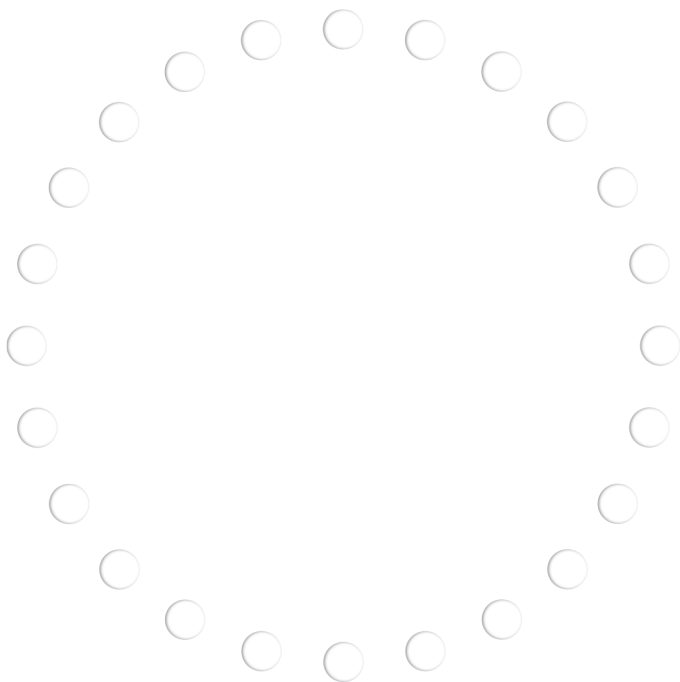


The Politics of Privacy

Autonomy and Power in the Digital Age



web3privacy  **now**

This anthology was commissioned and produced
by Web3Privacy Now.

First published in 2026

ISBN 9789083716701

Edited by	Martina Francesca Cavalot
Curated by	Piergiorgio Catti De Gasperi
Proofread by	Mariquita de Boissière
Printed by	SYL in Spain

Foreword

Privacy is a fundamental human right, enshrined in national constitutions and upheld by international law and social norms that protect our personal freedoms. Across civilisations and political systems, human beings have carved out protected spaces – legal, social, and architectural – within which thought, belief, intimacy, and dissent could develop. Long before we formally recognised privacy as a constitutional right, it was embedded in social practice: the sanctity of the home, the secrecy of correspondence, the confidentiality of confession, the anonymity of the ballot, the protection of sources, and the privacy of association, to name but a few. These customs were not incidental; they were structural features that enabled individual and collective liberty. Democracy depends on such protected spaces. Citizens must be able to deliberate without coercion, think without fear, assemble without surveillance, and vote without exposure. Autonomy, the capacity to form one's own judgments and pursue one's own conception of the good, requires a realm shielded from observation and manipulation. Without privacy, conscience withers, dissent becomes dangerous, and conformity becomes rational.

Modern constitutional democracies eventually codified these insights. The architects of liberal orders understood that unchecked power – whether monarchical, bureaucratic, or majoritarian – thrives on information asymmetry. The right 'to be left alone', famously articulated by Louis Brandeis and Samuel Warren, recognised that privacy is not merely about secrecy; it is about the distribution of power.¹ To observe is to

1

Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 4, no. 5 (1890): 193.

influence. To track and collect data is to accumulate leverage. To eliminate private space is to narrow the boundaries of freedom. For centuries, social norms, physical constraints, and technological limits reinforced privacy by default. With surveillance costly, information fragmented, and memory fallible, forgetting was natural. The effort required to monitor entire populations imposed practical limits on control.

That world no longer exists: the digital age has reversed those conditions. Today, our communications, movements, purchases, preferences, relationships, and even biometric data are continuously recorded, aggregated, analysed, and monetised. What was once ephemeral is now permanent. What was once local is now global. What was once private by nature is now public by design. Our interactions are increasingly mediated by algorithmic systems optimised not for autonomy and well-being, but for prediction, manipulation, and profit. Data brokers construct behavioural profiles, platforms curate information environments, and automated systems shape opportunities, visibility, and reputation. These processes often operate beyond conscious awareness, meaningful consent, or democratic oversight.

When behavioural data drives economic and political targeting, manipulation becomes scalable. By filtering democratic discourse through opaque algorithms, public reason itself is reshaped. The erosion of privacy thus threatens not only individual dignity but the structural conditions of democracy: equality, accountability, pluralism, and freedom of thought. As the new technological revolution unfolds, the frameworks designed to safeguard rights in earlier eras are struggling to keep pace. Legal doctrines built for paper records and physical searches lag behind real-time data extraction and machine learning. Regulatory systems remain largely national, while digital authority is transnational. Meanwhile, concentrated corporate actors command unprecedented informational dominance, redefining markets, media, and political discourse.

