Privacy from Below: Grassroots, Creative Computing, and Digital Sovereignty in Europe

Jernej Kaluža, Regina Seiwald, Ivo Furman, Carlos Cunha, Sašo Josimovski, Lidija Pulevska, Maryja Šupa, Nasir Muftić, Sandra Becker

Last updated August 2026

Funded by
the European Union

This publication is based upon work from COST Action GRADE CA21141, supported by COST (European Cooperation in Science and Technology).

COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career, and innovation.

cost.eu

Contents

Contents 2

Glossary 5

Disclaimer 6

I. Executive Summary 7

II. Introduction 12

1. Online privacy and grassroots communities of digital computing 12

2. Surveillance Capitalism and the Datafication of Everyday Life 15

3. Online Privacy as a Socio-Technical Issue 18

4. Global Approaches to Privacy Regulation: U.S., China, and the EU 20

4.1 From Commodification to Control: U.S. and China's Competing Visions of Digital Privacy 21

4.2 Between Surveillance and the Market: The EU's Third Way in Data Regulation 22

5. Methodological Approach: A Situated, Mixed-Methods Design 25

III. Case Studies 26

1. Institutionalising Grassroots Innovation: Creative Computing and Privacy in Focus 26

2. Grassroots Movements 31

2.1 Noyb – None of Your Business (Austria), founded in 2017 31

2.2 Iuridicum Remedium (IuRe) and Digitální Svobody (Czech Republic), founded in 2001 34

2.3 DECODE – Decentralised Citizen-Owned Data Ecosystem (EU-wide, origins in Spain, pilots in Amsterdam and Barcelona), founded in 2016 35

2.4 Tactical Tech (Germany), founded in 2003 38

2.5 K-Monitor (Hungary), founded in 2007 41

2.6 Panoptykon Foundation (Poland), founded in 2009 44

2.7 D3 – Defesa dos Direitos Digitais (Portugal), founded in 2017 47

2.8 Digital Freedom Alliance (Romania), founded in 2004, and Asociația pentru Tehnologie și Internet (Romania), founded in 2002 50

2.9 SHARE Foundation (Serbia), founded in 2012 51

2.10 Državljan D – Citizen D (Slovenia), founded in 2015 54
2.11 Open Rights Group (UK), founded in 2005 56
2.12 Privacy International (UK), founded in 1990 57
2.13 Privacy Issues as a Wikipedia Contributor 59
IV. Ethical Approaches to Grassroots Online Privacy Activism 62
1. Key Ethical Principles and Community-Centred Design 62
2. The Ethics of Resistance to Surveillance Capitalism 64
3. AI and the Ethics of Privacy Activism 67
4. Machine Unlearning and the Future of Data Privacy 67
4.1 Embedding 'Forgetting by Design' into AI Systems 68
4.2 Techniques for Selective Data Removal 68
4.3 Legal Imperatives and Verification Challenges 69
4.4 Balancing Privacy and Performance 70
4.5 Policy Implications for a Human-Centred AI Ecosystem 70
4.6 Recommendations for Researchers, Practitioners, and Grassroots Actors 71
5. Conclusion 71
V. Technical Approaches to Grassroots Online Privacy Protections 73
1. Core Privacy-Enhancing Technologies - Tools and Techniques 73
2. Front-End Tools for Daily Use 76
Use Case: VPN Access for Censored and High-Risk Regions 77
3. Creative Computing, Tactical Media, and Community Engagement 78
Use Case: Gamified Learning on Digital Privacy for Teens 78
4. Free/Libre Open Source Software (FLOSS) 80
Use Case: Building Privacy-First Infrastructure with FLOSS 80
5. Navigating Emerging Trends and Privacy Techniques in Artificial Intelligence 81
Use Case: AI-Based Privacy Alert System for Community Safety 82
6. Concluding Reflections: Shared Challenges and Grassroots Responses 83
VI. Findings & Analysis 86

1. Diverse Modes of Grassroots Engagement: Educational, Technical, and Artistic Practices 86
2. Navigating the Tension Between Innovation and Limited Resources 87
3. Building Trust and Participation: Community-Centred Privacy Advocacy..... 87
4. Shaping the Future: Grassroots Impact on Digital Culture and Policy 88

VII. Policy & Practice Recommendations 90

VIII. References 94

Glossary

Application Programming Interfaces (APIs)

