Privacy Detection and Response (PDR)™

Why Exploitation of an Individual's Digital-Footprint Makes PDR Fundamental to Privacy Operations, Privacy Governance, and Continuous Risk Reduction

Scott Foote

Last Updated: 11 April 2026

Phenomenati Consulting
www.phenomenati.com

6 Liberty Square, #2736
Boston, MA 02109
(508) 709-7990 (office)

<this page is intentionally blank>

Contents

Executive Thesis

The incident record now shows a repeatable pattern: threat actors use an individual's public or commercially available digital footprint - LinkedIn profiles, public role data, recruiter pretexts, exposed contact details, breached credentials, or executive media - to compromise the person first and their employer second [1]-[17]. The strategic implication is that privacy can no longer remain only a notice-and-retention discipline. The need for a distinct Privacy Detection and Response capability is emerging because organizations need a lawful, continuous way to discover, validate, prioritize, and reduce external personal-data exposure before it is weaponized. The objective is to continuously burn down risk for both the organization and the individual person - staff member, customer, constituent, or other stakeholder - whose data is being targeted [18]-[37].

Executive Summary

The opening evidence for PDR is not theoretical. It is operational. Across the incident record, attackers repeatedly started with a person's external footprint and only then moved into the employer's environment. That pattern appears in recruiter-themed malware campaigns, LinkedIn reconnaissance, help-desk impersonation, credential capture, and AI-enabled executive impersonation [1]-[17].

Those cases matter because they expose a structural gap. Traditional privacy programs have correctly concentrated on lawful basis, notice, minimization, retention, transfers, and internal safeguards. But the same individual whose data is protected inside the enterprise often has a much larger attack surface outside it - across data brokers, people-search sites, breached datasets, public records, social platforms, paste sites, and criminal marketplaces [19]-[23], [29]-[33]. When that external surface is dynamic, the operating model must also be dynamic [18]-[20].

This paper argues that Privacy Detection and Response is the missing operational layer between privacy compliance and real-world harm reduction. PDR is a continuous, risk-based capability that lawfully discovers externally exposed, inferable, leaked, or criminally traded personal data relating to identified people; assesses the likelihood and severity of harm; and orchestrates proportionate response and remediation actions to reduce that harm for both the person and the enterprise [18]-[21], [27]-[30].

For organizations building nascent privacy operations and more mature privacy governance, PDR becomes foundational because it turns privacy into an executable loop: discover, validate, respond, verify, and learn. It also creates the bridge to **Privacy Enhancing Technologies (PET)** and privacy-automation capabilities (via **Privacy Orchestration and Remediation** or **"POAR"™**) that can materially reduce exposure - including automated rights-request orchestration, broker deletion and opt-out workflows, takedown support, credential hardening, and evidence-based verification that the risk has actually gone down [21], [24]-[28], [33]-[36].

1 Incident-Driven Rationale behind the Emergence of PDR

How a Person's Digital Footprint Expands the Enterprise Attack Surface

The strongest justification for PDR is the incident pattern itself. In each case below, the threat actor weaponized information associated with a real person - often a staff member, sometimes an executive - and converted that exposure into compromise against the employer or its assets. The lesson is not merely that social engineering exists. It is that privacy exposure and cyber exposure have converged [1]-[17].

Year	Victim	Footprint Weaponized	Resulting Employer Compromise	Linkage
2011	**RSA Security**	Recruitment-themed spear-phish; post-incident analysis said target data was likely mined from social-networking sites.	Excel/Flash exploit opened a backdoor and led to theft of SecurID-related data [1][2].	Strongly indicated
2020	**Twitter**	LinkedIn scraping to identify staff with access and obtain phone/contact data; phone spear-phishing followed.	Employee credentials and 2FA codes were captured, enabling access to internal tools and takeover of high-profile accounts [3][4].	Direct
2020	**Operation In(ter)ception**	Fake LinkedIn personas initiated contact, built trust, then delivered malicious content under recruiting or business pretexts.	Victim endpoints were compromised, supporting espionage and attempted financial theft against employers [5].	Direct
2022	**Sky Mavis / Ronin Bridge**	Fake LinkedIn recruiters, multiple sham interviews, and a malicious offer PDF sent to a senior engineer.	The compromise gave the attackers access into Sky Mavis' environment, enabling validator control and a bridge theft exceeding $540 million [6][7].	Direct
2022/ 2023	**Spanish aerospace company**	Fake Meta recruiter on LinkedIn sent malicious coding challenges or quizzes to employees.	Execution on a corporate device delivered LightlessCan and gave Lazarus a covert foothold for cyber-espionage [8][9].	Direct
2023	**MGM Resorts International**	Public reporting said attackers used LinkedIn to identify an employee and then impersonated that person to the service desk.	The intrusion cascaded into major hotel and casino outages; MGM later reported roughly a $100 million negative impact on Q3 property EBITDAR [10][11][12].	Direct
2023	**Caesars Entertainment**	Open-source reporting ties the incident to false LinkedIn personas, admin pretexting, and help-desk impersonation.	Unauthorized network access and loyalty-program data theft followed the social-engineering attack on Caesars' IT support path [13][14][15].	Strongly indicated
2024	**Arup (Hong Kong office)**	Publicly available executive video and audio were weaponized into deepfake meeting participants.	An employee transferred HK$200 million after following fake executive instructions in a video call [16][17].	Direct