Before our eyes, a profound sociopolitical and anthropological transformation is underway.

This volume is the first in a series bringing together social scientists, technologists, philosophers, jurists, and social activists to analyse and confront this transformation. The purpose of this collaborative work is to critically examine the state of personal freedom in the digital age, renew its meaning, and issue an urgent call to action to safeguard it. In other words, *The Politics of Privacy* sets out to:

- 1 Expose the structural threats posed by surveillance capitalism, democratic erosion, technocratic governance, and the concentration of digital resources.
- 2 Reassess autonomy as the cornerstone of democratic rights and adapt its meaning for the digital era.
- 3 Propose concrete cultural, institutional, technical, and policy responses capable of restoring balance between power and freedom.

No single discipline can solve this challenge; no single reform will suffice. A concerted effort is needed to ensure that technological progress does not outpace moral and political wisdom. *The Politics of Privacy* demands intellectual pluralism and coordinated action across legal systems, technological design, civic culture, and democratic institutions. Only through such an effort can we hope to preserve the conditions under which human beings can remain authors, and not mere subjects, of their own lives. The restoration of our digital agency is a collective undertaking.

Welcome to the conversation.

99 Choosing the Right Tools

100	Browser	118	Cloud Storage
102	Search Engine	120	Crypto Storage
104	Messaging	122	Crypto Exchanges
106	Email	124	VPN Layer
108	Calendar	126	AI Tools
110	Team Chat	128	Social Networks
112	Video Calls	130	Maps
114	Cloud Docs	132	Translator
116	Passwords Managers		

“We shape our tools,
and thereafter they shape us”

John Culkin¹

The technologies we choose and adopt don't merely extend our capabilities; they gradually reshape our behaviours, cognitive patterns, and social structures. The same tools that threaten freedom can also become its instruments if understood and used with care. Choosing technologies that uphold our autonomy, self-determination, and privacy is one of the most powerful actions available to us as citizens and individuals to protect our own well-being and that of our societies. Together, we can become participants and advocates for a digital world that respects our data, minds, and freedom. Change starts with small but mindful choices.

1 John M. Culkin, 'A Schoolman's Guide to Marshall McLuhan', *Saturday Review*, 18 March 1967, 70.

Instead of

Google Chrome, Safari

Vulnerabilities

Behavioural Fingerprinting

Chrome tracks browsing history, tab behaviour, scroll depth, and interaction patterns. This telemetry feeds Google's advertising systems and AI data pipelines.

Cross-Site Tracking

Third-party cookies, tracking pixels, and embedded scripts follow you across sites, building a persistent profile of interests, habits, and identity.

Sync Data Harvesting

Browser sync uploads bookmarks, passwords, browsing history, and form data directly to Google's servers when signed into a Google account.

AI Threat

Browsing patterns and interaction data can be used to build behavioural profiles, predict preferences, and enable targeted phishing or manipulation campaigns.

Use

Brave or Hardened Mozilla Firefox

Why it protects you

Built-In Tracker Blocking (Brave)

Brave blocks ads, trackers, cross-site cookies, and many fingerprinting techniques by default, without requiring extensions.

Advanced Privacy Control (Firefox)

Firefox, combined with privacy extensions, enables granular control over tracking scripts, fingerprinting attempts, and third-party requests.

Reduced Corporate Data Harvesting

Neither Brave nor Firefox feeds browsing behaviour into Google's advertising or AI training ecosystem.

Open-Source Transparency

Firefox and Brave are open-source projects, meaning their privacy mechanisms can be independently audited.

Instead of

Google Search

Vulnerabilities

Query Logging

Google records every search query and associates it with your account, device fingerprint, IP address, and browser data. Sensitive queries (health, finance, legal) become part of a persistent profile.

Long-Term Behavioural Modelling

Years of search history allow highly accurate behavioural and psychological profiling. Search queries often reveal fears, intentions, beliefs, and preferences with high precision.

Personalisation Trap

Personalised search results create algorithmic filter bubbles while simultaneously feeding advertising and AI training systems.

Cross-Service Correlation

Queries can be correlated with activity across other Google services, such as YouTube, Gmail, and Google Maps, producing a unified behavioural profile.

