

anonym.legal

T1 — LINKABILITY

10 Case Studies — Problem Analysis & Solution Architecture

SOLID — Directly addressable through technical measures

Generated: February 2026
Source: anonym.community
Product version: Desktop 7.4.4

Table of Contents

01 Browser fingerprinting

Evidence refs: 2.5, 8.4, 10.3, 10.4

02 Quasi-identifier re-identification

Evidence refs: 13.3, 15.4

03 Metadata correlation

Evidence refs: 6.10, 8.3, 9.1, 9.7

04 Phone number as PII anchor

Evidence refs: 9.2

05 Social graph exposure

Evidence refs: 9.3

06 Behavioral stylometry

Evidence refs: 8.8, 12.3

07 Hardware identifiers

Evidence refs: 8.9

08 Location data

Evidence refs: 2.9

09 RTB broadcasting

Evidence refs: 2.3

10 Data broker aggregation

Evidence refs: 1.4

Transistor: T1 — LINKABILITY

Definition: The ability to connect two pieces of information to the same person.

01. Browser fingerprinting

Evidence refs: 2.5, 8.4, 10.3, 10.4

[Executive Summary](#)

Browser fingerprinting represents a critical privacy challenge: Linking device attributes into a unique identity — screen, fonts, WebGL, canvas combine into a fingerprint identifying 90%+ of browsers. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Linking device attributes into a unique identity — screen, fonts, WebGL, canvas combine into a fingerprint identifying 90%+ of browsers

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including device identifiers, advertising IDs, tracking cookies, user agent strings. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Redact is recommended: completely removing fingerprint-contributing values eliminates the data points that algorithms combine into unique identifiers. Replace provides an alternative — substituting with non-unique alternatives prevents cross-device correlation while preserving document readability. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 5(1)(c) data minimization, ePrivacy Directive tracking consent. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

02. Quasi-identifier re-identification

Evidence refs: 13.3, 15.4

[Executive Summary](#)

Quasi-identifier re-identification represents a critical privacy challenge: 87% of the US population identifiable by zip code + gender + date of birth alone. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

87% of the US population identifiable by zip code + gender + date of birth alone. Netflix Prize dataset de-anonymized via IMDB correlation

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including zip codes, dates of birth, gender markers, demographic quasi-identifiers. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Hash is recommended: deterministic SHA-256 hashing enables referential integrity across datasets while preventing re-identification from original values. Replace provides an alternative — substituting quasi-identifiers with type labels removes re-identification potential while preserving data structure. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Recital 26 identifiability test, Article 89 research safeguards. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

03. Metadata correlation

Evidence refs: 6.10, 8.3, 9.1, 9.7

[Executive Summary](#)

Metadata correlation represents a critical privacy challenge: Linking who/when/where without content — 'we kill people based on metadata' (former NSA director). This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Linking who/when/where without content — 'we kill people based on metadata' (former NSA director)

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including email addresses, timestamps, IP addresses, communication metadata, geolocation markers. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing metadata fields entirely prevents correlation attacks that link communication patterns to individuals. Mask provides an alternative — partial masking preserves format for system compatibility while breaking linkability. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 5(1)(f) integrity and confidentiality, ePrivacy Directive metadata restrictions. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

04. Phone number as PII anchor

Evidence refs: 9.2

[Executive Summary](#)

Phone number as PII anchor represents a critical privacy challenge: Linking encrypted communications to real-world identity via mandatory SIM registration in 150+ countries. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Linking encrypted communications to real-world identity via mandatory SIM registration in 150+ countries

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including phone numbers, IMSI numbers, SIM identifiers, mobile network codes. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Replace is recommended: substituting phone numbers with format-valid but non-functional alternatives maintains data structure while removing the PII anchor. Hash provides an alternative — deterministic hashing enables referential integrity across phone-linked records. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 9 special category data in sensitive contexts, ePrivacy Directive. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

05. Social graph exposure

Evidence refs: 9.3

[Executive Summary](#)

Social graph exposure represents a critical privacy challenge: Contact discovery maps entire relationship networks — personal, professional, medical, legal, political. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Contact discovery maps entire relationship networks — personal, professional, medical, legal, political

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including names, email addresses, phone numbers, social media handles, organizational affiliations. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing contact identifiers from documents prevents construction of social graphs from document collections. Replace provides an alternative — substituting names and identifiers with type labels preserves document structure while breaking the social graph. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The Desktop App (Windows 10+, macOS 10.15+, Ubuntu 20.04+) processes files locally with encrypted vault storage (AES-256-GCM). Files never uploaded — only extracted text is processed.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 5(1)(c) data minimization, Article 25 data protection by design. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

06. Behavioral stylometry

Evidence refs: 8.8, 12.3

[Executive Summary](#)

Behavioral stylometry represents a critical privacy challenge: Writing style, posting schedule, timezone activity uniquely identify users even with perfect technical anonymization. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Writing style, posting schedule, timezone activity uniquely identify users even with perfect technical anonymization. 90%+ accuracy from 500 words

