
- **Anarchist News.** In 2011, police acting for the Ontario Provincial Police visited an Anarchist News administrator at home and obtained the removal of posts about undercover officers.¹⁷⁸
- **Greek campus hosting.** The Espiv server at Panteion University was unplugged on the rector's order in 2014 and again in 2020, and Athens Indymedia was cut off at the National Technical University of Athens in 2013.¹⁷⁹

Comparison with Raddle. Raddle's infrastructure has the same exposure.

- **Cloudflare.** Raddle's traffic has passed through Cloudflare, the provider served in the AnarchistFederation.net case, since about August 2022.¹⁸⁰
- **Hosting.** Raddle's origin server has been hosted by a US company in the Netherlands, the country of the NoState and FIOD seizures.¹⁸¹
- **Registration.** Raddle's domain is held through a Canadian registrar that accepts process from four countries.¹⁸²
- **The operator.** ziq has reported at least one request from police for user data, in 2024.¹⁸³
- **Network.** Raddle is linked to Anarchist News and Anarchy Planet (Figure 9), and its operator called in 2020 for "a strong anarchist media alliance."¹⁸⁴

The October 2026 PHP disclosure. The critical PHP release of 21 October 2026 that took Raddle offline was coordinated in advance among security firms. The disclosure site lists Wiz, Calif and OpenAI as the reporting circle and names collaborators including Cloudflare, Akamai, CrowdStrike, Palo Alto Networks and Google.¹⁸⁵ OpenAI says US defensive cyber agencies, including the Office of the National Cyber Director and CISA, were briefed before disclosure.¹⁸⁶ Cloudflare, one of the collaborators, is Raddle's own provider; its presence in the disclosure chain is consistent with its ordinary role across the web.

Assessment. We assess with **high confidence** that the provider route is the most-used state route against platforms in this milieu, and that every element of it applies to Raddle. In the AnarchistFederation.net case, process reached the providers under a nondisclosure order, and the operators learned of it only when the order lapsed.

3.8 Policy drivers

US policy since 2023 directs agencies to buy the kind of data the vendors sell.

- The Defense Department’s open-source strategy says “Third-party data brokers, industry partners, and academia with persistent global reach can provide expertise, access, and agility far outpacing what the government can create.” It calls for a “diversified collection posture” not “overly-dependent on a specific social media outlet,” and for “machine association of disparate data points.”¹⁸⁷
- The intelligence community’s strategy says expanding access to publicly and commercially available information “will maximize the return on IC investment.”¹⁸⁸
- The Defense Department strategy warns that spam could push “many web platforms towards invitation-only, rendering these services inaccessible under current OSINT policies and authorities.” Raddle has closed new registrations several times while keeping all content readable, which keeps it inside open-source authority.
- The intelligence community’s definition of commercially available information excludes material “obtained from activities undertaken through human sources.”¹⁸⁹ Collection through an informant or a cooperating operator therefore falls outside the commercial-data reporting regime.
- The 2026 report on that regime classes data as “sensitive” when it reveals “political opinions” or “membership or participation in organizations or associations,” and reports 23 sensitive datasets in use, six of them US-focused. A feed of Raddle posts carries the characteristics the report associates with sensitive data.

Designations of anarchist groups have added a counter-terrorism basis for watching this milieu.

- On 20 November 2025 the State Department designated the Informal Anarchist Federation/International Revolutionary Front and three other groups as Foreign Terrorist Organizations.¹⁹⁰ Material support to such a group is a crime for persons subject to US jurisdiction.
- Raddle’s own search returns two posts naming the Informal Anarchist Federation: a podcast link of 2017 posted by foundstone, and an archived 2014 research profile of the group posted by stacat in 2023.¹⁹¹ Neither is a communiqué. Both posting accounts exercised administrator rights while absent from the public administrator list (Section 2.2).
- On 26 August 2026 the Treasury designated Autistici/Inventati, a hosting collective, extending terrorism sanctions to movement infrastructure.¹⁹²

Legal routes outside the United States have widened at the same time.

- The EU e-Evidence Regulation, applicable from 18 August 2026, lets authorities in one member state order a service provider in another to produce data directly.¹⁹³
- The UK’s Covert Human Intelligence Sources (Criminal Conduct) Act 2021 lets police and intelligence services authorise criminal conduct by their sources.¹⁹⁴

Assessment. We assess with **high confidence** that the policy environment of 2023–2026 increases both the demand for commercial collection of platforms like Raddle and the legal basis for process against them.

3.9 Synthesis

Figure 8 places Raddle among the cases.

- **Agency-run platforms.** Raddle shares the architecture (concentrated identifiers, persona use at the top, privacy promises) and, in May 2024, the takeover shape: police contact, an administrator's departure and a new account behind the familiar name within days. The defining element of these cases, a state controller, came to light in each case through prosecution records or official announcements.
- **Movement infiltration.** Raddle's operator shows the behavioural signature: control of infrastructure, division by false identity, control over who is called an informant, long tenure. The same signature fits a personal or factional operator.
- **Online covert action.** Raddle's persona practice matches the technique. The open admissions fit an amateur; the rotation of accounts behind a fixed administrator name shows managed identities.
- **Commercial collection.** Raddle has been a named, marketed source since June 2019, and the buyers include police, military, intelligence, immigration and fugitive-tracking agencies; one police buyer named Raddle and paid.
- **Provider routes and pressure.** Raddle's providers are the kind already served with process in this milieu in 2026, and the operator has reported a police request for user data.

We assess with **moderate confidence** that Raddle is best described as an independently run platform, governed through undisclosed accounts, whose content is collected and sold by commercial vendors to government customers and whose infrastructure is exposed to legal process in several countries. We assess with **low confidence** that a state body directs the platform or its operator, and with **low to moderate confidence** that the May 2024 handover may indicate a deliberate placement inside the administrator group. The features that would distinguish these readings are the ones that agency operations hide.

4. Implications

In brief

- Anything posted can enter vendor databases sold to police, military and immigration agencies.
- Users cannot tell who holds administrator access or which accounts are the administrators’.
- Most legal routes to users run through third parties that the warrant canary does not cover.

4.1 For users

- **Public posts are a commercial intelligence product.** Anything posted on Raddle can enter vendor databases sold to police, military, intelligence and immigration agencies, and to corporate security teams. Deleting a post on Raddle does not remove copies already collected.
- **Identifying data sits with a few people.** Every IP address a user has used is visible to whoever holds administrator rights. Those rights have been held by accounts the public list did not name, and by a listed name that stood for five accounts in turn. The same people decide who is exempted from IP storage.
- **Privacy statements are unreliable.** The platform has made incompatible statements on IP retention, has promised “Zero tracking or analytics” while loading Cloudflare’s analytics beacon, edited its privacy policy without notice in March 2024, loosened its non-cooperation promise in May 2024 and on 2 October 2026 dropped its pledge to delete the site rather than obey a court order.¹⁹⁵
- **State pressure has reached the operator.** By ziq’s own account, police sought identifying data about a user in 2024.¹⁹⁶ The claim that nothing was handed over is the operator’s, and the cooperation clause was loosened the same day.
- **The canary covers part of the exposure.** Raddle’s warrant canary refers to US National Security Letters, surveillance-court orders and gag orders, and it lapsed for about five months in 2021.¹⁹⁷ The canary live on 21 October 2026 was signed on 2 October.¹⁹⁸ A canary reports orders served on the operator. Process served on Cloudflare, the hosting company or the registrar, an informant’s report, or an operator’s voluntary disclosure would leave it unchanged.
- **The rules now discourage asking.** Since 20 October 2026 the terms tell users not to treat accounts as alts without strong grounds, written by an operator whose own alternate accounts are documented.¹⁹⁹
- **Who users are dealing with is unclear.** Users cannot tell which accounts are the administrator’s. Arguments, moderation and accusations of being a “cop” have come from accounts the administrator ran.

4.2 For the movement network

- **A single point of exposure.** Raddle is linked to Anarchist News, Anarchy Planet and allied publishers (Figure 9). An operator who controls one node and calls for “a strong anarchist media alliance” sits at a junction of the network.²⁰⁰

- **Designations change the stakes.** Since November 2025 posting, relaying or hosting material connected with designated anarchist groups carries a terrorism-law risk for anyone subject to US jurisdiction.²⁰¹ Platforms that carry such material, and their providers, are now plausible targets for process; the Autistici/Inventati case shows the consequences can include loss of domain, payments and the service itself.²⁰²
- **Infiltration lessons apply online.** The historical record shows infiltrators taking roles that held a group's money, communications and publishing. On an online platform the equivalent role is the administrator account. On Raddle, who holds that role is decided by the operator alone.
- **Informant accusations are a weapon.** COINTELPRO used false informant labels to break groups apart.²⁰³ On Raddle, the administrator and the administrator's undisclosed accounts have decided when the label is used and when it is punished.