Legal Exposure

Search history stored by companies can be requested by governments or law enforcement through legal processes, meaning past searches may become part of investigations or court records.

Use

DuckDuckGo or Startpage

Why it protects you

Identity Shielding (Startpage)

Startpage acts as a privacy proxy, sending your query to Google while removing identifying data before it reaches Google's servers.

No Personal Profiles

DuckDuckGo does not build persistent user profiles.

No Stored Search History

DuckDuckGo does not log personal search history or IP-linked queries.

Neutral Search Results

Both engines avoid deep personalisation, reducing filter bubbles.

Instead of

WhatsApp, Facebook, Messenger, Instagram

Vulnerabilities

Metadata Collection

Even when messages are encrypted, Meta collects metadata such as who you talk to, when you communicate, how often, and from which device and location. This builds detailed social graphs of your relationships.

Centralised Data Control

Messages, contacts, and activity data are tied to centralised accounts and infrastructure controlled by Meta, enabling large-scale data aggregation and analysis.

Contact Harvesting

Apps like WhatsApp and Messenger upload your phone contacts to their servers to identify other users, expanding the company's knowledge of your personal network.

Advertising and Behavioural Profiling

Data collected across WhatsApp, Messenger, Instagram, and Facebook contributes to large behavioural profiles used for advertising, targeting, and data analytics.

AI Threat

Messaging data and patterns can be analysed to generate predictive models of relationships, habits, and interests for manipulation or profiling.

Use

Signal, Telegram, SimpleX Chat

Why it protects you

Privacy by Default Architecture

Signal and SimpleX Chat are engineered to minimise data exposure at every level – no hidden trade-offs, no optional privacy modes.

True End-to-End Encryption

Signal applies rigorously audited encryption to all messages automatically, ensuring only sender and recipient can ever access the content.

No Metadata Collection

Both Signal and SimpleX Chat drastically limit or eliminate metadata collection, blocking the creation of social graphs and behavioural profiles.

No Phone Number Exposure

SimpleX Chat allows communication without phone numbers, usernames, or centralised identity accounts, reducing traceability.

Independent & Privacy-Focused Governance

Signal is run by a non-profit foundation, while SimpleX Chat is independent and open-source – both avoiding ad-driven business models.

Instead of

Gmail, Microsoft Outlook, Apple Mail

Vulnerabilities

Metadata Harvesting

These platforms retain metadata, including sender, recipient, timestamps, frequency of communication, and device information. Over time, this metadata builds a detailed map of professional and personal relationships.

Ecosystem Lock-In

Services like Gmail, Outlook, and Apple Mail integrate with cloud storage, calendars, search tools, and productivity platforms, creating a large interconnected data environment where activity across services can be correlated.

AI Training Signals

Google and Microsoft process behavioural profiles derived from email activity, such as open rates, reply timing, and engagement patterns, to improve automated systems and AI-powered features.

Use

Proton Mail

Why it protects you

End-to-End Encryption

Messages between Proton Mail users are encrypted so only the sender and recipient can read their contents.

Zero-Knowledge Architecture

Proton Mail encrypts mailbox data on the client side before it reaches Proton servers, meaning the provider cannot access message contents.

Minimal Data Collection

Proton Mail is designed to reduce stored metadata and does not use email content to build advertising profiles.

Open-Source Transparency

Proton Mail applications are open-source and regularly audited by independent security researchers.

Instead of

Google Calendar, Microsoft Outlook

Vulnerabilities

Event & Schedule Indexing

All event details, meeting titles, locations, and participant lists are stored on Google or Microsoft servers.

Cross-Product Profiling

Calendar activity is linked to Gmail, Outlook email, Teams, and Office 365, contributing to behavioural profiling and targeted ads.

Data Retention

Event history can be stored indefinitely and is accessible to internal systems.

Third-Party App Access

Connected apps and add-ons can read calendar data, including meeting metadata and attendee information.

Use

Proton Calendar

Why it protects you

End-to-End Encryption

Proton Calendar encrypts event details, attendees, and notes, so only authorised participants can access them.

Zero-Knowledge Architecture

Proton cannot read your calendar content, preventing AI training or internal profiling.

Cross-Platform Privacy

Use on web, desktop, or mobile without linking activity to external ad networks.

Reduced Third-Party Exposure

Calendar data is not automatically shared with add-ons or external services.

Instead of

Slack

Vulnerabilities

AI Feature Ingestion

Collaboration platforms owned by Salesforce integrate AI assistants that analyse internal conversations to generate summaries, recommendations, and automation features.

