cloak.business

T1 — LINKABILITY

10 Case Studies — Problem Analysis & Solution Architecture

SOLID — Directly addressable through technical measures

Generated: February 2026
Source: anonym.community
Product version: Analyzer 6.9.1 / Image Redactor 5.3.0

Table of Contents

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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including device identifiers, advertising IDs, tracking cookies, user agent strings. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 5(1)(c) data minimization, ePrivacy Directive tracking consent. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 certified hosting, provides documented technical measures for regulatory submissions.

T1 LINKABILITY — Case Study 2 of 10

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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including zip codes, dates of birth, gender markers, demographic quasi-identifiers. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Recital 26 identifiability test, Article 89 research safeguards. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 certified hosting, provides documented technical measures for regulatory submissions.

T1 LINKABILITY — Case Study 3 of 10

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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including email addresses, timestamps, IP addresses, communication metadata, geolocation markers. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 5(1)(f) integrity and confidentiality, ePrivacy Directive metadata restrictions. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including phone numbers, IMSI numbers, SIM identifiers, mobile network codes. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 9 special category data in sensitive contexts, ePrivacy Directive. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 certified hosting, provides documented technical measures for regulatory submissions.

T1 LINKABILITY — Case Study 5 of 10

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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including names, email addresses, phone numbers, social media handles, organizational affiliations. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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+, Tauri/Rust) processes documents locally. Combined with zero-storage server architecture, PII is processed and immediately discarded.

Compliance Mapping

This pain point intersects with GDPR Article 5(1)(c) data minimization, Article 25 data protection by design. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including text content, writing patterns, timestamps, posting metadata, timezone indicators. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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+, Tauri/Rust) processes documents locally. Combined with zero-storage server architecture, PII is processed and immediately discarded.

Compliance Mapping

This pain point intersects with GDPR Article 4(1) personal data extends to indirectly identifying information including writing style. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including MAC addresses, device serial numbers, CPU identifiers, TPM keys, hardware UUIDs. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 4(1) device identifiers as personal data, ePrivacy Article 5(3). cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including GPS coordinates, street addresses, zip codes, city names, country codes. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 9 when location reveals sensitive activities, Article 5(1)(c) minimization. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including advertising IDs, cookie identifiers, browsing interests, location markers, bid request parameters. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 6 lawful basis, ePrivacy Directive consent for tracking, Article 7 consent conditions. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 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. cloak.business addresses this through 390+ entity types with 317 custom regex recognizers, processed in-memory on German servers with zero third-party data sharing.

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 cloak.business Addresses This

Detection Capabilities

cloak.business identifies 390+ entity types including names, addresses, financial records, purchase history, app usage data, credit information. The dual-layer (317 custom regex + NLP) architecture uses 317 custom regex recognizers with context word analysis and confidence scoring 0.0–1.0 for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) — all self-hosted 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 (Business plan) provides programmatic access to 317 custom regex recognizers and 3 NLP engines. Session-based JWT auth for web/desktop; Bearer API key for MCP/REST integration.

Compliance Mapping

This pain point intersects with GDPR Article 5(1)(b) purpose limitation, Article 5(1)(c) minimization, CCPA opt-out rights. cloak.business's GDPR (Article 25 Privacy by Design), ISO 27001:2022 compliance coverage, combined with Germany only, no third-party transfers, ISO 27001:2022 certified hosting, provides documented technical measures for regulatory submissions.

Product Specifications

Platform Version Analyzer 6.9.1, Image Redactor 5.3.0

Entity Types 390+ (519 documented)

Detection Layers 317 custom regex + 3 NLP engines (all self-hosted)

Languages 48 UI languages, 37 OCR language packs

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

Architecture Zero-storage microservices (in-memory only)

Integration Points Web App, Desktop, Office Add-in, MCP Server (9 tools), REST API

Hosting Germany only, ISO 27001:2022, no third-party transfers

Compliance GDPR Article 25, ISO 27001:2022

Other Products Addressing This Transistor

- anonymize.solutions (Umbrella platform)
- anonym.legal (Cloud platform)
- anonym.plus (Licensed desktop)

Online versions available at:
https://anonym.community/cloak.business/