Table 1: Representative Incidents in which an Individual's External Digital Footprint was Used to Compromise the Employer or its Assets

1.1 What the Incident Record Actually Proves

First, online footprint data is no longer passive background information. It is actionable reconnaissance. Attackers used public professional profiles, role visibility, contact details, or public executive media to choose targets, craft pretexts, and close the trust gap needed for compromise [3]-[5], [8]-[17].

Second, the boundary between the person and the enterprise is porous. Once the threat actor can persuade, impersonate, or compromise the person, the employer inherits the blast radius. That is why privacy exposure affecting a staff member can rapidly become an operational, financial, legal, and reputational event for the organization [1]-[17].

Third, the risk is no longer confined to employees. The same logic applies to customers, constituents, members, patients, donors, and other stakeholders whose identities can be manipulated in ways that create fraud, account takeover, reputational harm, or institutional disruption. PDR therefore belongs not only in workforce security, but in broader privacy and trust strategy [19]-[23], [27]-[28].

Fourth, AI expands the attack surface rather than replacing it. The Arup case shows that publicly available media can now be fused into synthetic but credible executive presence. That means even benign-seeming public artifacts can become attack material when combined with modern impersonation tooling [16][17], [23], [30].

2 Why PDR is Emerging as a Distinct Operating Discipline

Working Definition

Privacy Detection and Response (PDR) is a continuous, risk-based capability that lawfully discovers externally exposed, inferable, leaked, or criminally traded personal data relating to identified individuals; assesses the likelihood and severity of privacy and security harm; and uses the concept of **POAR** to orchestrate proportionate response actions to reduce that harm for both the private individual person and the organization. It must be emphasized that PDR monitors the external privacy attack surface around the person; it does ***not*** license intrusive surveillance into the person's private life [18]-[21], [27]-[28].

PDR has emerged because several trends have now converged. Data brokers and digital platforms continue to aggregate and commercialize granular personal data at scale [22][23]. Criminal ecosystems continue to trade credentials, breach data, stealer-log material, and extortion content, while ENISA has described both a booming initial-access-broker market and a large share of intrusions leading to sale or exposure of stolen data [29][30]. At the same time, regulators are moving from abstract privacy rights toward operational remedies, including broker registration, deletion rights, and large-scale request mechanisms such as California's DROP platform [24]-[26], [37].

The conceptual move is similar to the one security leaders made with EDR. Once defenders accepted that endpoints were continuously exposed and continuously targeted, periodic controls were no longer enough; telemetry, triage, and response became indispensable. Privacy now faces the same reality on a different object of protection. The protected asset is not only a device or *system*. It is a *human being* whose personal data exhaust has become part of the individual's and organization's **attack surface** [18]-[20].

A distinct market category is therefore likely to form around capabilities that many organizations currently assemble only in disjoint fragments: digital-footprint discovery, breach and leak monitoring, lawful broker and people-search removal, identity-hardening workflows, takedown orchestration, rights-request automation, case management, and reporting that proves risk reduction. In other words, the PDR market emerges because the problem has become continuous, measurable, and operationally urgent [1]-[17], [22]-[26], [33]-[36].