4.3 For operator accountability

- **One person controls everything.** ziq holds the domain, the server, the funding and the administrator role, and says there is no collective.²⁰⁴ The platform's governance rests on ziq's word.
- **ziq's word has been unreliable.** ziq said in 2018 that ziq would step away from administration and moderation, then returned. ziq said "I'm not using any alts" while referring to "my old alts like brick." The moderation log contradicts the public administrator list in every year from 2020 to 2026.²⁰⁵
- **The record is edited.** The privacy policy was changed without notice in March 2024, a terms changelog line was rewritten after the fact, the October 2026 security-culture section was dated ten days before it appeared,²⁰⁶ the named administrator list was replaced with role descriptions in June 2024, and the canary lapsed in 2021 under the same signing key it still uses.²⁰⁷ Postmill added a setting in December 2025 that lets an operator hide the moderation log, the main public record against which the operators' statements can be checked.²⁰⁸
- **Critics are removed.** Questions about the operators' accounts and conduct are removed at about three times the rate of other content, often with no reason given or with labels that treat the questioner as an alternate account.²⁰⁹
- **The developer is inside the operation.** emma holds administrator rights shown on no public list and built the images the site depended on to come back on 21 October 2026.²¹⁰ The administrators page distinguishes a "sys admin (person with server access)" from site administrators and names neither.²¹¹
- **Security in practice.** The site returned on 21 October 2026 on Postmill v2.2.2, three months after v2.2.3 was published, and on PHP 8.5.12, a release publicly known to be incomplete.²¹² The same week, the operator's new rules told users to "Take Security Culture Seriously."²¹³
- **Insider risk is structural.** Any person behind any account with administrator rights, at any time, could see users' IP addresses. Who controlled the unlisted and renamed accounts, and what they did with that view, rests on the operator's word.

4.4 Legal reach

Route	Jurisdiction	Instrument	What it reaches
Cloudflare	United States	Court order, subpoena, National Security Letter; nondisclosure orders	Edge data: visitor IP addresses, request logs, analytics
Hosting provider	United States, Netherlands	US warrant (per provider guidelines); Dutch seizure; EU production order	Server contents, including stored IP addresses
Registrar and privacy service	Canada, United States, Denmark, Germany	Subpoena or warrant (per registrar policy); discretionary disclosure	Registrant details and account records
Operator	Wherever the operator is reachable	Police request (one reported in 2024); court order; home visit; informant recruitment	Everything administrators can see
Vendors	United States, Canada, United Kingdom	Purchase; no process needed	Public posts and account histories

Sources.²¹⁴

The table shows that most routes to Raddle’s users run through third parties, and that only the operator route is covered by the canary.

4.5 For assessing the platform’s risk

- **Collection is established; direction is the open question.** The external-collection relationship is documented. Any direct relationship between a state body and the operator would, on the comparators, be documented only through prosecution, official disclosure or leak. The May 2024 handover is the point where an inside relationship is most plausible on the public record, and it is where any further evidence should be sought.
- **The operator’s conduct raises the risk under every model.** Concentrated data, unlisted administrator rights, undisclosed accounts and unreliable statements increase the exposure of users whether the operator acts alone, for a faction, or for a sponsor.
- **Timing points to watch.** Four dated clusters fit the pattern of operator behaviour shifting after outside events:
 - **2021.** The warrant canary lapsed from about July to November 2021 and resumed with a notice of irregular updates; on 2 December 2021, after a reported attack and a change of server, the operator opened a Cloudflare account, and traffic was proxied from about August 2022.²¹⁵
 - **March to June 2024.** The privacy policy was edited without notice on 26 March. The DEA ordered an Echosec licence the next day.²¹⁶ On 4 May ziq reported a police request, the terms recorded that “u/Tequila_Wolf left,” and the non-cooperation clause was loosened that evening; a new account registered on 6 May later held the name. On 28 June the named administrator list was replaced with role descriptions and the hosting statement changed to “Various locations in the EU.”²¹⁷

- **October 2026.** The legal pages were rewritten on 2 October, 45 days after the EU e-Evidence Regulation began to apply and five weeks after the Autistici/Inventati designation.²¹⁸
- **After contact, October 2026.** Moderator roles were handed out on 15–18 October; questions were sent on 19 October; on 20 October ziq added the security-culture section, dated in the changelog to 10 October.²¹⁹
- Each cluster **may indicate** an operator responding to legal or security pressure. None establishes the source of that pressure. Vendor coverage of Raddle began in June 2019, before all three, so the vendor and procurement record runs ahead of these changes rather than following them. Echosec’s post naming Raddle a “new data provider” is dated 9 July 2019.²²⁰

5. Outlook and Indicators

In brief

- Commercial collection and legal process against the milieu are likely to increase.
- The indicators below would show whether the platform's relationship with the state is external only or reaches inside.

We assess it **likely** that commercial collection of Raddle will continue and that government purchases of the relevant vendor products will grow, given the ICE ceiling running to 2030, the US Marshals order running to 2029 and the policy direction set in 2023–2024.²²¹

We assess it **likely** that legal process against platforms and providers in the anarchist milieu will increase under the 2025–2026 US designations and the EU e-Evidence regime.

The following indicators would change this assessment.

Indicators of a direct state relationship with the platform:

- a court filing, exhibit or discovery record that cites Raddle data with an administrator-level detail (an IP address, a deleted post, a private message);
- a change in the warrant canary, its lapse, or a change of its signing key (the live canary is dated 2 October 2026);
- a statement of work or source list for the FBI or ICE Flashpoint licences that names Raddle, as could be sought under the Freedom of Information Act;
- a further renaming of an account holding administrator rights, or a new holder behind a listed administrator name, especially soon after a reported legal request;
- any further report by the operator of contact from police or courts, or a change in how such contacts are reported;
- use of Postmill's setting to hide the moderation log;
- the site staying on PHP 8.5.12 or Postmill v2.2.2 after complete fixes are available;
- a sudden change in software, hosting or administrator behaviour without a stated technical reason;
- a further change to the legal pages that loosens commitments to users;
- an official disclosure or leak describing a source with administrator access to an anarchist platform.

Indicators of continued external collection only:

- further vendor material naming Raddle;
- procurement records for the same vendors;
- research datasets citing Raddle posts;

- process served on Cloudflare, the host or the registrar, disclosed by the provider or the operator after a nondisclosure order lapses.

Indicators of factional or personal control:

- further removals of criticism under labels that treat critics as alternate accounts;
- new accounts with administrator rights absent from the public list;
- further evidence of administrator-run accounts in disputes.

Annex A. Chronology

Date	Event
Dec 2016	raddit.me launched on WordPress after Reddit banned r/LeftWithSharpEdge
Mar 2017	Appeal signed “Ziq” promises a warrant canary, “No data is collected” and a Netherlands server
Mar 2017	First Kiwi Farms thread on raddit.me; raddit.me carries a “Warrant Canary” badge
6 May 2017	emma, ziq and Defasher registered on the new database
10 May 2017	Postmill launch; 16 of 20 front-page items by ziq or later-admitted accounts
20 Jun 2017	Account A registered; later carries the listed name Tequila_Wolf
Jun 2017	First FAQ: IP addresses kept “only for 7 days,” two administrators
25 Aug 2017	German ban on linksunten.indymedia executed
9 Sep 2017	Useful_info forum, moderated by Defasher, carries a “Dox” posted by Cherimoya
11 Sep 2017	raddle.me registered through Tucows behind Contact Privacy
29 Oct 2017	Current canary signing key created
Nov 2017	Postmill stops storing IP addresses of allowlisted users
Sep 2017	UK Home Office card payment to Echosec
3 Apr 2018	ziq admits eleven alternate accounts and steps down
Apr 2018 – Feb 2019	BigG takes 287 moderation actions; ziq’s main account inactive
Dec 2017 – Oct 2020	Account A (now foundstone) takes 1,580 administrator actions under the listed name Tequila_Wolf
18 Feb 2019	ziq returns to the administrator list
Jun 2019	Echosec’s product changelog: “Echosec has a new data provider: Raddle.me”
9 Jul 2019	Echosec blog: Raddle “should be bookmarked by all retail security teams”
Dec 2019	Paladin white paper names Raddle
Feb 2020	Ogden police tender lists Raddle as a required source; second Kiwi Farms thread

Date	Event
FY2020–FY2021	Ogden City pays Echosec \$11,800 and \$11,000
Apr 2020	DarkOwl publishes Raddle comments with onion path
Jun 2020	Retail-industry webinar recommends monitoring Raddle
Sep 2020	Canada’s Department of National Defence contract for seven Echosec licences
13–14 Oct 2020	Account A’s last administrator action; Hibiscus_Syrup’s first, the next day
31 Mar 2021	Account B registered; holds the listed name Tequila_Wolf in 2021
2 Apr 2021	ICE HSI Philadelphia order for “Tailored Reporting Services”
Spring 2021	Dutch police seize a NoState server at British request
Apr 2021	EULEX Kosovo buys Social Links Pro
2021	LifeRaft tells loss-prevention staff to “bookmark Raddle.me”
Jul–Nov 2021	Warrant canary lapses; resumes 30 Nov “on an irregular basis”
2 Dec 2021	Raddle announces its move behind Cloudflare; Cloudflare account opened
Jan–Mar 2022	Account then named “Marco” (now stacat) takes the listed name Tequila_Wolf
Feb 2022	Brick begins moderating; bans a user for “badjacketing”
May 2022	Flashpoint’s 2021 review names Raddle; FBI Miami buys Flashpoint licences
3 Aug 2022	Flashpoint acquires Echosec
c. 18 Aug 2022	raddle.me traffic proxied through Cloudflare
Feb 2023	Raddle added to the nuclei-templates username checks
Jan–Jun 2023	FOMEC reports 56,091, then 87,766 Raddle posts
Jul 2023	Two ICE Flashpoint orders
Aug 2023	FBI order “Social Exploitation Tool-Flashpoint”
Oct 2023	US Attorney’s Office, EDNY, “Flashpoint Platform Database”
Sep 2023	NIJ award built on the FOMEC project
Oct 2023	DoD OSINT Strategy 2024–2028
Nov 2023	New York State Police “Flashpoint Echosec” subscriptions begin