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including text content, writing patterns, timestamps, posting metadata, timezone indicators. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Replace is recommended: replacing original text content with anonymized alternatives disrupts the stylometric fingerprint that writing analysis algorithms depend on. Redact provides an alternative — removing text content entirely prevents any stylometric analysis though it reduces document utility. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The Desktop App (Windows 10+, macOS 10.15+, Ubuntu 20.04+) processes files locally with encrypted vault storage (AES-256-GCM). Files never uploaded — only extracted text is processed.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 4(1) personal data extends to indirectly identifying information including writing style. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

07. Hardware identifiers

Evidence refs: 8.9

[Executive Summary](#)

Hardware identifiers represents a critical privacy challenge: MAC addresses, CPU serials, TPM keys — burned into hardware, persistent across OS reinstalls, the ultimate cookie. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

MAC addresses, CPU serials, TPM keys — burned into hardware, persistent across OS reinstalls, the ultimate cookie

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including MAC addresses, device serial numbers, CPU identifiers, TPM keys, hardware UUIDs. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Redact is recommended: completely removing hardware identifiers from documents and logs eliminates persistent tracking anchors that survive OS reinstalls. Hash provides an alternative — hashing hardware identifiers enables device-level analytics without exposing actual serial numbers. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 4(1) device identifiers as personal data, ePrivacy Article 5(3). anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

08. Location data

Evidence refs: 2.9

[Executive Summary](#)

Location data represents a critical privacy challenge: 4 spatiotemporal points uniquely identify 95% of people. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

4 spatiotemporal points uniquely identify 95% of people. Used to track abortion clinic visitors, protesters, military

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including GPS coordinates, street addresses, zip codes, city names, country codes. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Replace is recommended: substituting location data with generalized alternatives preserves geographic context while preventing individual tracking. Mask provides an alternative — truncating coordinate decimal places reduces precision while maintaining regional utility. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 9 when location reveals sensitive activities, Article 5(1)(c) minimization. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

09. RTB broadcasting

Evidence refs: 2.3

[Executive Summary](#)

RTB broadcasting represents a critical privacy challenge: Real-time bidding broadcasts location + browsing + interests to thousands of companies, 376 times per day per European user. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Real-time bidding broadcasts location + browsing + interests to thousands of companies, 376 times per day per European user

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including advertising IDs, cookie identifiers, browsing interests, location markers, bid request parameters. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing PII before it enters advertising pipelines prevents the 376-times-daily broadcast of personal information. Replace provides an alternative — substituting identifiers with non-trackable alternatives enables advertising analytics without individual targeting. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 6 lawful basis, ePrivacy Directive consent for tracking, Article 7 consent conditions. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

10. Data broker aggregation

Evidence refs: 1.4

[Executive Summary](#)

Data broker aggregation represents a critical privacy challenge: Acxiom, LexisNexis combine hundreds of sources — property records, purchases, app SDKs, credit cards — into comprehensive profiles. This pain point is driven by LINKABILITY — the ability to connect two pieces of information to the same person. anonym.legal addresses this through 260+ entity types with 3-layer hybrid detection accessible via 6 platforms including Chrome Extension for real-time browser anonymization.

[The Problem](#)

Acxiom, LexisNexis combine hundreds of sources — property records, purchases, app SDKs, credit cards — into comprehensive profiles

Root cause: T1 — LINKABILITY: The ability to connect two pieces of information to the same person.

[The Solution: How anonym.legal Addresses This](#)

[Detection Capabilities](#)

anonym.legal identifies 260+ entity types including names, addresses, financial records, purchase history, app usage data, credit information. The 3-layer hybrid (Presidio + NLP + Stance classification) architecture uses Microsoft Presidio deterministic rules with checksum validations (Luhn, RFC-822) for structured identifiers and XLM-RoBERTa + Stanza NER with Stance classification for disambiguation for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing identifiers before data leaves organizational boundaries prevents contribution to cross-source aggregation profiles. Hash provides an alternative — hashing identifiers enables internal analytics while preventing external parties from matching records. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The REST API (Basic plan+, €3/month) provides programmatic PII detection with Bearer token auth. Rate limited to 100 req/min, max 100 KB per request — the most accessible API entry point in the ecosystem.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 5(1)(b) purpose limitation, Article 5(1)(c) minimization, CCPA opt-out rights. anonym.legal's GDPR, HIPAA, PCI-DSS, ISO 27001 compliance coverage, combined with Hetzner Germany, ISO 27001 certified hosting, provides documented technical measures for regulatory submissions.

Product Specifications

Desktop Version 7.4.4

Entity Types 260+

Detection Layers 3-layer: Presidio + NLP +
Stance classification

Accuracy 95.5% tested (42/44 tests)

Languages 48

Anonymization Methods Replace, Redact,
Mask, Hash (SHA-256/512/MD5), Encrypt
(AES-256-GCM)

Platforms Web App, Desktop, Office Add-in,
MCP Server, Chrome Extension, REST API

Pricing Free €0, Basic €3, Pro €15,
Business €29

Hosting Hetzner Germany, ISO 27001

Compliance GDPR, HIPAA, PCI-DSS, ISO
27001

Other Products Addressing This Transistor

- anonymize.solutions (Umbrella platform)
- cloak.business (Air-gapped desktop)
- anonym.plus (Licensed desktop)

Online versions available at:

<https://anonym.community/anonym.legal/>

© 2026 curta.solutions & anonym.legal. All rights reserved.