Permanent Searchable Logs

Messages are indexed and stored to enable workspace-wide search and compliance features. On many paid plans, conversation history can be retained indefinitely.

Admin Visibility

Workspace administrators may have the ability to export message history for compliance or auditing purposes, including private channels, depending on plan configuration.

Third-Party App Access

Integrations with tools such as Notion, Jira, and Google Drive create additional data-sharing pathways where conversations may be accessed by external services.

Use

Element, Mattermost

Why it protects you

End-to-End Encryption

Element runs on the open Matrix protocol and supports end-to-end encrypted rooms so only participants can read messages.

Open Protocol Architecture

Matrix is an open communication protocol allowing independent servers to federate while maintaining control over their own data.

Self-Hosting Control

Mattermost can be deployed on infrastructure you control, meaning conversation data remains within your own servers rather than hosted on a third-party cloud platform.

Enterprise Privacy Adoption

Mattermost and Matrix-based platforms are used by organisations, including the Mozilla Foundation and several European public sector institutions, that prioritise sovereignty.

Reduced External Data Access

With self-hosting or encrypted rooms, conversation content is not accessible to external analytics or AI systems.

Instead of

Zoom, Google Meet

Vulnerabilities

AI Training on Meeting Content

Platforms like Zoom and Google Meet can process audio, video, and transcripts to power features like summaries and transcription – while also using this data to train and improve AI systems.

Behavioural Profiling

Meeting metadata, such as call duration, list of attendees, frequency of interaction, and engagement patterns, can be retained and analysed.

Centralised Infrastructure

Both platforms operate primarily under US legal jurisdiction, meaning meeting recordings, transcripts, and user data may be accessible through legal requests or subpoenas.

Use

Jitsi Meet, Signal video calls

Why it protects you

No Account Required

Jitsi Meet can be used instantly in a browser without creating an account, reducing identity linkage and stored user data.

Open-Source Transparency

Jitsi Meet is open-source, allowing independent verification of its security and privacy mechanisms.

No Default Content Storage

Jitsi meetings are not automatically recorded or stored unless explicitly configured.

End-to-End Encryption

Signal video calls use end-to-end encryption by default through the Signal Protocol, ensuring only participants can access call content.

Self-Hosting Option

Teams can deploy their own Jitsi servers, maintaining full control over infrastructure and meeting data.

Instead of

Google Docs

Vulnerabilities

Full Document Indexing

Every word you type in Google Docs is indexed, searchable by Google, and used to train AI systems.

IP and Strategy Exposure

Proprietary strategies, client documents, and financial plans live on Google's servers with limited technical barriers to automated processing.

Collaboration Tracking

Edit history is retained and analysed.

Cross-Product Profiling

Document behaviour links to your Gmail, Search, YouTube, and Ads profile, amplifying the behavioural model associated with you.

Use

CryptPad, Proton Drive, Fileverse

Why it protects you

End-to-End Encryption

CryptPad uses zero-knowledge encryption. The server cannot read your documents.

End-to-End Encrypted Storage

Proton Drive provides encrypted storage for files and folders.

Decentralised & Encrypted

Fileverse allows self-hosted or decentralised encrypted document storage.

Privacy-Preserving Collaboration

Collaboration is encrypted, so your content is not available for model training by the provider.

Instead of

Saved Passwords in Chrome, Safari

Vulnerabilities

Single Ecosystem Risk

All credentials stored in Chrome sync to Google's servers. One account compromise may expose your stored passwords.

Credential Reuse & Phishing Vulnerability

Most people reuse passwords across sites. Chrome makes this easier, not harder, amplifying breach exposure. Chrome's autofill can also be tricked by convincing domain clones.

No Zero-Knowledge Architecture

Google can technically read your saved passwords. The architecture does not guarantee end-to-end encryption of your credential vault.

Use

Bitwarden, NordPass

Why it protects you

Zero-Knowledge Encryption

Both Bitwarden and NordPass use a zero-knowledge architecture, meaning the company cannot access your passwords. Your vault is encrypted locally before syncing.

Unique Password Generation

Each login can automatically generate long, random passwords and store them securely. This eliminates password reuse across services.

Independent Security Model

Your credentials are stored in a dedicated password vault, separate from your browser account. Compromising your Google account does not expose your entire password database.

Phishing Protection

Autofill only works on the exact saved domain, making phishing sites far less effective.

Instead of

Google Drive

Vulnerabilities

Document Scanning

Google Drive scans all files for policy compliance and AI training signals. Your contracts, financials, and private documents are machine-readable.