Artificial Intelligence (AI)

AI Act (AIA)

Consumer Privacy Act (CCPA)

Court of Justice of the European Union (CJEU)

Data Governance Act (DGA)

Data Loss Prevention (DLP)

Data Protection Authorities (DPAs)

Differential Privacy (DP)

Digital Markets Act (DMA)

Digital Services Act (DSA)

Do-It-Yourself (DIY)

End-to-End Encryption (E2EE)

European Digital Rights (EDRi)

European Union (EU)

Freedom of Information (FOI)

Free/Libre Open Software (FLOSS)

General Data Protection Regulation (GDPR)

machine unlearning (MU)

Memorandum of Understanding (MoU)

National Security Agency (NSA)

Non-Governmental Organisations (NGOs)

Personal Information Protection Law (PIPL)

Privacy-Enhancing Technologies (PETs)

Secure Access Service Edge (SASE)

Secure Multi-Party Computation (SMPC)

Site Reliability Engineering (SRE)

Small and Medium-sized Enterprises (SMEs)

Software-as-a-Service (SaaS)

Science, Technology, Engineering, the Arts, and Mathematics (STEAM)

United States (U.S.)

Very Large Online Platforms (VLOPs)

Very Large Online Search Engines (VLOSEs)

Virtual Private Network (VPN)

Disclaimer

Parts of this white paper were reviewed using OpenAI's ChatGPT for grammar and style refinement. All substantive content, analysis, and conclusions were developed and verified by the authors.

I. Executive Summary

Aim & scope: This white paper explores the evolving meaning and practice of online privacy at a time when data extraction structures both corporate power and state governance. Moving beyond narrow legal and technical framings, it foregrounds the role of civil society actors, grassroots movements, and creative computing communities in reimagining privacy as a collective and political concern. Through case studies spanning litigation, advocacy, librehosting, privacy-enhancing technologies, and experimental approaches to Artificial Intelligence (AI), the paper demonstrates how bottom-up initiatives open new conceptual and practical horizons for digital rights.

These cases provide situated knowledge that informs our normative stance on the ethical use of technology. By framing privacy as a commons – an infrastructure vital to both individual autonomy and democratic publicness – the paper charts alternative pathways beyond compliance-driven regulation, offering insights and recommendations for policy, technology, and civic practice. Treating privacy as a relational, context-dependent, and socio-technical phenomenon, it situates grassroots practices within broader dynamics of datafication, surveillance capitalism, and the blurring of boundaries between the public and the private.

Introduction: First**,** the paper synthesises political-economic, socio-technical, and normative literatures into a single lens that explains **how platformised data extraction has reconfigured online privacy and why purely top-down regulation struggles to address entrenched power asymmetries**.
Second, it offers a **comparative account of privacy governance**, covering the European Union's (EU) rights-based regime (General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA), AI Act) alongside United States (U.S.) market-led and China state-centric models, and highlights where each advances or undermines autonomy, accountability, and competition.

Last, but not least, introduction surfaces a repertoire of **grassroots, creative-computing responses** that prefigure alternative data futures, distilling recurring tactics, the tension between informality and institutionalisation, and policy levers (funding, regulatory facilitation, education, networking) to support 'digital sovereignty from below'.

Methodologically, this white paper adopts a deliberately 'situated' research stance, combining desk research and selective interviews. We apply insights from critical theories of technology to

concrete case studies of grassroots organisations, while also working in reverse, deriving normative claims from the practices and activities of these organisations themselves.

Case-studies chapter: This chapter shows that online privacy is both the object of action and an internal organising principle for Europe's grassroots digital movements, and that their paths to institutionalisation are diverse, reversible, and negotiated between anonymity and transparency. The portfolio ranges from informal, federated service providers (Kompot/librehosters) to legal-advocacy engines (noyb; IuRe/Digitální Svobody), civic-tech transparency labs (K-Monitor), prefigurative edu-culture projects (Tactical Tech; Citizen D), EU-funded experiments in citizen data sovereignty (DECODE), and established watchdogs (Open Rights Group; Privacy International).