Date	Event
Mar 2024	IC OSINT Strategy
26 Mar 2024	Privacy policy edited without notice
27 Mar 2024	DEA Echosec licence
Late Apr 2024	Police seek identifying data about a user from the platform (per ziq)
4 May 2024	ziq reports a police request; “u/Tequila_Wolf left”; non-cooperation clause loosened
6 May 2024	Account C (now triangle) registered; later holds the listed name Tequila_Wolf
26 Jun 2024	Account C first seen holding the name Tequila_Wolf, without administrator rights
28 Jun 2024	Named administrator list replaced with role descriptions
26 Jun – 17 Jul 2024	Account C gains administrator rights
13 Jul 2024	“ruminator” removal label first used; the holder of the name Tequila_Wolf says the admin keeps alts
Jul 2024	Members allege gokuscloud and factotum are ziq’s
Sep 2024	ICE Flashpoint renewal, \$644,930
Jul–Nov 2024	The name “kin” passes from a 2020 account to one registered in April 2024
26 Nov 2024	ziq locks the 2018 thread “I’m not even the only admin who used alts”
28 Aug 2025	Account D registered; current holder of the name Tequila_Wolf
Aug 2025 – Jan 2026	Cloudflare analytics beacon added
Sep 2025	ICE Flashpoint order with \$3.195m ceiling to 2030
20 Nov 2025	US designates the Informal Anarchist Federation/International Revolutionary Front
Dec 2025	Postmill adds a setting to hide the moderation log
Jul–Aug 2026	FBI process on Cloudflare and Google over AnarchistFederation.net
18 Aug 2026	EU e-Evidence Regulation applies
25 Aug 2026	ICE arrest in Ogden with a local officer present
26 Aug 2026	Autistici/Inventati designated a Specially Designated Global Terrorist
30 Aug 2026	ICE exercises option 1 on the current Flashpoint order

Date	Event
8 Sep 2026	US Marshals order “Flashpoint Identify”
21 Sep 2026	FBI order “CYD Flashpoint,” \$1.19m
Sep 2026	ODNI report on sensitive commercially available information
2 Oct 2026	Raddle rewrites its legal pages and drops the pledge to delete the site rather than comply; warrant canary signed
15–18 Oct 2026	Several members given moderator roles on several forums at once
18 Oct 2026	Raddle offline about 05:34–11:46 UTC
19 Oct 2026	Questions sent to ziq, emma, Flashpoint and the Anarchist News collective; copy to ziq@raddle.me bounces
20 Oct 2026	ziq posts “Take Security Culture Seriously”; changelog dates it to 10 October
21 Oct 2026	Critical PHP release; Raddle offline 00:44–17:09 UTC; returns on PHP 8.5.12 images built by emma’s Codeberg account; no replies by the deadline

Annex B. Administrator rights in the moderation log

Actions taken with site-administrator rights over the whole log, October 2017 to October 2026, set against the public administrator list in the terms of service.²²² Before mid-2018 the log also marked at least one non-administrator as “admin,”²²³ so rows before July 2018 should be read with that caveat. Figure 3 counts from July 2018.

Account	Actions	First	Last	Listed when acting
ziq	5,310	Oct 2017	Oct 2026	Yes, except Apr 2018 – Feb 2019
foundstone (account A)	1,580	Dec 2017	Oct 2020	Yes, as Tequila_Wolf
mofongo	854	May 2019	Oct 2026	Yes
emma	700	Nov 2017	Aug 2026	No after Mar 2018 (administrator icon on profile, Aug 2020 – Oct 2026)
Fossidarity	419	Apr 2018	Jul 2019	Yes
stacat (formerly “Marco”)	345	Apr 2021	Apr 2024	As Tequila_Wolf from early 2022; not before
GrimWillow	286	Jul 2018	May 2019	Yes (listed from 16 Jul 2018)
triangle (account C)	47	Jul 2024	Mar 2025	No (the name Tequila_Wolf had left the list)
leftous	44	Apr 2018	Apr 2018	—
Hibiscus_Syrup	43	Oct 2020	Mar 2021	No
ziq_themes2	39	Oct 2017	Jan 2018	No
not_active	1	Feb 2022	Feb 2022	No

Holders of the listed name “Tequila_Wolf”:

Holder	Registered	Held the name	Later name
Account A	20 Jun 2017	2017 – at least late Sep 2020	An_Old_Big_Tree, then foundstone
Account B	31 Mar 2021	2021 – early 2022	Tequilx_Wolf (“retired account”)

Holder	Registered	Held the name	Later name
Account then named “Marco”	2021 or earlier	Jan/Mar 2022 – May 2024	stacat
Account C	6 May 2024	2024 – at least 27 Nov 2024	triangle
Account D	28 Aug 2025	2025 – present (no administrator icon on 21 Oct 2026)	—

Annex C. Moderation statistics

All figures are the author’s tabulation of the public moderation log, 23 October 2017 to 13 October 2026.²²⁴

Measure	All removals, bans and locks	Criticism of operators	Surveillance and security topics
Entries	16,253	367	201
Spam or bot reason	45%	—	54%
No reason given	17%	49%	24%
Alt, sock, ban-evasion or troll label	5%	14%	2%

Other figures:

- ziq took 5,657 of 16,565 entries (34%) on 1,570 separate days.
- Of 80 removals of posts naming ziq, ziq took 31.
- The “ruminator” label was used on 131 actions against 44 accounts; ziq took 85.

Annex D. Glossary

Term	Meaning
Administrator rights	Site-wide powers in Postmill, including viewing users' IP addresses and banning by IP
Administrator icon	The wrench Postmill draws on a profile when the account holds administrator rights at the moment the page is served
Administrator seat	A public administrator name on the list, as distinct from the account holding it at a given time
Allowlist	Postmill's list of "trusted" users exempt from IP checks, whose IP addresses are not stored
Alternate account (alt)	A second account run by the same person, undisclosed to other users
Attributed	An account this assessment treats as ziq's on the investigator's assessment, beyond ziq's own admissions
Badjacketing	Falsely labelling someone an informant
CAI	Commercially available information, as defined by the US intelligence community
Canary	A statement an operator stops publishing if served with a secret order
COINTELPRO	FBI counter-intelligence programmes against domestic political groups, 1956–1971
Moderation log	Raddle's public record of staff removals, bans and locks
Nondisclosure order (NDO)	A court order barring a provider from telling its customer about legal process
OSINT	Open-source intelligence
Postmill	The forum software Raddle runs, written by emma
SDGT	Specially Designated Global Terrorist, a US Treasury sanctions designation

Notes

1. Background

1. Matsakis, “Radical Leftists Built Their Own Reddit”.
2. raddit.me, WordPress site (2016–17); raddit.me, “This is a Safe Space,” March 2017.
3. “Make raddit.me your back up plan”.
4. raddit.me, “History” (2017).
5. raddit.me front page, May 10, 2017.
6. Raddle, user registration records.
7. ziq, “I’m stepping down as admin”.
8. Identity Digital, RDAP record for raddle.me; Whoxy, WHOIS history of raddle.me.
9. ziq, “We’ve rebranded to raddle.me”.
10. Tucows, eNom acquisition release.
11. Tucows WHOIS record for raddle.me.
12. ziq, “Privacy policy and terms of service have been updated”.
13. Raddle, “Moderation Log”.
14. ziq, “ziq-raddle.me,” Patreon.
15. ziq, comment in /f/lobby/158174.
16. ziq, Liberapay profile.
17. ziq, Liberapay profile.
18. Raddle, legal and administrator pages.
19. ziq, comments in /f/meta/201436 and /f/Mutual_Aid/191431.
20. Raddle, “Terms of Service”.
21. Postmill v2.2.2 source code.
22. Raddle, /f/anarchism.
23. Anarchist News, editorial change, August 2015; The Anarchist Library, home page, June 2012.
24. Little Black Cart, “What’s new with LBC - Fall 2019”.
25. ziq, “We need a strong anarchist media alliance”.
26. CrimethInc., “A Hell of a Mistress, the Beautiful Idea”.

2. The Platform Profile

27. Postmill v2.2.2 source code.
28. Codeberg, Postmill repository, Actions runs and packages.
29. Postmill v2.2.2 source code.
30. Raddle, “Privacy Policy”; Raddle, legal and administrator pages.
31. ziq, “A FAQ and Introduction to raddit.me”.
32. Raddle, “FAQ”.
33. Postmill v2.2.2 source code.
34. Postmill v2.2.2 source code; Postmill, CHANGELOG.
35. Raddle user pages, captures 2019–2024; Raddle, “Moderation Log”.
36. Postmill v2.2.2 source code; Raddle, “Moderation Log”.
37. Raddle, “Terms of Service”.