Centralised Data Graph

Drive integrates with Gmail, Docs, Sheets, and Calendar. Your files become nodes in a comprehensive behavioural and professional intelligence graph.

US Legal Jurisdiction

Google is a US company subject to CLOUD Act requests. Government agencies can compel disclosure of your stored files without proper notification.

Use

Tresorit, Proton Drive

Why it protects you

Zero-knowledge by default

Tresorit encrypts everything before it leaves your device – no access, no visibility, not even the provider can read your files.

True end-to-end storage

Proton Drive ensures only you hold the keys, with encryption applied client-side and maintained across storage and sharing.

Outside data-extraction jurisdictions

Both operate under strong Swiss privacy protections, keeping your data away from mass-surveillance frameworks and extraterritorial access laws.

No scanning, no profiling

Your files remain opaque – no content analysis, no AI training pipelines, no behavioural mapping.

Instead of

Storing Funds on Coinbase, Binance, or Other Exchanges

Vulnerabilities

Custodial Control

On Coinbase, you do not own your crypto. They control the private keys.

Exchange Surveillance

Every transaction, portfolio balance, and trading behaviour is permanently logged and shared with the IRS, FinCEN, and analytics firms like Chainalysis.

Regulatory Freezes

Exchanges have frozen accounts during market stress, regulatory action, and at government request, with limited user recourse in practice.

Counterparty Risk

FTX held \$8 billion in customer funds. They collapsed overnight. Custodial risk is not theoretical.

Use

Trezor, Ledger Hardware Wallet

Why it protects you

Hardware Wallet

Private keys never touch the internet. Signing happens on the device itself.

Open Source Firmware

Trezor has fully open-source firmware for maximum auditability.

Multisig

For long-term holdings, Multisig setups require multiple keys to authorise any transaction, eliminating single points of failure.

Instead of

Binance, Coinbase

Vulnerabilities

Custodial Risk

Binance and Coinbase hold your private keys, meaning the platform can freeze, seize, or restrict access to your funds.

KYC & Personal Data Exposure

These platforms require identity verification, storing personal data and linking it to your transactions, which can be subpoenaed or hacked.

Centralised Control

Trading, listing, and withdrawals are controlled by the company, creating single points of failure.

Regulatory Surveillance

Governments can access your transaction history through the platform's reporting, reducing financial privacy.

Use

Uniswap, SushiSwap

Why it protects you

Non-Custodial Control

Uniswap and SushiSwap are decentralised exchanges (DEXs) where you retain full control of your private keys and funds.

No KYC Required

DEXs generally do not require personal identity verification, protecting your privacy and unlinking your trades from your real-world identity.

Open & Transparent Protocols

Smart contracts on Ethereum or other blockchains are auditable and open-source, ensuring predictable behaviour and community oversight.

Decentralised & Censorship-Resistant

Trades happen peer-to-peer onchain, reducing the risk of government or platform intervention.

Instead of

No VPN

Vulnerabilities

ISP Surveillance

Without a VPN, your Internet Service Provider can see the domains you visit and log your browsing activity. In many regions, this data can be retained or sold to advertising networks, analytics companies, and data brokers.

IP-Based Profiling

Your IP address acts as a persistent identifier linking activity across websites, services, and sessions. Even private browsing mode cannot hide your destinations from your ISP or network operator.

Network Metadata Retention

Connection metadata such as timestamps, session duration, and destination domains may be logged by ISPs for extended periods depending on local regulations and company policies.

Public Network Exposure

On public WiFi networks such as hotels, airports, and cafés, traffic that is not encrypted can potentially be monitored by network operators or malicious actors on the same network.

Use

Mullvad VPN, Proton VPN, NordVPN

Why it protects you

Encrypted Tunnel

A VPN encrypts your internet traffic and routes it through a secure server so your ISP can only see an encrypted connection rather than the specific websites you visit.

Minimal Identity Requirements

Mullvad allows account creation without email or personal information and identifies users through a random account number.

Privacy-Focused Jurisdiction

Proton VPN operates under Swiss privacy laws and publishes an audited no-logs policy designed to limit retained activity data.

Additional Security Layers

NordVPN offers features such as malware blocking, tracker filtering, and multi-hop routing to enhance network privacy and protection.

IP Address Masking

Websites see the VPN server's IP address instead of your real one, reducing the ability to link activity to your physical location or home network.

Instead of

ChatGPT

Vulnerabilities

Data Logging & Retention

Inputs and conversations are stored on OpenAI servers and may be used to train AI models. Users have minimal control over how training data is used or stored.