Together, these cases reveal complementary repertoires – strategic litigation, Freedom of Information (FOI) and policy work, tool-building and datasets, exhibitions and kits, coalitions and local networks – while insisting that privacy often functions as a **precondition for open and public knowledge in addition to transparency of social processes.**

Geography and politics matter: Central- and Eastern-European actors work under tighter civic constraints, making independent funding, cross-border alliances, and pragmatic hybridity (grassroots + institutional tactics) pivotal. Framed against datafication and surveillance capitalism, the common thread is **privacy as a collective condition for democratic life**, **not a mere consumer choice.**

Our analysis of case study examples reveals: (1) **Institutionalisation is non-linear:** groups oscillate between informality and formalisation as they balance safety, visibility, and impact. (2) **Plural strategies, shared goals:** legal enforcement (noyb, IuRe), civic-tech transparency (K-Monitor), creative computing and public pedagogy (Tactical Tech, Citizen D), and watchdog research (ORG, PI) are complementary rather than competing. (3) **Privacy as infrastructure:** for many, privacy is achieved via collective ownership and federated maintenance. (4) **Adoption, usability, and scale are hard:** ambitious techno-political builds expose trade-offs between cryptographic privacy, service usefulness, literacy, and long-term sustainability. (5) **Enforcement gaps persist:** uneven Data Protection Authorities (DPAs) capacity and regulatory capture mean civil-society litigation and coordinated complaints are crucial levers. (6) **Transparency + privacy co-depend:** anti-corruption/open-data work must pair proactive disclosure with sanctions and privacy safeguards to avoid new harms. (7) **Context sensitivity:** CEE cases (Panoptykon, SHARE, D3, Digital Freedom Alliance/ApTI) underline the value of independent funding, networks (EDRi, regional coalitions), and defensive security practices. (8) **Design matters for participation:** platforms like Wikipedia illustrate gendered and safety-related privacy asymmetries, showing

why defaults, identity management, and governance shape who can contribute. Overall, funders and policymakers should back bottom-up infrastructures, legal capacity, literacy, and cross-movement bridges to translate these experiments into durable, democratic data practices.

Ethical-approaches chapter: Based on the analysis of case studies, this chapter reframes online privacy as a moral and socio-technical project rather than a mere compliance exercise. It grounds grassroots activism in four core principles – **autonomy**, **informed consent**, **data justice**, and **contextual integrity** – and shows how these translate into community-centred practices such as **participatory design** and **privacy-as-a-commons**.

Against the backdrop of surveillance capitalism, it catalogues a repertoire of ethical resistance: exposing dark-patterned consent; defending the **right to opacity** and **ethical refusal** (minimal-data systems); and enacting **prefigurative politics** and **relational ethics** through open-source communities.

The chapter then turns to AI: it highlights how AI can bolster privacy (e.g. tracker detection) yet risks reproducing extractive logics, urging democratic accountability and safeguards against 'dataset hunger'. A major technical focus is **machine unlearning (MU)** ('forgetting by design' aligned with GDPR's right to erasure) surveying families of methods (influence-based updates, model perturbation, modular/ensemble designs), verification via membership-inference tests and differential-privacy bounds, inherent utility–privacy trade-offs, and policy instruments (standards, procurement attestation, open-source MU libraries, even a European Unlearning Office).

The overall claim: grassroots ethics can hard-wire dignity, autonomy, fairness, and collective governance into digital infrastructures, making privacy a condition for democratic life rather than a consumer afterthought.

Most important takeaways: (1) **Privacy is collective:** treat it as a shared precondition for participation and safety, not just an individual preference. (2) **Three ethical anchors →** practice: autonomy and *genuine* consent (beyond nudges), data justice that protects the vulnerable, and context-respecting flows (e.g. risks from digitising once-obscure public records). (3) **Design with, not for, people:** participatory methods and commons-oriented infrastructures operationalise ethics. (4) **Expose and counter manipulation:** document dark patterns and deceptive settings; centre platform accountability rather than user blame. (5) **Legitimise opacity and refusal:** minimal-data architectures and opt-outs are affirmative rights, not impediments to innovation. (6) **Prefigure alternatives now:** open, auditable code and community maintenance make ethics verifiable (relational trust > black boxes). (7) **Use AI carefully:** deploy AI for privacy protection while resisting co-optation, bias, and data maximisation; require transparency and contestability.

