List of terms in the Dictionary of Privacy

(N,K) Rule
Abortion
Abstract
Access Control
Access Control List
Access Point
Account Management
Accountability
Accuracy
Ad Exchange
Ad Hoc Network
Ad Network
Adchoices
Additivity
Adequacy
Adtech
Advanced Encryption Standard (AES)
Adversary
Adware
Affinity Analysis
American Data Privacy and Protection Act
Analogue Hole
Analytical Completeness
Analytical Validity
Anonymisation
Anonymisation Decision-Making Framework (ADF)
Anonymising Proxy
Anonymity
Anonymous Search Engine
Anti-Discrimination Law
Anti-Malware
Anti-Virus Software
Apec Privacy Principles
API
Application (App)
Application Layer Attack
Appropriate Safeguards
Appropriate Technical and Organisational Measures
Appropriation Of Name or Likeness
Article 29 Working Party
Artificial Intelligence (Ai)
Asset
Associational Privacy
Asymmetric Cryptography
Asymmetric Information
Attack Surface
Attack Tree
Attacker
Attention as a Resource
Attention Tracking
Attentional Privacy
Attitude-Behaviour Gap
Attribute Disclosure
Attribution
Audit Trail
Augmented Reality
Authentication
Authorisation
Automated Decision-Making
Autonomous Systems
Autonomy
Auxiliary Knowledge
Availability
Back Up
Backdoor
Barnardisation
Behavioural Advertising
Benefits Of Privacy
Bicycle Attack
Big Brother
Big Data
Binding Corporate Rules
Biobank
Biometrics
Black Hat Attack
Blacklist
Blackmail
Blinding
Blockchain
Blocking Variable
Blue Team
Bluetooth
Bodily Privacy
Bot
Botnet
Boundary
Bounded Rationality
Bounds
Brain Implant
Brain-Computer Interface (BCI)
Brainwashing
Breach
Breach Disclosure
Breach Of Confidence
Bring Your Own Device (BYOD) Policy
Browser Fingerprinting
Browsing History
Brussels Effect
Brute Force Attack
Buffer Overflow Attack
Bug
Business Case
Business Impact Level
Celebrity Privacy
Cell Suppression
Censorship
Census
Centralised Governance
Certification
Certification Authorities
Chain Of Trust
Challenge Response
Charter Of Fundamental Rights
Charter Rights
Checksum
Chief Privacy Officer
Chief Privacy Officer
Chilling Effect
Chinese Wall
Cia Triad
Cipher
Cipher Text
Classified Information
Clear Text
Clickstream Data
Client Confidentiality

Closed Circuit Television
Cloud Computing
Cloud Storage
Co-Privacy
Code Audit
Code Of Conduct
Code Of Ethics
Commodification
Common Law
Communication
Communication Privacy
Communication Privacy Management (CPM) Theory
Community Privacy
Compliance
Concentration Rule
Conditions For Processing
Confidence
Confidentiality
Confidentiality Club
Confidentiality Pledge
Conflict Of Rights
Connectomics
Consent
Consent Forms
Consequential Data
Consistency Mechanism
Consumer Information Markets
Consumer Preference Information
Content Data
Contextual Advertising
Contextual Integrity
Continuous Data
Controlled Rounding
Controlled Tabular Adjustment
Convention 108
Cookie
Cooperation Mechanism
Correct Attribution Probability
Count Data
Credentials
Creepiness
Creepy Line, The
Crime Prevention Exemptions
Cross Device Tracking

Cross-Border Data Processing
Cross-Site Scripting
Cryptanalysis
Crypto Wars
Crypto-Shredding
Cryptocurrency
Cryptographic Hash Function
Cryptographic Key
Cryptographic Protocol
Cryptography
Currency
Customer Relationship Management
Customer Tracking
Cyber Resilience
Cybercrime
Cybersecurity
Cyberstalking
Cyberterrorism
Cyberwarfare
Cypher
Cypherpunk
D Privacy
Dark Pattern
Dark Web
Data
Data Abuse
Data Ageing
Data At Rest
Data Breach
Data Breach Notification
Data Broker
Data Capture
Data Centre
Data Classification
Data Controller
Data Curation
Data Custodian
Data Degaussing
Data Destruction
Data Divergence
Data Enclave
Data Environment
Data Environment Analysis
Data Ethics