Profile Linking

Interactions can be linked to your account, email, or usage history, contributing to behavioural profiles.

Proprietary Model Access

AI outputs may include information inferred from other users' prompts or proprietary data.

Military & Defence Ties

OpenAI collaborates with US defence and the Pentagon; your prompts help build AI for surveillance, intelligence, and warfare.

Use

AkashChat, Venice.ai, Claude, Perplexity, MidJourney (Images)

Why it protects you

Reduced Data Logging

Claude and Perplexity minimise or avoid using your chats for training – your data isn't the product.

Privacy by Design

Venice.ai runs without storing personal data – no profiles, no tracking, no shadow records.

Encrypted by Default

Akash Chat uses end-to-end encryption – your conversations stay yours, not theirs.

No War Pipeline

These models operate without known defence ties – your prompts aren't feeding military AI systems.

Instead of

X

Vulnerabilities

Data Hoarding

X stores everything – posts, DMs, clicks – indefinitely.

Profile Exploitation

Every action feeds a behavioural profile built to predict and influence you.

Black-Box Feed

What you see is controlled by opaque algorithms optimised for engagement, not truth.

Ad Surveillance Engine

Your activity is tracked and monetised across ads and partner networks.

Use

Bluesky, Mastodon, Nostr

Why it protects you

No Single Owner

Mastodon and Nostr distribute control – no central authority owns your data.

Open, Inspectable Systems

Bluesky (AT Protocol), ActivityPub, and Nostr are transparent – you can see how they work.

You Own Your Identity

Choose your server or hold your own keys – no forced corporate account.

No Ad Tracking Machine

No built-in surveillance ads, no cross-platform profiling, no hidden data trade.

Instead of

Google Maps

Vulnerabilities

Location Tracking

Google Maps continuously logs your real-time location, routes, and travel history.

Profile Linking

Your movement data is linked to your Google account, enhancing profiling for Ads, YouTube, and Search.

Data Retention

Historical location data is stored indefinitely unless manually deleted.

Shared Location Exposure

Location sharing with others is accessible to Google and third-party apps.

Use

Waze, Magic Earth

Why it protects you

No Central Profiling

Waze provides navigation and traffic alerts without directly feeding Google's advertising ecosystem.

Privacy-Focused Maps & Offline Use

Magic Earth uses OpenStreetMap data, supports offline maps, and does not track your identity.

Data Minimalism

Both limit long-term storage – less history, less risk.

No Data Web

Reduced linking across services means your movements stay isolated, not exploited.

Instead of

Google Translate

Vulnerabilities

Data Logging & Retention

Google Translate logs every text you input, which can include sensitive or proprietary content.

Profile Linking

Input may be associated with your Google account and used to improve AI models or feed targeted advertising.

Cross-Service Data Use

Text data can be analysed and linked across Google services, including Gmail, Docs, and Ads, increasing privacy exposure.

Limited Transparency

Users cannot fully control how long translations are stored or how they are used to train models.

Use

Kagi Translate, DeepL

Why it protects you

No User Profiling

Kagi Translate does not link inputs to personal accounts, preventing cross-service tracking and profiling.

End-to-End Privacy

DeepL does not use the content of paid users' translations to train its models, ensuring confidential data remains private.

Minimal Data Retention

Both alternatives minimise logging and store data only as needed for service functionality, reducing exposure.

Transparent Policies

Clear privacy policies explain how input is processed, stored, and deleted, giving users control over sensitive information.

Secure & Independent Platforms

These services are independent from major advertising ecosystems, meaning your translation data is not harvested for marketing purposes or AI training.

A Algorithmic Governance

The use of algorithms and automated decision systems to manage social, economic, or administrative processes. Algorithmic governance can increase efficiency but raises concerns about transparency, accountability, and bias.

A Anonymity

The ability to interact, communicate, or transact without revealing one's real-world identity. Anonymity can protect freedom of expression and political participation, but it also creates challenges for accountability and regulation. See also: Pseudonymity; Privacy Coin.

A Anonymous Credentials

Cryptographic credentials that allow individuals to prove specific attributes – such as age or membership – without revealing their full identity or unnecessary personal information.

A Artificial General Intelligence (AGI)

A hypothetical form of artificial intelligence capable of performing any intellectual task at human or superhuman level. Unlike specialised AI systems, AGI would possess generalised reasoning and learning abilities.

B Blockchain

A system where a network of computers agrees on and stores records of transactions in a shared ledger, without central authority. Once a record is added, it is designed to be permanent and difficult to alter.