2.1 The EDR Analogy - and Where the Analogy Must Stop

Dimension	EDR	PDR
Protected Asset	Endpoint, workload, or device	Person, identity surface, and associated privacy context
Telemetry	Processes, files, registry, network behavior, agent signals	Approved identity attributes, broker records, breach hits, leaked credentials, paste records, public exposure signals
Primary Response	Contain, isolate, eradicate, reimage, recover	Remove, opt out, takedown, notify, harden accounts, support the person, document outcome
Core Metric	Mean time to detect and respond	Mean time to detect, remove, and materially reduce exposure
Critical Constraint	Operational continuity	Human dignity, legality, proportionality, and trust

Table 2: PDR Borrows the Operating Rhythm of EDR,

The EDR analogy is useful because it gives privacy leaders an operational vocabulary: telemetry, detection, triage, response, and continuous improvement. But the analogy must stop where human beings begin.

An *endpoint* can often be rebuilt; a person's *identity*, home address history, family exposure, or reputational harm cannot. For that reason, PDR must be more conservative, more transparent, and more humane than many traditional monitoring models [18][19][21][27].

2.2 What cannot be Deleted can at least be Degraded

Where aggregated PII cannot be deleted, one defensive technique which this author has advocated for since prior to 2016 is to lawfully "*poison*" the personal data that is being aggregated in these digital platforms and criminal ecosystems by strategically *dis*-informing the collectors and data pipelines that feed them - *obfuscating* the real data and systematically reducing the *value* of the data over time.

3 PDR as a Foundational Capability within Privacy Operations

Privacy Operations is the *execution* layer of the privacy program: intake, triage, rights handling, case management, remediation, coordination, and measurement. PDR belongs here because it provides the continuous discovery and response loop that ordinary policy artifacts cannot provide on their own. A privacy office can publish a retention rule; it cannot thereby remove a broker listing, detect a stealer-log hit, verify the reappearance of exposed credentials, or coordinate a rapid response for an overexposed executive or vulnerable customer. PDR supplies that missing operational muscle [19]-[21], [24]-[28], [33]-[36].

Operational Element	What PDR Adds	Risk Reduction Effect
Intake and Detection	Continuous monitoring of approved surface-web and dark-web sources for exposures tied to defined people or cohorts.	Earlier discovery of exploitable exposure before phishing, fraud, or compromise occurs.
Triage and Prioritization	Case scoring based on sensitivity, exploitability, breadth, context, recency, and confidence.	Attention goes first to exposures most likely to harm the individual and the enterprise.
Remediation Orchestration	Broker deletions, takedown support, rights-request workflows, account hardening, credential resets, fraud controls, and escalation.	Exposure is reduced rather than merely observed.
Verification and Recurrence Tracking	Evidence that the listing was removed, the credential was rotated, or the data reappeared elsewhere.	Measures whether risk actually went down and stayed down.
People-Centered Assistance	Notice, support, and escalation pathways for staff, customers, constituents, and stakeholders affected by verified exposure.	Improves resilience, trust, and duty-of-care outcomes.

Table 3: In Privacy Operations, PDR Turns Exposure Discovery into a Repeatable Response Workflow

That people-centered point is essential. Properly designed, PDR is ***not*** a program for catching employees out. It is a protective control that treats *the monitored person* as the *beneficiary* of the workflow. The aim is to reduce attackability, not to expand surveillance. That is why the ***operating objective*** should always be framed in dual terms: continuously **reduce measurable risk** to the **organization** and continuously **reduce measurable harm** potential to the private **individual person** [19][21][27][28].

In practice, that makes PDR especially valuable for **three cohorts**. The ***first*** is *executives* and highly visible staff, because their public role data and media presence are unusually rich. The ***second*** is the *workforce* more broadly, because leaked credentials, home-contact data, and oversharing patterns can be transformed into phishing and service-desk abuse. The ***third*** is *external populations* - customers, constituents, patients, members, donors, students, and other stakeholders – but *only* when the organization has both sufficient legal basis and a genuine ***duty of care*** to assist them [1]-[17], [21], [27]-[28].

4 PDR as a Foundational Capability within Privacy Governance

If **Privacy Operations** is the *execution* layer, **Privacy Governance** is the *authority* layer. Governance determines whether PDR is lawful, proportionate, explainable, and trusted. Without governance, continuous monitoring of personal-data exposure can drift into overcollection, imprecise matching, unnecessary retention, or uses that undermine the very privacy interests the program claims to protect [19]-[21], [27]-[28], [35]-[36].

Governance therefore has to answer several threshold questions before scale: who is in ***scope***; what ***legal basis*** supports monitoring and response; which ***sources*** are *approved*; which ***attributes*** may be used for matching; what ***level of confidence*** triggers action; which ***cases*** require *human review*; what ***retention limits*** apply; how are vendor sources ***vetted***; and how are *benefit*, *necessity*, and *proportionality* demonstrated for each monitored cohort [19]-[21], [27]-[28].