(8) **Make 'forgetting' practical:** embed MU hooks (checkpoints, modularity) early; accept that approximate, attestable unlearning, with measurable residual-influence bounds, is the realistic path at scale. (9) **Standardise and certify:** define auditor-ready MU metrics (e.g. membership-inference near-chance, Differential Privacy (DP)-calibrated noise) and tie them to procurement and conformity assessments. (10) **Resource equity matters:** fund open-source MU and literacy so Small and Medium-sized Enterprises (SMEs) and grassroots actors can comply without ceding ground to dominant platforms. Together, these points convert ethics from rhetoric into architecture, governance, and day-to-day practice.

Executive summary of the technical-approaches chapter: The chapter positions technology as both the vector of surveillance and the medium of resistance, and then maps a grassroots privacy-enhancing technologies (PETs) toolkit that spans **'hard PETs'** (encryption, anonymisation/pseudonymisation, decentralised architectures) and **'soft PETs'** (usable privacy – clear settings, opt-outs, supportive interfaces). Through concrete, regionalised use-cases we show how communities localise advanced methods for everyday safety.

At the cultural layer, **creative computing** and **tactical media** (e.g. Tactical Tech's *Glass Room*, the North Macedonian game *Track Me If You Can*) translate abstractions into graspable practice, while Free/Libre Open Software (FLOSS) (Nextcloud, CryptPad, Matrix/Element, Mastodon) anchors 'privacy-by-infrastructure' through auditability and self-hosting. Looking ahead, the chapter inventories **AI-adjacent PETs** (differential privacy, synthetic data, minimal-disclosure credentials, privacy automation, and AI-based tracker detection), arguing for deployments that enhance autonomy without reproducing 'dataset hunger'. **The chapter closes with a challenges → responses table (complexity, resources, adoption, censorship, sustainability) and a method: blend high-tech with low-tech pedagogy, localise tools, and govern them collectively so privacy becomes a shared capability, not a niche privilege.**

Most important takeaways:

1. **Two-tier PETs lens:** Distinguish **hard PETs** (crypto, anonymisation, decentralised designs) from **soft PETs** (usable defaults, clear choices). Both are required to make privacy *work* for non-experts.

2. **Encryption as baseline practice:** End-to-end encryption (Signal/Matrix) plus verification rituals and key-management training materially reduce interception and impersonation risks for Non-Governmental Organisations (NGOs), journalists, and whistleblowers.

3. **Anonymisation ↔ pseudonymisation trade-offs:** Pseudonymisation preserves utility for civic analytics while shielding identity; full anonymisation minimises risk but can limit usefulness.
4. **Differential privacy for aggregates:** Injecting calibrated noise lets communities publish trends (access, energy, mobility) without exposing individuals; utility–privacy balance must be explicitly managed.
5. **Keep data local when you can: Federated learning** and Secure Multi-Party Computation (SMPC) enable collective insight with minimal data movement (training on-device and computing across partitions without revealing raw records).
6. **Everyday stack, taught locally:** Privacy-centric browsers, Tor, reputable Virtual Private Networks (VPNs), burner e-mail, and tracker-blocking give immediate wins (especially in censored or high-risk contexts) when delivered via hands-on clinics.
7. **Advance beyond basics where needed:** Activist collectives can adapt Data Loss Prevention (DLP) and explore Secure Access Service Edge (SASE) architectures to prevent leaks and secure distributed work (once literacy and maintenance capacity exist).
8. **Make it visible, playable, memorable: Creative computing** and **tactical media** (exhibitions, games, story-driven tutorials) convert abstract harm into lived understanding, boosting adoption (e.g. youth gamification).
9. **Privacy-by-infrastructure (FLOSS):** Self-hosting **Nextcloud/CryptPad/Matrix** demonstrates accountable, auditable alternatives; peer training spreads skills and helps neighbouring NGOs replicate setups.
10. **AI for privacy, on clear terms:** Pair **DP**, **synthetic data**, **minimal-disclosure wallets**, and **privacy automation** with governance that resists data-maximalist drift; AI detectors can flag trackers in real time but must avoid new collection risks.
11. **Localise, translate, co-govern:** Training, language localisation, and shared stewardship turn tools into *institutions*; community governance sustains them after pilots end.
12. **Design for constraints:** Treat resource scarcity, censorship, and adoption friction as design conditions – blend high-tech PETs with low-tech outreach, document clearly, and budget for maintenance to keep infrastructures alive.