B Blockchain Layers

Layer 1: a basic infrastructure layer.

Layer 2: a performance-enhancing layer for off-chain transaction consolidation or parallel processing on side chains.

Layer 3: an application layer for decentralised apps (DApps).

B Blockchain Types

Permissionless: a blockchain open to the public.

Private: a closed blockchain network that only allows access to known devices.

Permissioned: a blockchain available to users that meet the criteria determined by a central authority; it may operate as a public or private network.

B Central Bank Digital Currency (CBDC)

A digital currency issued and backed by a central bank that runs on a centrally permissioned blockchain as an alternative to cash.

C **Certified News**

A proposed model of digital journalism in which journalists cryptographically sign their content, allowing readers to verify authenticity, authorship, and professional credentials.

C **Community Currency**

A locally issued currency designed to facilitate economic exchange within a specific community and strengthen local economic networks.

C **Communities of Common Interest**

Groups formed around shared goals, values, or interests rather than geographic proximity. Digital technologies increasingly enable such communities to organise globally.

C **Consensus Mechanism**

A protocol used by blockchain networks to reach agreement on the validity of transactions without relying on a central authority.

C **Contextual Integrity**

A theory of privacy proposing that information sharing should respect the norms of the social context in which the information was originally provided.

C Creative Collaboration Platforms

Digital systems designed to enable large-scale collaboration among individuals and organisations in areas such as research, innovation, and policymaking.

C Cryptocurrency

A cryptographically secured digital currency transacted as tokens on a blockchain.

C Cryptocurrency Wallet

A physical or digital storage device for a private key – which allows access to cryptocurrency holdings and the signing of transactions – linked to a public key, which functions as an account number.

C Cryptography

The science of securing information through mathematical algorithms, enabling confidential communication, authentication, and data integrity.

C Cypherpunk

A movement advocating the use of cryptography and privacy technologies to protect civil liberties, freedom of expression, and individual autonomy in digital environments.

D Data Minimisation

A privacy principle stating that organisations should collect and store only the data strictly necessary for a specific purpose.

D Data Sovereignty

The principle that individuals, communities, and nations should retain control over their own data rather than relinquishing it to external organisations.

D Decentralisation

The distribution of authority and control across a network rather than within a single institution.

D Decentralised App (DApp)

An application that runs on a blockchain or peer-to-peer network rather than centralised servers.

D Decentralised Autonomous Organisation (DAO)

An organisation governed by its members through blockchain-based voting rights, which are held as governance tokens rather than tied to shares or legal membership.

D Decentralised Exchange (DEX)

A cryptocurrency exchange that allows peer-to-peer trading by facilitating markets automatically through liquidity pools of invested assets and accepting trades via smart contracts.

D Decentralised Finance (DeFi)

A blockchain-based financial system that does not rely on intermediaries to maintain trust.

D Decentralised Identity (DID)

A digital identity system in which identifiers are created and controlled by individuals rather than centralised identity providers.

See also: Self-Sovereign Identity.

D Digital Commons

Shared digital resources that are collectively governed and maintained for public benefit.

D Digital Identity

A set of digital attributes representing an individual, organisation, or device in online environments.

D **Differential Privacy**

A statistical technique that protects individuals within datasets by introducing controlled noise into the data, enabling analysis without revealing personal information.

D **Distributed Trust Networks**

Economic or social systems based on peer-to-peer trust relationships rather than centralised institutions such as banks or governments.

E **End-to-End Encryption (E2EE)**

A communication method in which messages are encrypted on the sender's device and can only be decrypted by the intended recipient.

E **EuroStack**

A proposed European digital infrastructure initiative launched in 2024 by a group of tech experts, economists, and industry leaders to reduce reliance on foreign technology providers and strengthen Europe's digital sovereignty.

E **European Digital Identity (EUDI) Wallet**

A digital wallet that enables citizens to securely store and share identity credentials across online services within the European Union.

F **Faceted Identity**

The idea that individuals present different aspects of their identity depending on social context, such as professional, personal, or political environments.

G **Gas Fees**

Transaction fees paid to blockchain validators or miners for processing and recording transactions on the network.

G **Generative Foundation Models (GFM)s**

Large artificial intelligence models capable of generating text, images, and code across multiple domains.

G **Governance Tokens**

Cryptographic tokens that grant holders voting rights within decentralised organisations such as DAOs.

H **Homomorphic Encryption**

A cryptographic technique that allows computations to be performed on encrypted data without decrypting it first.