Governance Question	Why it Matters	Typical Control
Purpose and Lawful Basis	PDR must operate as a protective privacy and security control, not an open-ended intelligence program.	Documented purpose statements, legal review, records of processing, and transparency language [21][27][28].
Source Policy	Not every accessible source should be monitored; relevance and legality matter.	Approved-source catalog, vendor due diligence, prohibited-source rules, and access controls [21][27].
Identity Matching Discipline	False positives can create fresh privacy harm or misdirect remediation.	Conservative matching logic, confidence thresholds, and human review for high-impact cases [19][20].
Data Handling and Retention	PDR findings may themselves contain sensitive exposure data.	Role-based access, case logging, minimization, and retention schedules [19][21].
Escalation and Accountability	Response often crosses privacy, security, legal, HR, fraud, and customer teams.	Defined playbooks, ownership matrix, approval thresholds, and executive reporting.

Table 4: Governance Determines Whether PDR Remains Lawful, Proportionate, and Trusted as it Scales.

The crucial governance principle is simple: *the person must remain the beneficiary of the control*. If a PDR program cannot explain how it reduces harm to the monitored individual - not only to the enterprise - then it has not been designed correctly. The program should increase trust, reduce exposure, and support lawful remediation. If it becomes a covert instrument for employee monitoring or unjustified profiling, it defeats its own purpose [19][21][27][28].

5 POAR and PET-Enabled Response and Remediation

This is where PDR moves from detection to burning down risk.

The practical value of PDR appears only when detection is connected to action. That is where Privacy Enhancing Technologies (PET) and privacy-automation capabilities (e.g., Privacy Orchestration and Remediation or POAR™) matter. In the narrow technical sense, PETs include techniques such as differential privacy, secure multiparty computation, trusted execution environments, privacy-enhancing cryptography, pseudonymization, and other methods that minimize unnecessary exposure of personal information [35][36]. In the broader operational sense relevant here, organizations also need PET-informed automation that helps remove, suppress, or reduce externally exploitable exposure once it has been found [21], [24]-[26], [35]-[36].

The clearest example of a POAR or most specifically PDR capability is automated rights-request orchestration. A mature PDR capability should not stop at finding a broker listing or people-search exposure. It should be able to launch and track the lawful remediation path - whether that is a data subject access or consumer-rights workflow, an erasure or deletion request, an opt-out, a correction request, or another approved legal mechanism. California's DROP platform is especially important because it demonstrates the direction of travel: a single verified workflow can route deletion requests across a very large broker population instead of forcing the private individual person to fight the market one broker at a time [24]-[26], [37].

Response / Remediation Capability	How it Supports PDR	Illustrative Authority or Enabling Source
Automated Deletion and Opt-Out Requests	Converts a detected broker or people-search exposure into a tracked removal workflow.	GDPR rights framework; California DROP / Delete Act; broker due-diligence obligations [21], [24]-[27], [37].
Subject Access / Consumer-Rights Orchestration	Allows detection events to trigger lawful access, correction, deletion, or objection workflows where appropriate.	GDPR; EDPB breach and data-subject guidance context [21][28].
Credential and Breach Monitoring	Identifies exposed email addresses, breach appearances, and stealer-log-related signals so accounts can be hardened quickly.	Have I Been Pwned operational model and APIs [33][34].
Identity-Hardening Automation	Drives password resets, MFA or passkey rollout, aliasing, and reduced discoverability for high-risk people.	NIST continuous risk management and privacy-engineering approaches [19][20][36].
Verification and Recurrence Analytics	Confirms that a removal succeeded and detects if the same data reappears elsewhere.	Necessary for proving that risk went down rather than simply generating tickets.