Data Exhaust
Data Flow
Data Flow Diagram
Data Governance
Data Harmonisation
Data Harvesting
Data In Motion
Data In Transit
Data In Use
Data Intermediary
Data Intruder
Data Intrusion Simulation
Data Lifecycle
Data Lifecycle Management
Data Linkage
Data Map
Data Minimisation
Data Minimisation Principle
Data Mining
Data Owner
Data Portability
Data Processing
Data Processor
Data Protection
Data Protection Authority
Data Protection by Default
Data Protection by Design
Data Protection Directive
Data Protection Impact Assessment(DPIA)
Data Protection Officer
Data Protection Policy
Data Protection Principles
Data Provenance
Data Quality
Data Recipient
Data Release
Data Retention
Data Safe Haven
Data Sanitisation
Data Schema
Data Share
Data Sharing Agreement
Data Situation
Data Situation Audit

Data Sovereignty
Data Steward
Data Stewardship Organisation
Data Storage
Data Subject
Data Subject Access Request
Data Synthesis
Data Transfer
Data Trust
Data Unit
Data User
Data Utility
Data Warehouse
Database Of Ruin
Datafication
Dataset
Dataveillance
Distributed Denial Of Service
De-Identification
Deanonymisation
Decentralisation of the Web
Decisional Privacy
Declared Data
Decryption Algorithm
Deep Learning
Deepfake
Defamation
Default Settings
Delta
Demographic Advertising
Demonstration Attack
Denial Of Service (DoS)
Deterministic Record Linkage
Device Fingerprinting
Dicom Standard
Differencing
Differential Identifiability
Differential Privacy
Digital Assistant
Digital Breadcrumbs
Digital Certificate
Digital Economy
Digital Fingerprinting
Digital Footprint
Digital Hygiene

Digital Identity
Digital Inequalities
Digital Inheritance
Digital Literacy
Digital Rights Management
Digital Self-Determination
Digital Signature
Digital Wallet
Dignity
Direct Access Attack
Direct Identifier
Direct Marketing
Directory Indexing
Disassociability
Disclosive Data
Disclosure
Disclosure And Barring (Check)
Disclosure Control Methods
Disclosure Risk
Discretionary Access Control
Disguise
Dns Server
Do Not Track (Protocol)
Dominance Rule
Doxxing
Drm
Duty Of Confidence
Duty To Protect
Duty To Warn
Dyad
Dynamic Consent
Dynamic Data Situation
E-Commerce
Eavesdropping Attack
Economics Of Privacy
Electronic Health Record
EM Algorithm
Emotion Recognition
Employee Information
Encrypt-Everything-Everywhere (E3)
Encryption
Encryption Algorithm
Encryption Key
End User Licence (Agreement)

End-To-End Encryption
Endpoint Security
Enhanced Privacy Id
Eprivacy Directive
Eprivacy Regulation
Epsilon
Equivalence Class
Equiveillance Class Structure
Erasure
Escrow
Ethical Hacking
Ethics Committee
Ethics Engineering
European Convention On Human Rights
European Data Protection Board (EDPB)
European Data Protection Supervisor (EDPS)
Explainable Ai
Extranet
Extrinsic Privacy
Facial Recognition Technology
Fair
Fair Information Practice Principles
Fair Processing Notice (FPN)
Fairness
Fake Profile
False Light
False Negative
False Positive
Family Resemblance
Feature
Federal Trade Commission
Federated Identity
Federated Learning
Feminist Critique of Privacy
Fiduciary Duty
Filing System
Financial Privacy
Fipps
Firewall
Firmware
Fishing Attack
Five Eyes

Five Safes
Flexible Output
Formal Anonymisation
Formal Privacy
Format Preserving Encryption
Foundation Model
Freedom Of Expression
Freedom Of Information
Freely Given Consent
Frequency Data
Fully Automated Remote Analysis System
Fully Homomorphic Encryption (FHE)
Function Creep
Functional Anonymisation
Functional Unique Identifier
Fuzzing
Gait Recognition
Game Theory
Gatekeeper
Gendered Spaces
General Data Protection Regulation (GDPR)
Generative Ai
Genetic Privacy
Genomics Data
Geo-Social Data
Geographical Resolution
Geoprivacy
Geotagging
Get Method
Global Privacy Control
Global Recoding
Global Suppression
Globally Unique Identify (Guid)
Gossip
Graduated Security
Grey Hat Attack
Group Harms
Group Privacy
Hacking
Harm
Harassment
Hashing (Functions)