Recommendations and Conclusions

Privacy, this paper argues, is a collective infrastructure built and maintained by grassroots actors who blend legal enforcement, creative computing, FLOSS infrastructures, and privacy-enhancing technologies. These communities face persistent constraints – patchy regulatory enforcement, usability and adoption gaps, fragile funding, regional pressures, and official neglect – while navigating the non-linear, contested path of institutionalisation that pits visibility against safety

and transparency against privacy. Support must therefore reach beyond professionalised NGOs to include informal, Do-It-Yourself (DIY), and amateur initiatives through flexible funding, space, recognition, and protection that preserve autonomy. Two time-sensitive dynamics heighten the stakes: balancing privacy and transparency amid accelerated AI development, and safeguarding online interactions as cybersecurity risks intensify in Europe. Anchored in 'privacy as commons', prefigurative practice, usable PETs, accountable AI, and cross-movement coalitions, the section translates these insights into actionable levers.

The recommendations prioritise durable capacity: dedicated grants and Digital Autonomy Hubs; EU-level showcases; commons-cloud cooperatives; and paid open-source sustainers. They call for autonomy-respecting, institutional partnerships (red-line Memorandums of Understanding [MoU], participatory design, model charters, open documentation); regional collaboration (cross-border legal/policy labs, librehosting federations, European Digital Rights [EDRi]-style coalitions); and educational integration (Science, Technology, Engineering, the Arts, and Mathematics [STEAM] curricula, Privacy Clinics, teacher fellowships, localised repositories). PETs deployment is tied to usability, with audits, redesigns, and accessible automation. Accountable AI measures include unlearning attestations, open-source libraries, and independent 'deletion certificate' attestations with transparency dashboards. To close the enforcement gap, the paper proposes pooled litigation funds, complaint factories, and DPA–civil society liaison units. Finally, it makes FLOSS-first, self-hosted infrastructure a policy default; pairs transparency with privacy in open-data work; advances inclusive, safer participation; and embeds shared indicators and open learning to drive replication and long-term resilience.

II. Introduction

1. Online privacy and grassroots communities of digital computing

Privacy is a contested and multifaceted concept, interpreted differently across disciplines such as communication studies, sociology, law, and computer science. A wealth of scholarship, policy

frameworks, and legislation testifies to its centrality as one of the most pressing and polarising issues in contemporary societies shaped by big data and algorithmic control. Its heterogeneity and context-dependent nature have led researchers to treat privacy as a relational and situated issue (see Nissenbaum, 2004; 2009), inseparable from broader 'socio-technical systems and devices' and 'technology-based systems and practices' (Nissenbaum, 2009, p. 5). Online privacy, in particular, has proven to be deeply shaped by its empirical context and by shifting technological developments. Concerns over newspaper photography in the late 19th century (Warren & Brandeis, 1890) were fundamentally different from those provoked by the creation of large-scale state databases in the 1960s, or by the anxieties surrounding early Web 2.0 platforms such as MySpace and Facebook at the turn of the new millennium.

The rapid technological advances after 2010 (with the rise of big data, the algorithmisation of everyday life, and the platformisation of the internet) deepened anxieties around online privacy (Turow, 2011; Lyon, 2014) and prompted the EU's first major regulatory Artificial Intelligence (AI) response, the General Data Protection Regulation (GDPR) of 2017. Yet, the accelerating development of AI has further exposed the fragility of such protections, raising doubts about whether regulatory frameworks can keep pace with the logics of technological innovation and capitalist valorisation. In this light, online privacy has become a key site where the structural contradictions of platform capitalism (between control and autonomy, exploitation and rights) are most visibly played out (Zuboff, 2019).

Constant technological transformation continuously reshapes the ways in which privacy is conceptualised. In other words, what may link diverse approaches to privacy is precisely a persistent undercurrent of 'anxiety, protest and resistance in the name of privacy' (Nissenbaum, 2009, p. 3). Many of these concerns have also been articulated and contested through grassroots movements in digital computing, which are the focus of this white paper.

The meaning of privacy is highly context-dependent and varies significantly depending on whether we are discussing life in the urban public sphere, the online behaviour of internet users, the anonymity of hateful comments, the (mis)use of personal data by digital corporations, cyber threats or distinctions between the private and public sectors, spheres, or actors. However, this does not imply that the concept of privacy is entirely blurred or that systematic, time-transcending definitions are without value. For example, Judith DeCew (2013) identifies five distinct meanings and values of privacy, which remain relevant across diverse empirical contexts: (1) control over information; (2) human dignity or the protection of an 'inviolate personality'; (3) intimacy involving love, friendship, and trust; (4) the diversity of interpersonal relationships; and (5) exclusive access to a personal realm of one's own.