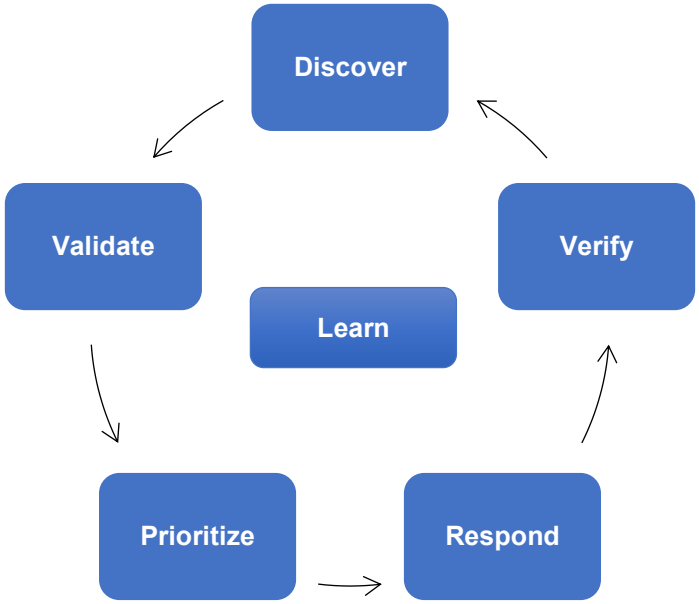
Table 5: PETs and privacy automation help PDR convert a detected exposure into a measurable reduction in risk.

This is the bridge from Privacy Detection and Response to Privacy Operations and Privacy Governance. Governance authorizes the workflow and sets the boundaries. Operations executes the workflow. PETs and privacy automation make the workflow scalable enough to matter. Together, they create a practical way to burn down risk that would otherwise remain scattered across policy documents, manual spreadsheets, and ad hoc remediation efforts [19]-[21], [24]-[28], [35]-[36].

6 Operating Model and Measures of Success

A usable PDR program runs as a loop rather than a one-time project. It discovers exposures, validates them, prioritizes the ones most likely to create real harm, responds through approved playbooks, verifies the outcome, and then learns from recurrence patterns. That loop is how privacy becomes ***operational*** rather than merely ***declarative*** [19][20].

Figure 1: The Core PDR Loop



What matters is not alert volume. It is ***measurable exposure reduction***. For the organization, that means fewer high-severity external exposures tied to sensitive cohorts, shorter dwell time for harmful listings, faster removal of broker records, fewer verified reused credentials after exposure, and fewer cases in which a person's public footprint can be used to impersonate the organization. For the individual person, it means fewer exposed identifiers, shorter duration of public discoverability, faster support when a breach or broker listing appears, lower repeat exposure, and higher confidence that the organization is acting as a *protector* rather than a *passive observer* [1]-[17], [19]-[21], [24]-[28].

A mature **privacy scorecard** should therefore include at least these **measures**:

- percentage of monitored people with high-severity external exposures;
- median time to detect verified exposure;
- median time to remove or suppress harmful data;
- percentage of verified exposures remediated through deletion, takedown, or hardening;
- recurrence rate for removed data;
- false-positive rate of the matching engine; and
- user-assistance completion rates for staff, customers, constituents, and stakeholders receiving support.

Those are the kinds of metrics that show whether risk is actually burning down [19]-[21], [24]-[28], [33]-[36].

Conclusion

The list of incidents of digital-footprint exploitation at the front of this paper should be read as market evidence, not isolated anecdotes. They show that an individual's external data exposure can now be weaponized into enterprise compromise with disturbing regularity. That operating reality creates demand for a dedicated discipline able to discover, validate, prioritize, and remediate personal-data exposure continuously rather than episodically [1]-[17].

That discipline is Privacy Detection and Response. For organizations building or maturing Privacy Operations and Privacy Governance, PDR (including POAR to activate relevant PET) is likely to become fundamental because it closes the gap between policy and protection. It gives the enterprise a lawful, measurable way to reduce external privacy attack surface, support the affected person, and prove that response actions materially lowered risk. In that sense, PDR is not simply another privacy slogan. It is the people-centered operational layer that lets the organization continuously reduce risk for itself and for the individual human beings connected to it [18]-[37].

In One Sentence

Endpoint Detection and Response protects devices from compromise; Privacy Detection and Response protects people - and therefore the organizations connected to them - from the harms created when personal data becomes externally exposed, inferable, or traded.