38. Raddle, “Moderation Log”; Raddle, “Terms of Service”.
39. Raddle, user profile pages, 2020–2026.
40. Raddle user pages, captures 2019–2024; Raddle, “Moderation Log”; Raddle, user page “Tequila_Wolf”.
41. Raddle user pages, captures 2019–2024; Raddle, “Moderation Log”.
42. Raddle, “Administrators,” revision of June 28, 2024; Raddle, user profile pages, 2020–2026.
43. Raddle, user profile pages, 2020–2026.
44. Raddle, /f/ToSBreaches/193983.
45. Raddle, /f/ToSBreaches/193983.
46. Raddle, “Terms of Service”.
47. “Made a cloudflare account today”.
48. Certificate-transparency and DNS records for raddle.me.
49. Certificate-transparency and DNS records for raddle.me; Raddle, legal and administrator pages.
50. Cloudflare, “The RUM Diaries”.
51. Raddle, “Why Raddle?”.
52. RapidDNS, raddle.me.
53. Delivery-status notification for ziq@raddle.me.
54. Raddle, “Legal Requests,” captures 2019–2025; Raddle, “Terms of Service,” revisions of May–June 2024.
55. DigitalOcean, “Law Enforcement Guidelines”.
56. Tucows, “Subpoena and Warrant Policy”.
57. Contact Privacy Inc., “Terms of Service”.
58. Raddle, “Warrant Canary”.
59. Raddle, “Warrant Canary,” captures 2018–2026.
60. Raddle, “Warrant Canary,” as read October 21, 2026.
61. zal, “Raddle’s warrant canary - update frequency?”; Raddle, “Warrant Canary,” captures 2018–2026.
62. Raddle, “Terms of Service”; Raddle, “Terms of Service,” revisions of May–June 2024; ziq, “Privacy policy and terms of service have been updated”; Raddle, legal and administrator pages.
63. Regulation (EU) 2023/1543.
64. ziq, “Transparency: Received a legal request from the police”.
65. Raddle, “Terms of Service,” revisions of May–June 2024.
66. Raddle, “Privacy Policy,” revision of March 26, 2024.
67. Raddle, “Terms of Service”.
68. raddit.me front page, May 10, 2017.
69. raddit.me front page, February 4, 2017.
70. ziq, “I’m stepping down as admin”.
71. ziq, “I’m stepping down as admin”.
72. Raddle, “Moderation Log”.
73. Raddle, “Terms of Service”.
74. Raddle, user registration records.
75. ziq, comments in /f/mediation/201606.
76. raddit.me, /f/Useful_info, September 9, 2017.
77. Raddle, /f/AskRaddle/193697 and /f/AskRaddle/193993.
78. Raddle, “Moderation Log”.

- 79. Raddle, “Moderation Log”.
- 80. Raddle, “Moderation Log”.
- 81. Raddle, “Moderation Log”.
- 82. Postmill v2.2.2 source code.
- 83. Raddle, “Moderation Log”; Raddle, /f/meta/29891.
- 84. Raddle, /f/meta/143382.
- 85. Raddle, “Moderation Log”.
- 86. LexieAssassin, “Wait... I’m a moderator now?”; Postmill v2.2.2 source code; Raddle, user profile pages, 2020–2026.
- 87. Investigator’s correspondence records, October 19–21, 2026; Delivery-status notification for ziq@raddle.me.
- 88. ziq, “New ToS Section: Take Security Culture Seriously”.
- 89. Raddle, “Terms of Service,” October 19–20, 2026; Investigator’s monitoring records of Raddle, October 19–21, 2026.
- 90. Investigator’s monitoring records of Raddle, October 19–21, 2026; Raddle, maintenance notices, October 2026.
- 91. PHP Group, news archive, October 20–21, 2026.
- 92. Raddle, maintenance notices, October 2026; Codeberg, Postmill repository, Actions runs and packages.
- 93. php-src issue tracker and pull request 24479.
- 94. Codeberg, Postmill repository, Actions runs and packages.
- 95. php-src issue tracker and pull request 24479.
- 96. Raddle, “Warrant Canary,” as read October 21, 2026.

3. Comparative Analysis

- 97. SC Magazine, “Cybersting: FBI ran DarkMarket forum”.
- 98. United States v. Anzalone.
- 99. Engadget, “Australian police posed as child abusers”.
- 100. Help Net Security, “Dark web Hansa Market shut down”.
- 101. LRT; Baltic Times; 404 Media, on ANOM.
- 102. ziq, “Transparency: Received a legal request from the police”.
- 103. Raddle, “Terms of Service,” revisions of May–June 2024; Raddle, “Moderation Log”.
- 104. Raddle user pages, captures 2019–2024; Raddle, user profile pages, 2020–2026; Raddle, /f/ToSBreaches/193983.
- 105. Raddle, “Administrators,” revision of June 28, 2024.
- 106. Raddle, “Terms of Service,” revisions of May–June 2024.
- 107. Raddle, /f/ToSBreaches/193983.
- 108. Senate Select Committee, Final Report, Book III.
- 109. The Canary, March 27, 2026 (Undercover Policing Inquiry).
- 110. CIVICUS Monitor, October 2022.
- 111. Deutscher Bundestag, Drucksache 18/3754.
- 112. Jungle World and Interventionistische Linke statement, 2026.
- 113. Washington Times, December 1, 2009; Salon, November 29, 2009.
- 114. The Intercept, “Deconstructed: FBI Informant Protests”.
- 115. United States v. Monsegur, S.D.N.Y., Dkt. 30.
- 116. ziq, Liberapay profile; ziq, comments in /f/meta/201436 and /f/Mutual_Aid/191431.
- 117. ziq, “I’m stepping down as admin”.
- 118. ziq, comments in /f/mediation/201606.
- 119. raddit.me, /f/Useful_info, September 9, 2017.

120. Raddle, “Moderation Log”.
121. NBC News, February 2014 (GCHQ JTRIG).
122. U.S. Air Force solicitation RTB220610.
123. HMIC, “An Inspection of Undercover Policing”.
124. FBI, Domestic Investigations and Operations Guide (excerpts).
125. raddit.me front page, May 10, 2017; ziq, “I’m stepping down as admin”.
126. ziq, “I’m stepping down as admin”.
127. Raddle, /f/AskRaddle/193697 and /f/AskRaddle/193993.
128. Raddle, “Moderation Log”; ziq, comments in /f/mediation/201606.
129. Raddle user pages, captures 2019–2024.
130. Raddle, /f/ToSBreaches/193983.
131. Raddle, “Moderation Log”; Raddle, /f/meta/29891.
132. Kiwi Farms, “raddit.me - It’s like Voat for SJWs”; Kiwi Farms, “Raddle- Reddit knockoff for far left larpers”.
133. ziq, “I’m stepping down as admin”.
134. Raddle, “Moderation Log”.
135. Raddle, “Moderation Log”; Raddle, “Terms of Service”; Raddle user pages, captures 2019–2024.
136. Echosec, “Product Updates,” June 2019.
137. Echosec, “What Is Raddle.me” (2019 capture).
138. Echosec, “What Is Raddle.me and Why Should Retailers Care?”.
139. Echosec, “Social Media Monitoring”; Echosec, Beacon documentation.
140. Flashpoint, “Platform Overview”.
141. Flashpoint, “Year in Review 2021”.
142. Flashpoint, “Flashpoint Acquires ... Echosec Systems”.
143. Social Links, product pages.
144. LifeRaft, “Loss Prevention Pros: Why You Should Bookmark Raddle.me”; LifeRaft, “What is Raddle.me?”.
145. DarkOwl, “Coronavirus on the darknet Pt 2”.
146. LifeRaft, “What is Raddle.me?” (removed).
147. gallery-dl; nuclei-templates; WhatsMyName.
148. Paladin Risk Solutions, “Social Media Threat Monitoring”; RILA, webinar slides, June 24, 2020.
149. Rogers, FOMEC reports.
150. National Institute of Justice, award 15PNIJ-23-GG-01382-DOMR.
151. Home Office, procurement card spend, September 2017; USAspending, award HSCETE14P00033; CanadaBuys, contract W8484-219879; Government of Canada, proactive disclosure of contracts; Transparent Utah, Ogden City payments to Echosec; USAspending, award 70CMSD21P00000038; USAspending, TSA, USMC and FBI orders, 2021–2026; EULEX Kosovo, “Awarded Contracts” 2021; FPDS, 47QFCA19F0040; FPDS, 15F06722P0000529; FPDS, 15F06723F0001672; FPDS, 15JA5324P00000008; Open Book New York, Consortium Networks LLC; FPDS, 15DDHQ24P00000321; USAspending, award 70CMSD23P00000064; USAspending, award 70CMSD23FR0000083; USAspending, IDV HSHQDC13D00026, order 70CMSD24FR0000086; USAspending, award 70CMSD25FR0000069; FPDS, 15M10226PA4700305.
152. USAspending, award HSCETE14P00033.
153. FPDS, 15F06722P0000529.
154. FPDS, 15F06723F0001672.
155. USAspending, TSA, USMC and FBI orders, 2021–2026.
156. USAspending, award 70CMSD25FR0000069.
157. USAspending, IDV HSHQDC13D00026, order 70CMSD24FR0000086.