I Immersive Shared Reality (ISR)

Digital environments combining virtual reality, augmented reality, and mixed reality to create interactive shared experiences.

I Infrastructural Power

The influence that arises from controlling key technological infrastructure, platforms, or communication networks.

L Layer 2 Scaling

Technologies designed to improve blockchain scalability by processing transactions outside the main blockchain while maintaining security guarantees.

L Liquid Democracy

A governance model that combines elements of direct and representative democracy, allowing individuals to vote directly or delegate their vote.

L Liquidity Pool

A pool of cryptocurrency assets locked in a smart contract to facilitate decentralised trading.

M Metadata

Information describing other data, such as timestamps, locations, or sender and recipient identifiers.

M Metaverse

A shared, persistent virtual world in which users can interact, create, and transact, often with a built-in onchain economy.

M Multicreds

Composite digital credentials that combine multiple verified attributes into a single privacy-preserving proof.

M Multiparty Computation (MPC)

A cryptographic method that allows multiple parties to compute a shared result without revealing their individual inputs.

N Neural Interfaces

Technologies that enable direct communication between the human brain and digital systems.

N Non-Fungible Token (NFT)

A blockchain record of ownership of a unique digital asset that, unlike regular tokens, cannot be exchanged on a one-for-one basis with another.

O Oracle

An interface that provides dynamic off-chain inputs, such as financial market data or supply chain events, to onchain smart contracts.

O **Open-by-Default Policy**

A public procurement principle that prioritises open-source software in government digital infrastructure.

O **Overlapping Consensus**

A concept from political philosophy describing agreement on shared political principles among groups with differing beliefs.

P **Platform Sovereignty**

The ability of societies or governments to regulate the digital platforms shaping economic and social activity.

P **Plural Publics**

Distinct communities that maintain their own informational environments and social norms.

P **Plurality**

A governance philosophy that emphasises collaboration among diverse groups and perspectives.

P **Privacy by Design**

A system design approach that incorporates privacy protections into technologies from the earliest stages of development.

P Privacy Coin

A cryptocurrency designed to conceal transaction details and protect financial privacy.

P Privacy-Enhancing Technologies (PETs)

Technologies designed to protect personal data and reduce the need for centralised data collection.

P Privacy-First Protocol

A digital protocol designed primarily to ensure user privacy in its architecture and functionality.

P Proof of Stake (PoS)

A blockchain consensus mechanism in which participants validate transactions by staking cryptocurrency.

P Proof of Work (PoW)

A consensus mechanism that requires computational work to validate blockchain transactions.

P Public Digital Infrastructure

Government-supported digital systems providing essential services such as identity verification, payments, and data exchange.

P Pseudonymity

The use of pseudonyms or persistent identifiers rather than real names in digital interactions.

Q Quadratic Funding (QF)

A funding mechanism that amplifies the impact of many small contributions to support public goods.

Q Quadratic Voting (QV)

A voting mechanism that allows individuals to allocate votes based on the intensity of their preferences.

S Selective Disclosure

A cryptographic technique that allows individuals to reveal only specific information from a credential.

S Self-Sovereign Identity (SSI)

A digital identity model in which individuals own and control their identity credentials.

S Smart Contract

Self-executing code deployed on a blockchain that automatically carries out an agreement between parties when certain conditions are met, such as the creation or transfer of a token.

S Stablecoin

A cryptocurrency pegged to a stable asset, such as a fiat currency.

S Surveillance

The monitoring of individuals' activities, communications, or behaviours by governments, corporations, or other entities.

S Sovereign Technology Fund

A proposed public investment mechanism that supports the domestic development of sovereign digital infrastructure.

T Technocracy

A governance system in which decision-making authority is primarily exercised by technical experts rather than elected representatives.

T Threat Actor

Any individual or organisation that poses a risk to digital systems, privacy, or cybersecurity.

T Token

A blockchain record of ownership of a fungible or non-fungible asset.

T **Tokenisation**

The process of converting real-world assets into digital tokens recorded on a blockchain.

U **Utility Token**

A token that provides access to an organisation's products or services. When it additionally grants voting rights within a decentralised autonomous organisation (DAO), it is known as a governance token.

W **Web 3.0**

A yet-to-be-defined term for a decentralised internet built on blockchain technology, envisioned as a successor to the user-generated, platform-dominated Web 2.0, and to the passive content of Web 1.0.

Z **Zero-Knowledge Proofs (ZKPs)**

A cryptographic technique that allows one party to prove a statement is true without revealing the underlying information.