References

[1] "RSA/EMC: Anatomy of a compromise," SANS Internet Storm Center Diary. https://isc.sans.edu/diary/10645

[2] "RSA discloses phishing-attack data breach details," ComputerWeekly. https://www.computerweekly.com/news/1280095593/RSA-discloses-phishing-attack-data-breach-details

[3] "An update on our security incident," X (formerly Twitter) Blog. https://blog.x.com/en_us/topics/company/2020/an-update-on-our-security-incident

[4] Dan Goodin, "Twitter hackers used phone spear phishing in mass account takeover," Ars Technica. https://arstechnica.com/information-technology/2020/07/twitter-hackers-used-phone-spear-phishing-in-mass-account-takeover/

[5] "Operation In(ter)ception: Starting with a LinkedIn message, threat actors went after both secret information and money," ESET. https://www.eset.com/gr-en/about/newsroom/press-releases-1/operation-interception-starting-with-a-linkedin-message-threat-actors-went-after-both-secret-inf-3/

[6] "Back to Building: Ronin Security Breach Postmortem," Ronin / Sky Mavis. https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364

[7] "How a fake job offer took down the world's most popular crypto game," The Block. https://www.theblock.co/post/156038/how-a-fake-job-offer-took-down-the-worlds-most-popular-crypto-game

[8] "ESET Research: North Korea-linked Lazarus impersonates Meta on LinkedIn to attack an aerospace company in Spain," ESET. https://www.eset.com/us/about/newsroom/press-releases/north-korea-linked-lazarus-impersonates-meta-on-linkedin-to-attack-an-aerospace-company-in-spain/

[9] "Lazarus luring employees with trojanized coding challenges: the case of a Spanish aerospace company," WeLiveSecurity / ESET. https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/

[10] "MGM reeling from cyber chaos 5 days after attack as experts say issue could last weeks," ABC News. https://abcnews.go.com/Business/mgm-reeling-cyber-chaos-5-days-after-attack/story?id=103148809

[11] "MGM Resorts breached by Scattered Spider hackers," Reuters. https://www.reuters.com/technology/moodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13/

[12] MGM Resorts International 2023 Form 10-K. U.S. SEC filing. https://www.sec.gov/Archives/edgar/data/789570/000078957024000005/mgm-20231231.htm

[13] Caesars Entertainment data-breach notification (Maine Attorney General viewer). https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml

[14] "Scattered Spider: Three things the news does not tell you," BleepingComputer. https://www.bleepingcomputer.com/news/security/scattered-spider-three-things-the-news-doesnt-tell-you/

[15] "MGM/CAESARS Cyber Incident Analysis," Guy Carpenter. https://www.guycarp.com/content/dam/guycarp-rebrand/insights-images/2024/02/2024_2_Casino_Incident_Analysis_publish.pdf

[16] "Cybercrime: Lessons learned from a $25m deepfake attack," World Economic Forum. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

[17] "Everyone looked real: multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video conference," South China Morning Post. https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage

[18] NIST, "Architecture and Builds - Implementing a Zero Trust Architecture." https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html
[19] NIST, "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Version 1.0)." https://csrc.nist.gov/pubs/cswp/10/nist-privacy-framework-version-10/final
[20] NIST SP 800-37 Rev. 2, "Risk Management Framework for Information Systems and Organizations." https://csrc.nist.gov/pubs/sp/800/37/r2/final
[21] Regulation (EU) 2016/679 (GDPR), official text. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[22] FTC, "Data Brokers: A Call for Transparency and Accountability." https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014
[23] FTC, "A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services." https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services
[24] California Privacy Protection Agency, "Delete Request and Opt-out Platform (DROP)." https://privacy.ca.gov/drop/
[25] California Privacy Protection Agency, "About DROP and the Delete Act." https://privacy.ca.gov/drop/about-drop-and-the-delete-act/
[26] FTC, "FTC Reminds Data Brokers of Their Obligations to Comply with PADFAA." https://www.ftc.gov/news-events/news/press-releases/2026/02/ftc-reminds-data-brokers-their-obligations-comply-padfaa
[27] ICO, "Organisations using marketing services of data brokers." https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/organisations-using-marketing-services-of-data-brokers/
[28] EDPB, "Guidelines 9/2022 on personal data breach notification under GDPR." https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en
[29] ENISA, "ENISA Threat Landscape 2023." https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
[30] ENISA, "ENISA Threat Landscape 2025." https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf
[31] CISA, "#StopRansomware: Medusa Ransomware" (AA25-071A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a
[32] CISA, "#StopRansomware: Play Ransomware" (AA23-352A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
[33] Have I Been Pwned. https://haveibeenpwned.com/
[34] Have I Been Pwned API v3. https://haveibeenpwned.com/api/v3
[35] ICO, "Privacy-enhancing technologies (PETs)." https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
[36] NIST, "PETs Testbed." https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/pets-testbed
[37] California Privacy Protection Agency, "CalPrivacy Celebrates Data Privacy Week with Practical Tools Like DROP."