158. FPDS, 15M10226PA4700305.
159. Ogden City, “RFP Dark Web Software”.
160. Ogden City, RFP questions and answers.
161. Transparent Utah, Ogden City payments to Echosec.
162. Vandenack, “ICE arrest in Ogden”; Kelleher, “Six weeks after ICE arrest”.
163. Ogden City Police, Flock transparency portal.
164. Flashpoint, “How CSI-NY Prevented a Synagogue Attack”.
165. Houston Landing, Dataminr renewal.
166. Brennan Center, D.C. police social media monitoring records.
167. Brennan Center, “LAPD Social Media Monitoring Documents”.
168. Open Book New York, Skopenow C002165.
169. Indymedia server seizures.
170. Autistici/Inventati, 2004 server search.
171. Treasury, press release sb0616; OFAC recent actions, August 26, 2026.
172. ARTICLE 19, “USA: Terrorism designation has global consequences”.
173. The Intercept, September 10, 2026 (Noblogs).
174. BVerwG, 6 A 1.19.
175. NoState, statement on 2021 server seizure.
176. BleepingComputer, May 2026 (FIOD seizure).
177. No Gods No Masters, transparency notices; Washington Examiner, August 31, 2026.
178. “Toronto G20 Main Conspiracy Group”; “The Anarchist Media to Come”.
179. Cybrigade, espiv shutdown announcement, July 7, 2014; infolibre.gr, June 8, 2020; Anarchist Federation (Scotland), May 7, 2013.
180. “Made a cloudflare account today”; Certificate-transparency and DNS records for raddle.me.
181. RapidDNS, raddle.me; DigitalOcean, “Law Enforcement Guidelines”.
182. Tucows, “Subpoena and Warrant Policy”.
183. ziq, “Transparency: Received a legal request from the police”.
184. ziq, “We need a strong anarchist media alliance”.
185. Wiz, “PHP2Shell”.
186. OpenAI, “Coordinated disclosure of critical vulnerabilities”.
187. Defense Intelligence Agency, DoD OSINT Strategy 2024–2028.
188. ODNI and CIA, IC OSINT Strategy 2024–2026.
189. ODNI, 2026 CAI Biannual Report.
190. Department of State, Public Notice 12865.
191. Raddle site search, “Informal Anarchist Federation”.
192. Treasury, press release sb0616; OFAC recent actions, August 26, 2026; ARTICLE 19, “USA: Terrorism designation has global consequences”.
193. Regulation (EU) 2023/1543.
194. Covert Human Intelligence Sources (Criminal Conduct) Act 2021.

4. Implications

195. Raddle, “Why Raddle?”; Raddle, “Privacy Policy,” revision of March 26, 2024; Raddle, “Terms of Service,” revisions of May–June 2024; ziq, “Privacy policy and terms of service have been updated”; Raddle, legal and administrator pages.
196. ziq, “Transparency: Received a legal request from the police”.

- 197. Raddle, “Warrant Canary”; Raddle, “Warrant Canary,” captures 2018–2026.
- 198. Raddle, “Warrant Canary,” as read October 21, 2026.
- 199. ziq, “New ToS Section: Take Security Culture Seriously”; ziq, “I’m stepping down as admin”.
- 200. ziq, “We need a strong anarchist media alliance”.
- 201. Department of State, Public Notice 12865; Treasury, press release sb0616; OFAC recent actions, August 26, 2026.
- 202. ARTICLE 19, “USA: Terrorism designation has global consequences”.
- 203. Senate Select Committee, Final Report, Book III.
- 204. ziq, Liberapay profile; ziq, comments in /f/meta/201436 and /f/Mutual_Aid/191431.
- 205. ziq, “I’m stepping down as admin”; ziq, comments in /f/mediation/201606; Raddle, “Moderation Log”; Raddle, “Terms of Service”.
- 206. Raddle, “Terms of Service,” October 19–20, 2026.
- 207. Raddle, “Privacy Policy,” revision of March 26, 2024; Raddle, “Terms of Service”; Raddle, “Administrators,” revision of June 28, 2024; Raddle, “Warrant Canary,” captures 2018–2026.
- 208. Postmill, CHANGELOG.
- 209. Raddle, “Moderation Log”.
- 210. Raddle, user profile pages, 2020–2026; Codeberg, Postmill repository, Actions runs and packages.
- 211. Raddle, “Administrators,” revision of June 28, 2024.
- 212. Codeberg, Postmill repository, Actions runs and packages; php-src issue tracker and pull request 24479.
- 213. ziq, “New ToS Section: Take Security Culture Seriously”.
- 214. DigitalOcean, “Law Enforcement Guidelines”; Tucows, “Subpoena and Warrant Policy”; Contact Privacy Inc., “Terms of Service”; Raddle, “Warrant Canary”; No Gods No Masters, transparency notices; Regulation (EU) 2023/1543; ziq, “Transparency: Received a legal request from the police”.
- 215. Raddle, “Warrant Canary,” captures 2018–2026; “Made a cloudflare account today”; ziq, /f/meta/137200; Certificate-transparency and DNS records for raddle.me.
- 216. Raddle, “Privacy Policy,” revision of March 26, 2024; FPDS, 15DDHQ24P00000321.
- 217. ziq, “Transparency: Received a legal request from the police”; Raddle, “Terms of Service,” revisions of May–June 2024; Raddle user pages, captures 2019–2024; Raddle, “Administrators,” revision of June 28, 2024.
- 218. ziq, “Privacy policy and terms of service have been updated”; Regulation (EU) 2023/1543; Treasury, press release sb0616; OFAC recent actions, August 26, 2026.
- 219. LexieAssassin, “Wait... I’m a moderator now?”; Investigator’s correspondence records, October 19–21, 2026; ziq, “New ToS Section: Take Security Culture Seriously”; Raddle, “Terms of Service,” October 19–20, 2026.
- 220. Echosec, “What Is Raddle.me” (2019 capture).

5. Outlook and Indicators

- 221. USAspending, award 70CMSD25FR0000069; FPDS, 15M10226PA4700305; Defense Intelligence Agency, DoD OSINT Strategy 2024–2028; ODNI and CIA, IC OSINT Strategy 2024–2026.

Annex B. Administrator rights in the moderation log

- 222. Raddle, “Moderation Log”; Raddle, “Terms of Service”; Raddle user pages, captures 2019–2024.
- 223. “Rotate the Spambuster position”.

Annex C. Moderation statistics

- 224. Raddle, “Moderation Log”.

Bibliography

Raddle and operator material

“An Appeal to All Reddit Radicals: Make raddit.me Your Back Up Plan.” Signed “Ziq, <https://raddit.me>.” Reddit, r/Anarchism, March 2017. https://www.reddit.com/r/Anarchism/comments/62fo8w/an_appeal_to_all_reddit_radicals_make_radditme/.

“Announcement: temp ban of u/mima while we evaluate claims of zionism.” Raddle, /f/ToSBreaches/193983, July 13, 2024, with comments. Internet Archive capture 20240714002340.

LexieAssassin. “Wait... I’m a moderator now?” Raddle, /f/AskRaddle/217849, October 17, 2026, with replies by ziq, mofongo and others. <https://raddle.me/f/AskRaddle/217849>.

“Made a cloudflare account today.” Raddle, /f/meta/137277, December 2, 2021; page saved October 3, 2026. <https://raddle.me/f/meta/137277/made-a-cloudflare-account-today>.

raddit.me. “/f/Useful_info” forum page. archive.today capture iwFZr, September 9, 2017.

raddit.me. “History.” Site wiki. Internet Archive capture of September 7, 2017.

raddit.me. “This is a Safe Space” page, with warrant-canary badge. Screenshot dated March 31, 2017, held by the investigator; front page, archive.today capture JPqFG, March 28, 2017.

Raddle. “/f/anarchism” forum page and sidebar. Accessed October 5, 2026. <https://raddle.me/f/anarchism>.

Raddle. “Administrators.” Wiki page as revised by ziq, June 28, 2024. <https://raddle.me/wiki/administrators>.

Raddle. “FAQ.” Raddle wiki. Accessed October 13, 2026. <https://raddle.me/wiki/faq>.

Raddle. “Legal Requests.” Internet Archive captures 2019–2025, including the revision of October 10, 2024 and capture 20250806000230. https://raddle.me/wiki/legal_requests.

Raddle. “Privacy Policy.” Accessed October 13, 2026. https://raddle.me/wiki/privacy_policy.

Raddle. “Privacy Policy.” Internet Archive captures 20220530182609 and 20241126193630; revision by ziq dated March 26, 2024. https://raddle.me/wiki/privacy_policy.

Raddle. “Terms of Service,” with the administrator changelog, as captured at 12:36 UTC on October 19, 2026 and about 14:55 UTC on October 20, 2026. https://raddle.me/wiki/terms_of_service.

Raddle. “Terms of Service,” with the dated administrator changelog. Accessed October 9 and 13, 2026. https://raddle.me/wiki/terms_of_service.

Raddle. “Terms of Service.” Internet Archive captures 20240224174239 and 20240626160914, with the page revision history of May 4 and June 2024. https://raddle.me/wiki/terms_of_service.

Raddle. “Warrant Canary,” text as displayed about 23:00 UTC on October 21, 2026 (“As of Fri Oct 2 20:42:21 2026”). PGP signature checked against key 44A5B09AA78E62C513C84CA69BEA87514DF6298C; signature made October 2, 2026, 17:42:21 UTC. https://raddle.me/wiki/warrant_canary.

Raddle. “Warrant Canary.” Dated October 2, 2026. https://raddle.me/wiki/warrant_canary.