Header Information
Health Information Exchange
Health Insurance Portability and Accountancy Act (HIPAA)
Hellinger Distance
Hierarchical Data
History Of Privacy
Homomorphic Encryption
Honey Pot
Hub Of All Things (HAT)
Human Rights Impact Assessment
Hypertext Transfer Protocol Secure (Https)
I2P
IAB
ICO
Idem-Identity
Identifiability
Identifiable Data
Identifiable Individual
Identifiable Natural Person
Identification Card
Identification File
Identified Data
Identifiers
Identity
Identity Assurance
Identity Cloning
Identity Disclosure
Identity Documents
Identity Management
Identity Provider
Identity Theft
Ideological Privacy
Impact Management
Inadvertent Disclosure
Incognito Mode
Incremental Authorisation
Incremental Authorisation
Indirect Identifier
Inference
Inference Attack
Inferred Data
Information Broker
Information Classification Table

Information Ethics
Information Governance
Information Lifecycle Management
Information Loss
Information Owner
Information Security
Informational Privacy
Informational Self-Determination
Informed Consent
Infosphere
Inherence
Input Privacy
Integrity
Intellectual Privacy
Intellectual Property
Intention-Behaviour Gap
Intentional Data
Interference
Internal Security Testing
International Transfer
Internet
Internet Of People
Internet Of Things
Internet Protocol
Interoperability
Interval Publication
Intimacy
Intranet
Intruder
Intruder Testing
Intrusion Detection System
Intrusion Prevention System
Intrusion Upon Seclusion
Invasive BCI
Inversion Attack
Inviolate Personality
IP
IP Address
Ipse-Identity
Iris Scanning
Irreversibility
Iso27001
Iso27002
Isolation
Jenson-Shannon Divergence

Jigsaw Identification
Joint Data Controller
Jurisdiction
Just In-Time Consent
Just-In-Time Notice
K-Anonymity
Key Logging
Key Variable
Kompromat
L-Diversity
Laplace Noise
Large Language Model
Lawful Basis
Lawfulness
Layered Notice
Layered Security Model
Lead Supervisory Authority
Least Privilege
Legal Basis for Processing
Legitimate Interest (Of the Data Controller)
Libel
Licence Agreement
Life Stream
Lifecasting
Lifelogging
Link Encryption
Linkability
Linkable Information
Linkage Attack
Local Shared Objects
Local Suppression
Location Based Services
Location Data
Location Tracking
Locational Privacy
Logic Bomb
Longitudinal Data
Loyalty Cards
M-Probability
Machine Learning
Magnitude Data
Main Establishment
Male Gaze, The
Malicious Proxy Server

Malware
Man-In-The-Middle Attack
Management Information System
Mandatory Access Control
Mandatory Decryption
Mandatory Key Disclosure
Manual Key Transport
Mash Attack
Mask
Masking
Matching
Material Scope
Material Transfer Agreement
Maximum Knowledge Intruder
Media Access Control (Mac) Address
Membership Inference Attack
Mental Capacity
Mental Privacy
Mesh Network
Message Digest
Metadata
Metadata-Level Controls
Metasploit Framework
Metaverse
Microaggregation
Microdata (Set)
Minimal Unique
Mirai
Missing Data
Mission Creep
Misuse Of Private Information
Mobility Traces
Model Inversion Attack
Molka
Monetary Equivalent Burden
Monetisation
Mosaic Identification
Motivated Intruder
Motivated Intruder Test
Multi Vector Attacks
Multi-Factor Authentication
Multimodal De-Identification
Multiple Imputation
Mutual Assistance

Mutual Authentication
National Security
Natural Person
Necessity
Need-To-Know
Negative Externalities of Disclosed Data
Negligence
Network
Network Encryption
Network Layer Attack
Network Security
Network Segmentation
Neural Prosthesis
Neurocapitalism
Neurodata
Neuroethics
Neuroprivacy
Neuroprosthetics
Neurotechnology
Noise Addition
Nom De Guerre
Nom De Plume
Non-Disclosure Agreements
Non-Discrimination Law
Non-Invasive BCI
Notice And Consent
Nudge Theory
Obfuscation
Objective Harm
Oblivious Transfer
Obscurity
Obtrusion
Oecd Guidelines Governing the Protection Of Privacy And Transborder Flows Of Personal Data (1980)
Offline Dictionary Attack
One-Stop Shop
One-Way Hash Function
Onion Routing
Online Vetting
Onward Transfer
Open Access
Open Data