Raddle. “Warrant Canary.” Internet Archive captures, May 2018 to January 2026, including 20211125025033, 20211201220540, 20241126222527 and 20260119234756; PGP signatures checked against key 9BEA87514DF6298C. https://raddle.me/wiki/warrant_canary.

Raddle. “Why Raddle?” Raddle wiki. Accessed October 13, 2026. https://raddle.me/wiki/why_raddle.

Raddle. Legal-requests, administrators and warrant-canary pages of the Raddle wiki, as revised October 2, 2026. Read October 13, 2026.

Raddle. Maintenance page and notices of October 21, 2026, 00:45–17:09 UTC, served through Cloudflare; and ziq, “Site was down for about 5 hours,” /f/meta, October 2026.

Raddle. Site search for “Informal Anarchist Federation.” Accessed October 2026. Results: /f/Podcasts/8165 (September 25, 2017) and /f/Italy/153639 (April 17, 2023).

Raddle. Thread /f/meta/29891, April 2018, with comments by ziq; locked November 26, 2024.

Raddle. Threads /f/AskRaddle/193697 (c. July 9, 2024) and /f/AskRaddle/193993 (July 13, 2024). Ghostarchive captures DSeUI and 5k1no, July 10 and 13, 2024.

“Rotate the Spambuster position to the next person as voted by the community.” Raddle, /f/meta/20652, 2018. archive.today capture of April 2, 2018 (yUv4g).

“Why is raddle.me IP address in Ontario, Canada?” Raddle, /f/meta/143382, May 4, 2022, with replies by ziq. Post body removed. <https://raddle.me/f/meta/143382/->.

zal. “Raddle’s warrant canary - update frequency?” Raddle, /f/meta, c. 2023. Found through Raddle site search for “canary,” October 21, 2026.

ziq. “A FAQ and Introduction to raddit.me.” raddit.me, /f/meta/1502, June 5, 2017, edited June 7, 2017. Internet Archive capture 20170607131349.

ziq. “I’m stepping down as admin because of some shit I did - emma will be returning as webmaster and leftous will take a temp admin position.” Raddle, /f/lobby/28422, April 3, 2018. Internet Archive capture of April 5, 2018.

<https://web.archive.org/web/20180405002453/https://raddle.me/f/lobby/28422/i-m-stepping-down-as-admin-because-of-some-shit-i-did-emma>.

ziq. “New ToS Section: Take Security Culture Seriously.” Raddle, /f/meta/217898, October 20, 2026, 12:59 UTC, edited 13:03 UTC. <https://raddle.me/f/meta/217898>.

ziq. “Privacy policy and terms of service have been updated.” Raddle, /f/meta, October 2, 2026. <https://raddle.me/f/meta/217569>.

ziq. “Transparency: Received a legal request from the police a few days ago.” Raddle, /f/meta/188876, May 4, 2024. Internet Archive capture 20240504105606.

ziq. “We’ve rebranded to raddle.me.” Raddle, /f/meta/6779, September 2017. <https://raddle.me/f/meta/6779/we-ve-rebranded-to-raddle-me>.

ziq. “ziq-raddle.me.” Patreon. Accessed October 3 and 5, 2026. <https://www.patreon.com/ziq>.

ziq. Comment in /f/lobby/158174 (“The site is entirely funded via donations to my patreon”). Raddle. <https://raddle.me/f/lobby/158174>.

ziq. Comments in /f/meta/201436 and /f/Mutual_Aid/191431. Raddle, c. 2024. Read October 11, 2026. <https://raddle.me/f/meta/201436>.

ziq. Comments in thread /f/mediation/201606. Raddle, c. 2024–25. Read October 11, 2026. <https://raddle.me/f/mediation/201606>.

ziq. Liberapay profile. Accessed October 5 and 9, 2026. <https://liberapay.com/ziq/>.

ziq. Post on the server move after a DDoS. Raddle, /f/meta/137200. <https://raddle.me/f/meta/137200>.

Records about the platform

Cloudflare. “The RUM Diaries: Enabling Web Analytics by Default.” Cloudflare Blog. <https://blog.cloudflare.com/the-rum-diaries-enabling-web-analytics-by-default/>.

Codeberg. Postmill/Postmill repository: docker-build.yaml workflow runs of October 21, 2026, container packages pushed by postmill-bot, tags, and the history of src/Command/PruneIpAddressesCommand.php. Codeberg API. Accessed October 21, 2026. <https://codeberg.org/postmill/postmill>.

Contact Privacy Inc. “Terms of Service.” Accessed October 2026. https://www.contactprivacy.com/?action=wp_mailer_show_terms.

crt.sh and Cert Spotter certificate records for raddle.me, 2017–2026, with Internet Archive homepage captures of July–September 2022.

DigitalOcean. “Law Enforcement Guidelines.” Accessed October 5, 2026. <https://www.digitalocean.com/legal/law-enforcement-guidelines>.

emma. Postmill forum software, version 2.2.2 and earlier releases. Source code. Mirror at <https://github.com/Mewgood/postmill>. Accessed October 2026.

Identity Digital. Registry RDAP record for raddle.me. Accessed October 2026. <https://rdap.identitydigital.services/rdap/domain/raddle.me>.

Investigator's correspondence records. Letters to ziq, emma, Flashpoint (via its press contact) and the Anarchist News collective, sent October 19, 2026 (resent October 20), with delivery-status notifications to October 21, 2026. Held by the investigator.

Investigator's monitoring records of Raddle and related sites, October 19–21, 2026: feed captures, page screenshots and change logs with SHA-256 hashes. Held by the investigator.

Matsakis, Louise. "Radical Leftists Built Their Own Reddit After It Banned Them." Vice, September 29, 2017.

<https://www.vice.com/en/article/radical-leftists-built-their-own-reddit-after-it-banned-them/>.

Postmill. CHANGELOG.md, versions 0.2.0 to 2.2.1. <https://gitlab.com/postmill/Postmill/-/blob/main/CHANGELOG.md>.

Proton Mail delivery-status notification for a message of October 19, 2026 to ziq@raddle.me ("connect to mail2.raddle.me[128.199.53.87]:25: Connection timed out," status 4.4.1), generated at 13:40 UTC on October 21, 2026; with the RIPE RDAP record for 128.199.53.87 (DigitalOcean). Held by the investigator.

raddit.me. Front page. Internet Archive captures of May 9, 2017 (staging site radzi.me) and May 10, 2017, 13:32 UTC (20170510133236).

raddit.me. WordPress and BuddyPress site, front, registration and menu pages. Internet Archive captures, December 2016 to May 2017, and archive.today captures of December 15–16, 2016.

raddit.me. WordPress front page. Internet Archive capture of February 4, 2017 (20170204233533).

Raddle. "Moderation Log" (site-wide), 332 pages, 16,565 entries, October 23, 2017 to October 13, 2026. Read October 13 and 15, 2026. https://raddle.me/moderation_log. All counts and percentages in this assessment are the author's tabulation of this log.

Raddle. Public user-profile endpoints for emma, ziq, Defasher, mofongo, BigG and Brick, giving internal user ID and registration time. Accessed October 13, 2026.

Raddle. User page "Tequila_Wolf." Internet Archive captures of December 12, 2019 and August 31, 2020.

Raddle. User pages Tequila_Wolf, An_Old_Big_Tree, Tequilx_Wolf, Marco, foundstone, stacat and triangle. Internet Archive captures of December 12, 2019; August 31, 2020; January 28, 2021; June 8 and November 19, 2021; July 12, 2022; February 22, June 27, August 1, September 18 and November 26, 2024; and archive.today capture oDYu2, February 29, 2020.

Raddle. User profile pages for emma, mofongo, GrimWillow, Fossidarity, Tequila_Wolf and kin: Internet Archive captures from August 2020 to April 2025, and live pages of October 21, 2026, showing registration times and the administrator icon.

<https://raddle.me/user/emma>.

RapidDNS. Historical DNS records for raddle.me. Accessed October 5, 2026. <https://rapiddns.io/subdomain/raddle.me?full=1>. With RIPE NCC RDAP record for 178.62.216.192, <https://rdap.db.ripe.net/ip/178.62.216.192>.

Tucows Inc. "Tucows Inc. Subpoena and Warrant Policy." April 2, 2019. <https://tucowsdomains.com/help/legal-submissions/tucows-inc-subpoena-and-warrant-policy/>.

Tucows Inc. Press release on its agreement to acquire eNom from Rightside. Toronto, January 20, 2017.

Tucows. WHOIS record for raddle.me, database update of October 16, 2026. Via <https://www.whois.com/whois/raddle.me>.

Whoxy. Historical WHOIS records for raddle.me, 2017–2026. <https://www.whoxy.com/raddle.me#history>.

Vendors, buyers and procurement

Brennan Center for Justice and Data for Black Lives. Records released by the D.C. Metropolitan Police Department after litigation filed in 2022, as reported by the Brennan Center, StateScoop and the D.C. Open Government Coalition.

Brennan Center for Justice. "LAPD Social Media Monitoring Documents." Resource page, accessed October 16, 2026.

DarkOwl. "Coronavirus on the darknet Pt 2: The scams keep on coming." April 9, 2020, modified January 21, 2022. <https://www.darkowl.com/blog-content/more-covid-scams-on-the-darknet/>.

Echosec Systems. "Product Updates" ("June 2019 ... Echosec has a new data provider: Raddle.me"). Internet Archive capture of July 18, 2019 (20190718122432). echosec.net/product-updates.