Open Source
Opt-In
Opt-Out
Order-Preserving Encryption
Orwell Attack
Other
Outing
Outlier
Output Checking
Output Privacy
Output Statistical Disclosure Control
Overimputation
P/Q Rule
P% Rule
P3p
Packet Filter
Packet Sniffing
Panopticon
Paparazzi
Paparazzi Attack
Parental Controls
Partially Homomorphic Encryption
Participant Information Sheets
Participatory Surveillance
Passive Collection
Password
Password Manager
Patch
Patch Management
Peeping Tom
Penetralia
Penetration (Pen) Test
Persistent Cookie
Persistent Pseudonym
Personal Data
Personal Data Store (Pds)
Personal Identification Number (PIN)
Personal Information
Personal Information Management System (Pims)
Personal Space
Personalisation
Personalisation Reactance

Personalised Medicine
Personalised Services
Personally Identifiable Information
Perturbation
Pharming
Philosophy Of Information
Phishing
Physical Privacy
PII
Pinging
Pixelization
Plaintext
Platform For Privacy Preferences (P3P)
Poisoning Attack
Population
Population Unique
Population Unit
Port Scan
Positive Externalities from Disclosed Data
Post Method
Post Quantum Cryptography
Post Randomisation (Pram)
Predictive Analytics
Presence Detection
Price Discrimination
Primary Data
Prior Posterior Ambiguity Rule
Privacy
Privacy As A Source Of Economic Inefficiency
Privacy As Control
Privacy As Redistribution Of Costs
Privacy Avatar
Privacy Budget
Privacy By Design
Privacy Calculus
Privacy Concern
Privacy Elasticity
Privacy Engineering
Privacy Enhancing Technology
Privacy First
Privacy Fundamentalists
Privacy Guarantee

Privacy Impact Assessment
Privacy Insurance
Privacy Notice
Privacy Officer
Privacy Paradox
Privacy Policy
Privacy Pragmatists
Privacy Premium
Privacy Preserving Data Analytics
Privacy Preserving Data Mining
Privacy Preserving Data Publishing
Privacy Preserving Machine Learning
Privacy Preserving Record Linkage
Privacy Risk
Privacy Screen
Privacy Settings
Privacy Threat
Privacy Tort
Privacy Trade-Off
Privacy Unconcerned
Privacy-Invasive Technology
Privacy-Related Interaction
Privacy, Cultural Variation Of
Private Army
Private Biometrics
Private Enterprise
Private Key
Private Parts
Private Property
Private School
Private Sector
Private Sphere
Probabilistic Record Linkage
Processing
Profiling
Proportionality
Proprietary Privacy
Protocol
Proxy
Pseudonym
Pseudonymisation
Psychographic Advertising
Psychological Privacy
Public

Public Disclosure of Private Facts
Public Domain
Public Figure
Public Interest
Public Key
Public Records
Public Sphere
Public-Key Cryptography
Public-Key Infrastructure (PKI)
Publication
Publicity
Publishing
Purchase History
Purple Team
Purpose Limitation
Purpose Specification
Quantum Computing
Quasi Identifier
Query Logging
Query Overlap
Radical Transparency
Radio Frequency Identification (RFID)
Random Rounding
Random Unique
Randomised Response
Ransomware
Rational Consumer
Reality Mining
Reasonable Expectation of Privacy
Reasonable Search
Recommendation System
Reconstruction Attack
Record
Record Linkage
Record Suppression
Records Management
Rectification
Red Team
Redaction
Reference Monitor
Regulators
Reidentification
Reidentification Attack
Relational Autonomy

Release And Forget
Reliance Authentication
Remailing
Remediation
Remote Access
Remote Access Server
Remote Analysis Server
Remote Query
Replay Attack
Repurposing
Reputation Management
Reserve
Respondent
Response Knowledge
Restricted Access
Retention
Revenge Porn
Reverse Fishing Attack
Reversibility
Revocation
Right Of Access
Right To Be Forgotten
Right To Be Informed
Right To Be Let Alone
Right To Correct
Right To Data Portability
Right To Data Protection
Right To Deletion
Right To Explanation
Right To Object
Right To Privacy
Right To Rectification
Right To Restriction of Processing
Risk
Risk Assessment
Risk Tolerance
Risk Utility Trade Off
Roe Vs Wade
Role Based Access Control
Rounding
RSA Encryption
RU Map
Safe Data
Safe Harbor
Safe Outputs

Safe People
Safe Projects
Safe Settings
Safety
Salt
Saml
Sample Unique
Sample Unit
Sampling
Sampling Fraction
Sandbox
Scenario Analysis
Schrems
Search
Search Engine
Seclusion
Secondary Data
Secondary Differentiation
Secondary Use
Secrecy
Secret
Secret Ballot
Secret Sharing
Secure Communication
Secure Multi Party Computation
Secure Sockets Layer (SSL)
Secure Web Gateway
Secure Web Platform
Security
Security Assertion Markup Language
Security Assertion Markup Language
Security Audit
Security By Design
Security Information Management
Security Parameter
Security Posture
Security Requirement
Security Token
Security-By-Obscurity
Self
Self-Disclosure
Self-Reflection
Self-Archiving

Self-Control Security
Self-Sovereign Identity (SSI)
Semantic Security
Semi-Invasive BCI
Sensitive Variables
Sensitivity
Serial Number
Service User Agreements
Sessional Cookie
Single Out
Single Sign On
Singularity, The
Slander
Smart City
Smart Device
Smart Grid
Smishing
Snowden Revelations, Edward Snowden
Social Credit System
Social Engineering
Social Genome
Social Network
Social Network Analysis
Social Profiling
Social Steganography
Software
Software Development Life Cycle (SDLC)
Solid (Social Linked Data)
Solitude
Sousveillance
Spam
Spatial Cloaking
Spatial Privacy
Spear Phishing
Special Category Data
Special Unique
Speech Recognition
Split Tunnelling
Spontaneous Recognition
Spoofing Attack
Spyware
SQL Injection
SSI

Stakeholder
Standard
Standard Contractual Clauses
Standard Model Clauses
Static Key
Statistical Disclosure
Statistical Disclosure Control (SDC)
Statistical Disclosure Limitation
Steganography
Storage Limitation
Streisand Effect
Structural Zero
Structured Query Language (SQL)
Subject Access Request
Subjective Harm
Subliminal Advertising
Subtraction Attack
Succinct Non-Interactive Zero-Knowledge Proof (SNARK)
Super Cookie
Supervisory Authority
Suppression
Surname Attack
Surveillance
Surveillance Capitalism
Swapping Key
Symmetric Key Encryption
Synthetic Data
T-Closeness
Table Redesign
Tabular Data
Tagging
Target Dataset
Target Variable
Targeted Advertising
Telephone Tapping
Terms Of Service
Territorial Privacy
Territorial Scope
Text Anonymisation
Therapeutic Alliance
Thermal Imaging
Third Party
Third Party Doctrine
Threat Modelling

Threshold Rule
Time Bomb
Time Series
Tips
Tokenisation
Topcoding
Tor
Tracing
Tracker
Tracker Blocker
Tracking
Traffic Data
Transmission Control Protocol
Transparency
Transparency Notice
Transport Layer Security (TLS)
Trap Door
Trespass
Trojan Horse
Trust
Trusted Computing Base
Trusted Execution Environment (TEE)
Trusted Research Environment(TRE)
Trusted Third Party(TTP)
Tunnel Encryption
Two Factor Authentication (2FA)
Two-Factor Authentication
U-Probability
Ubiquitous Computing (Ubicomp)
Unambiguous Consent
Unicity
Uniform Resource Locator (URL)
Unique Identifier
Uniqueness
Unreasonable Search
User
User Centric Design
User Modelling
Username
Utility First
Value Of Data
Value Of Privacy
Value Sensitive Design

Value-Action Gap
Veil
Verifiable Secret Sharing (VSS)
Virtual Machine (VM)
Virtual Private Network (VPN)
Virus
Vital Interests
Voice Over Internet Protocol
Voyeurism
Vulnerability Management
Vulnerability
Vulnerable Population
Web 2.0
Web 3.0
Web Beacon
Web Bug
Web Of Trust
Web Profiling
Web Skimming Attack
Whistleblowing
White Box Testing
White Hat Attack
Wiretapping
World Wide Web
Worm
Zero Day Attack
Zero Knowledge
Zero Trust Security