Echosec Systems. "Social Media Monitoring." Internet Archive capture of August 3, 2021. echosec.net/social-media-monitoring.

Echosec Systems. "What Is Raddle.me and Why Should Retailers Care?" Echosec blog, July 9, 2019. Internet Archive capture of July 7, 2021. echosec.net/blog/what-is-raddle.me.

Echosec Systems. "What Is Raddle.me And Why Should Retailers Care?" Internet Archive capture of July 18, 2019 (20190718122251). echosec.net/blog/what-is-raddle.me.

Echosec Systems. Beacon product documentation, “Open Web Sources” list.

EULEX Kosovo. “Awarded Contracts (1st of February 2021 – 31st of August 2021),” contract 2021-PROC-1031. https://www.eulex-kosovo.eu/eul/repository/docs/1195-EULEX_Kosovo_Awarded_Contracts_%281st_of_February_2021_-_31st_of_August_2021%29..pdf.

Federal Procurement Data System. Order 15DDHQ24P00000321, Drug Enforcement Administration, “Echosec Platform (User License),” March 27, 2024. <https://www.fpds.gov/ezsearch/FEEDS/ATOM?FEEDNAME=PUBLIC&q=15DDHQ24P00000321>.

Federal Procurement Data System. Order 15F06722P0000529, Federal Bureau of Investigation, Miami Field Office, Flashpoint licences, May 26, 2022. <https://www.fpds.gov/ezsearch/FEEDS/ATOM?FEEDNAME=PUBLIC&q=15F06722P0000529>.

Federal Procurement Data System. Order 15F06723F0001672, Federal Bureau of Investigation, “Social Exploitation Tool-Flashpoint,” August 31, 2023, \$329,558, via ThunderCat Technology, off NASA SEWP. Retrieved through USAspending, October 21, 2026.

Federal Procurement Data System. Order 15JA5324P00000008, US Attorney’s Office, Eastern District of New York, “Flashpoint Platform Database,” October 24, 2023, \$137,958. Retrieved through USAspending, October 21, 2026.

Federal Procurement Data System. Order 15M10226PA4700305, U.S. Marshals Service, “Flashpoint Identify,” signed September 8, 2026. <https://www.fpds.gov/ezsearch/FEEDS/ATOM?FEEDNAME=PUBLIC&q=15M10226PA4700305>.

Federal Procurement Data System. Task order 47QFCA19F0040, BAE Systems, U.S. Army open-source intelligence support. <https://www.fpds.gov/ezsearch/FEEDS/ATOM?FEEDNAME=PUBLIC&q=47QFCA19F0040>; BAE Systems, “BAE Systems Selected to Provide Open Source Intelligence Support to the U.S. Army,” October 15, 2019, <https://www.baesystems.com/en/article/bae-systems-selected-to-provide-open-source-intelligence-support-to-the-us-army>.

Flashpoint. “Flashpoint Acquires Open-Source Intelligence Leader Echosec Systems.” Business Wire, August 3, 2022. <https://www.businesswire.com/news/home/20220803006063/en/>.

Flashpoint. “Flashpoint Year in Review 2021.” PDF, 2022. https://flashpoint.io/wp-content/uploads/2022/05/Flashpoint_YearinReview_2021.pdf.

Flashpoint. “How CSI-NY Prevented a Synagogue Attack with Flashpoint.” Customer case study. Accessed October 16, 2026.

Flashpoint. “Platform Overview.” PDF, August 2022. <https://flashpoint.io/wp-content/uploads/2022/08/Platform-Overview.pdf>.

gallery-dl, extractor postmill.py, first commit December 12, 2023; ProjectDiscovery nuclei-templates, osint/raddleme.yaml, first commit February 20, 2023; WhatsMyName, wmn-data.json, 2025. GitHub.

Government of Canada. Proactive disclosure of contracts, Department of National Defence contracts with Echosec Systems (2018–2020) and EJ2 Communications (2023). search.open.canada.ca/contracts.

Home Office. “Procurement Card Spend Over £500: September 2017.” GOV.UK. <https://www.gov.uk/csv-preview/5b7ac0c7e5274a44c06361a8/Home-Office-Procurement-Card-Spend-Over-500-September-2017-CSV.csv>.

Houston Landing. “Houston Council Renews Support for Dataminr Social Media Monitoring Tool Used by Police.” February 21, 2024. <https://houstonlanding.org/houston-council-renews-support-for-dataminr-social-media-monitoring-tool-used-by-police/>.

Kelleher, Liv. “Six Weeks after ICE Arrest, Ogden Has No Date for Revised Police Policy.” KUTV, October 9, 2026.

LifeRaft. “Loss Prevention Pros: Why You Should Bookmark Raddle.me.” Internet Archive capture of July 30, 2021. liferaftinc.com/resources/what-is-raddle-me/.

LifeRaft. “What is Raddle.me? A Crucial Tool for Loss Prevention.” LifeRaft blog. <https://liferaftlabs.com/blog/what-is-raddle-me>.

LifeRaft. “What is Raddle.me?” page, returning HTTP 404 on October 21, 2026; earliest Internet Archive capture November 4, 2024. <https://liferaftlabs.com/blog/what-is-raddle-me>.

National Institute of Justice. Award 15PNIJ-23-GG-01382-DOMR, “A Frame Analysis of Violence and Accelerationism in Cognitive Radicalization.” Youngstown State University, September 8, 2023. <https://nij.ojp.gov/funding/awards/15pnij-23-gg-01382-domr>.

Office of the New York State Comptroller. Open Book New York, contracts of the Division of State Police with Consortium Networks LLC, including C002192, “Flashpoint Echosec license subscriptions.” <https://wwe2.osc.state.ny.us/transparency/contracts/contractresults.cfm?ID=238285>.

Office of the New York State Comptroller. Open Book New York, Division of State Police contract C002165 with Skopenow Inc. and amendments, 2023–2026.

Ogden City Police Department. Flock Safety transparency portal. Last updated October 15, 2026. <https://transparency.flocksafety.com/ogden-city-ut-pd>.

Ogden City. “Dark Web Analysis Software RFP,” questions and answers (document 11933), 2020. Third-party copy at <https://www.scribd.com/document/873422944/QandA-Documen-TOR-Browser>.

Ogden City. “RFP Dark Web Software.” Document 11786, February 13, 2020. https://www.ogdencity.gov/DocumentCenter/View/11786/RFP-Dark-Web-Software_FINAL-02-13-2020.

Paladin Risk Solutions. “Social Media Threat Monitoring to Predict and Prevent Mass Violence.” White paper, December 12, 2019. <https://paladinrisksolutions.com/wp-content/uploads/2019/12/Whitepaper-OSINT-Report-threat-monitoring.pdf>.

Public Services and Procurement Canada. CanadaBuys contract history W8484-219879, “7x Echosec Licenses,” Department of National Defence, 2020–2023. <https://canadabuys.canada.ca/en/tender-opportunities/contract-history/w8484-219879/001/pi-008>.

Retail Industry Leaders Association. “#DEFEATTHIS: Beating the Bloggers at Their Own Game.” Webinar slides, June 24, 2020. <https://www.rila.org/getattachment/9ee71fce-96e2-4458-a092-436e9c4eab22/REVISED-FINAL-RILA-SLIDES-for-06242020-WEBINAR.pdf>.

Rogers, Richard Lee. Frames of Misinformation, Extremism, and Conspiracism (FOMEC) monthly reports, January 2023 and June 2023 (Appendix B, “Posts by Platform”). Youngstown State University. <https://www.rogersperspectives.com/tracking-of-extremism-report>.

Social Links. Product and industry pages, including “SL Professional for Maltego” and “Cybersecurity.” Accessed October 9, 2026. <https://sociallinks.io/products/sl-professional/maltego>; <https://sociallinks.io/industries/cybersecurity>; Maltego Transform Hub, “Social Links Pro,” <https://www.maltego.com/transform-hub/social-links-pro/>.

USAspending.gov. Award 70CMSD21P00000038, U.S. Immigration and Customs Enforcement, EJ2 Communications, “Tailored Reporting Services,” April 2, 2021.

USAspending.gov. Award 70CMSD23FR0000083, U.S. Immigration and Customs Enforcement, Blue Tech Inc., “Flashpoint,” July 13, 2023.

USAspending.gov. Award 70CMSD23P00000064, U.S. Immigration and Customs Enforcement, EJ2 Communications (Flashpoint), July 10, 2023 to July 9, 2024. Award ID CONT_AWD_70CMSD23P00000064_7012.

USAspending.gov. Award 70CMSD25FR0000069, U.S. Immigration and Customs Enforcement, ThunderCat Technology (Flashpoint licences), from September 30, 2025. Accessed October 16, 2026. https://www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000069_7012_NNG15SC92B_8000.

USAspending.gov. Award HSCETE14P00033, U.S. Immigration and Customs Enforcement, EJ2 Communications, August 20, 2014.

USAspending.gov. IDV HSHQDC13D00026, “Orders Made Under this IDV,” order 70CMSD24FR0000086, “Flashpoint Software Renewal,” September 30, 2024 to September 29, 2025. https://www.usaspending.gov/award/CONT_IDV_HSHQDC13D00026_7001.

USAspending.gov. Transportation Security Administration orders 70T02021F7554N007 and 70T02022F7554N003 (“Echosec-Beacon Systems User Licenses”); U.S. Marine Corps orders M0026424F0093 and M0026425F0258 (“Flashpoint Echosec”); Federal Bureau of Investigation order 15F06726F0001642 (“CYD Flashpoint,” September 21, 2026).

Utah State Auditor. Transparent Utah, vendor payments by Ogden City to Echosec Systems Ltd, fiscal years 2020 and 2021. transparent.utah.gov.

Vandenack, Tim. “ICE Arrest in Ogden as Police Officer Looks On Sparks Intense City Council Discussion.” KSL, September 2, 2026.

Law, policy and official records

ARTICLE 19. “USA: Terrorism Designation Has Global Consequences for Open Internet and Free Expression.” September 9, 2026. <https://www.article19.org/resources/usa-terrorism-designation-has-global-consequences-for-open-internet-and-free-expression/>.

Bundesverwaltungsgericht. Judgment 6 A 1.19, January 29, 2020, and press release 5/2020 (linksunten.indymedia.de).

Defense Intelligence Agency. “Department of Defense Open Source Intelligence Strategy 2024–2028.” October 2023. <https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf>.

European Parliament and Council. Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence, and Directive (EU) 2023/1544 on legal representatives. Applicable from August 18, 2026.

Federal Bureau of Investigation. Domestic Investigations and Operations Guide, sections on undisclosed participation, as excerpted by the Brennan Center for Justice and reported by The Intercept.

Her Majesty's Inspectorate of Constabulary. "An Inspection of Undercover Policing in England and Wales." October 2014.

No Gods No Masters network. "Transparency Notice: FBI Court Order Relating to AnarchistFederation.net" and follow-up notices on Google subpoenas, July–August 2026. nogodsnomasters.org; mirrored on anarchistnews.org.

Office of the Director of National Intelligence and Central Intelligence Agency. "The IC OSINT Strategy 2024–2026." March 2024. https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

Office of the Director of National Intelligence. "2026 Commercially Available Information Biannual Report." September 2026. https://www.intelligence.gov/assets/documents/cai/2026_CAI_Report_Final.pdf.

OpenAI. "Coordinated disclosure of critical vulnerabilities" ("Patch the Planet"). October 2026. <https://openai.com/index/coordinated-disclosure-of-critical-vulnerabilities/>.

PHP. php-src issue tracker regressions reported against 8.5.12, and follow-up pull request #24479. GitHub. Accessed October 21, 2026. <https://github.com/php/php-src>.

The PHP Group. "Upcoming Critical PHP Security Release" (October 20, 2026) and the security release of October 21, 2026 (PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35). <https://www.php.net/archive/2026.php>.

U.S. Department of State. "Designation of ... Informal Anarchist Federation/International Revolutionary Front ... as Foreign Terrorist Organizations." Public Notice 12865. Federal Register 90 (November 20, 2025): 52552. FR Doc. 2025-20663.

U.S. Department of the Treasury. Press release sb0616 and OFAC recent actions, August 26, 2026. <https://home.treasury.gov/news/press-releases/sb0616>; <https://ofac.treasury.gov/recent-actions/20260826>; Federal Register notice 2026-17724, August 31, 2026, <https://www.govinfo.gov/content/pkg/FR-2026-08-31/html/2026-17724.htm>.

U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities. "Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans," Book III, Final Report, S. Rep. No. 94-755. April 1976. <https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-94755-iii.pdf>.

United Kingdom. Covert Human Intelligence Sources (Criminal Conduct) Act 2021, c. 4, with explanatory notes. legislation.gov.uk.

Washington Examiner. "Anarchist Tech Group Braces in Case It's Next on Trump's Target List." August 31, 2026.

Wiz. "PHP2Shell." Coordinated-disclosure site, with its list of collaborating organisations. Accessed October 21, 2026. <https://www.php2shell.com/>.

Comparator cases

"Autistici/Inventati." Wikipedia, accessed October 9, 2026 (2004 search of the main server by the Italian Postal Police, disclosed in 2005).

BleepingComputer. Report on the Dutch FIOD seizure of more than 800 servers linked to THE.Hosting/WorkTitans, May 2026.

CIVICUS Monitor. Report on the Schwerin court finding on the deployment of a UK undercover officer in Germany, October 10, 2022; Statewatch, January 2022.

Deutscher Bundestag. Drucksache 18/3754 (federal government answer concerning a Hamburg police undercover officer at a community radio station, 2003–2006); taz, January 8, 2015.

Engadget. "Australian Police Posed as Child Abusers for a Dark Web Sting." October 9, 2017. <https://www.engadget.com/2017-10-09-australian-police-child-abuse-dark-web-sting.html>; iTWire, "Qld Cops Ran Child Porn Site for 11 Months to Trap Abusers," <https://itwire.com/security/qld-cops-ran-child-porn-site-for-11-months-to-trap-abusers.html>.

Help Net Security. "Dark Web Hansa Market Shut Down after Being Run for a Month by Law Enforcement." July 20, 2017. <https://www.helpnetsecurity.com/2017/07/20/hansa-market-shut-down/>.

Jungle World. Report on a state-intelligence informant inside the Interventionistische Linke in Bremen, 2026, with the group's public statement.

LRT and The Baltic Times, reporting on the Vilnius Regional Court order of October 3, 2019 (Operation Trojan Shield), September 2025; 404 Media, reporting on defence discovery in ANOM cases, December 2024.

NBC News. Reports on GCHQ's Joint Threat Research Intelligence Group based on documents provided by Edward Snowden, February 2014.

nostate.net. Statement on the seizure of a server by Dutch police at British request, spring 2021.

Reporting on the 2004 FBI-requested seizure of Indymedia servers hosted by Rackspace, the Bristol Indymedia seizures of 2005 and 2014, and the withdrawn 2009 subpoena for visitor IP addresses, as summarised in “Indymedia,” Wikipedia, accessed October 9, 2026.

SC Magazine. “Cybersting: FBI Ran DarkMarket Forum to Catch Cybercriminals.” October 2008.

<https://www.scmagazine.com/news/cybersting-fbi-ran-darkmarket-forum-to-catch-cybercriminals>; NPR, “The FBI Agent ...,” Planet Money, June 17, 2011, <https://www.npr.org/sections/money/2011/06/17/137251254/the-fbi-agent>.

The Canary. Report on Undercover Policing Inquiry evidence concerning officer HN3 (Special Demonstration Squad), March 27, 2026; Campaign Opposing Police Surveillance (COPS), inquiry summaries.

The Intercept. “Deconstructed: FBI Informant Protests.” February 10, 2023.

<https://theintercept.com/2023/02/10/deconstructed-fbi-informant-protests>; Denverite, “How a Local Activist Found Himself Buying a Gun for a Supposed FBI Informant,” February 10, 2023, <https://denverite.com/2023/02/10/how-a-local-activist-found-himself-buying-a-gun-for-a-supposed-fbi-informant/>.

The Intercept. Report on the defacement of Noblogs after the Autistici/Inventati designation, September 10, 2026.

U.S. Air Force. Solicitation RTB220610, “Persona Management Software,” MacDill Air Force Base, June 22, 2010; contract award to Ntrepid as reported in 2011.

United States v. Anzalone, 923 F.3d 1 (1st Cir. 2019). <https://cite.case.law/f3d/923/1/>.

United States v. Monsegur (S.D.N.Y.), docket entry 30.

Washington Times. Report on the trial of Hal Turner, December 1, 2009; Salon, report on Hal Turner’s FBI informant role, November 29, 2009; JTA via New Jersey Jewish News, 2009.

Movement network and hostile monitoring

Anarchist Federation (Scotland). Report on the shutdown of Athens Indymedia, 98FM and Radio Entasi at the National Technical University of Athens, May 7, 2013.

Anarchist News. Announcement of the moderator’s resignation and the editorial collective “thecollective,” August 17, 2015. anarchistnews.org.

CrimethInc. “A Hell of a Mistress, the Beautiful Idea: An Interview with Aragorn!” February 19, 2020.

Cybrigade. Announcement on the shutdown of the espiv.net server at Panteion University, July 7, 2014. English translation by Contra Info.

infolibre.gr. Espiv solidarity statements on the May 21, 2020 shutdown of espiv.net. June 8, 2020.

Kiwi Farms. “raddit.me - It’s like Voat for SJWs.” Thread 29612, March 30 – May 11, 2017. <https://kiwifarms.st/threads/raddit-me.29612/>.

Kiwi Farms. “Raddle- Reddit knockoff for far left larpers.” Thread 66734, February 29, 2020. <https://kiwifarms.st/threads/raddle-reddit-knockoff-for-far-left-larpers.66734/>.

Little Black Cart. “What’s New with LBC - Fall 2019.” November 3, 2019. littleblackcart.com.

The Anarchist Library. Home page. Internet Archive capture of June 5, 2012.

“The Anarchist Media to Come.” Originally posted to Stalking the Earth; republished by It’s Going Down, August 17, 2022.

“Toronto G20 Main Conspiracy Group: The Charges and How They Came To Be.” 2011, edited 2012. Copy held by the No Trace Project.

ziq. “We Need a Strong Anarchist Media Alliance.” Anarchist News, from raddle.me/f/Anarchism/117186, August 2020. Internet Archive capture of May 18, 2021.