A crucial conceptual turn in thinking about privacy was driven by the technologically induced blurring of the once-clear divide between publicness and privacy that had been constitutive of modern democracies (see Bobbio, 1980/1989). In his classical conception, Dewey (1927/1954, p. 12) argued that transactions are private if their consequences concern only the people directly involved, and public if their relevance extends more broadly (see also Splichal, 2018). A major consequence of internetisation (and, more specifically, of the big-data turn and the algorithmisation of diverse social processes) is that even the most 'private' transactions are recorded and repurposed for ends far beyond those of the individuals directly involved.

Unsurprisingly, informal and self-organised grassroots movements in digital computing, such as Germany's Chaos Computer Club (CCC) or France's La Quadrature du Net, were among the pioneers warning against these developments. They operated at the intersection of the private and public spheres, balancing professional, free-time, and subcultural activities. Their involvement in technological developments took multiple forms: as technical experts who designed technology, as activists and advocates who raised concerns about its effects on privacy, and as users who sought to protect their privacy without abandoning the semi-public networks they had established with their peers. Their activities, which linked hacker ethics with broader civil liberties struggles, were crucial in establishing online privacy as a political cause.

The tension between the normative ideals of privacy and publicness long predates the internet, algorithms, and big data; it is embedded in the very foundations of modern European democracy. Enlightenment thought introduced the ideal of absolute transparency and visibility, epitomised by Bentham's panopticon (1787–1791/1995) and later critically reinterpreted by philosophers such as Foucault (1975/1995) and Deleuze (1992), while simultaneously giving rise to the bourgeois, private sphere and the right to privacy, tied to the rational, individualised subject. The historical evolution of the public–private divide is central here; privacy came to be framed as both the protection of personal autonomy and subjectivity, and as the preservation of private interest in the free market, conceived as a domain shielded from state interference. By contrast, publicness was articulated as the realm of collective visibility, accountability, and deliberation, where private interests were expected to yield to the common good.

This ambivalence between the ideals of privacy and publicness still persists today. The EU's regulatory approach to data protection, for instance, seeks to balance transparency and state oversight of private actors on the one hand, with the protection of individual rights on the other. A similar tension is visible in the activities of digital computing grassroots movements; some advocate for greater transparency in data flows, the protection of whistleblowers, and open-access code, while others concentrate on safeguarding private transactions, defending piracy and shadow libraries, and ensuring the privacy of online communication.

Without delving deeply into specific empirical contexts, it is impossible to decide unequivocally which of the two normative principles should prevail. As Splichal (2025, p. 10) observes, 'just as complete privacy has always been utopian – and probably never socially desirable – so too is the idea of "total publicness".' This very principle of uncertainty (according to which solutions are rarely black or white but instead lie somewhere among many shades of grey) underpins our effort to frame online privacy as a highly context-dependent issue. In this regard, not only the perspectives of 'data-hungry' digital giants or state authorities, but also those of grassroots digital movements and wider associations of internet users, or citizens more generally, must be taken into account.

This white paper maps and critically examines the observations, critiques, and self-organised actions of grassroots digital-computing communities that shape online privacy, while clarifying the ethical and technical stakes of activism and advocacy in this field. By treating privacy as a relational, context-dependent, and socio-technical phenomenon, it situates these grassroots practices within the broader dynamics of datafication, surveillance capitalism, and the long-contested boundary between the public and the private.

2. Surveillance Capitalism and the Datafication of Everyday Life

The process of datafication (driven by surveillance technologies, platformisation, and algorithmisation) marks a profound transformation in the modern relationships between individuals, corporations, and the state. It also radically complicates the once stable distinction between the public and private spheres, forcing us to rethink the broader context in which the issue of online privacy should be addressed. Datafication, namely, refers to the transformation of previously unquantified aspects of (private) life into quantified and monetised data (Cukier & Mayer-Schönberger, 2013). This can be seen as a continuation of the neoliberal transformations that began in the 1980s, which insisted 'that market functioning should govern all of life, not just formal economic processes', leading to 'the invasion of market logics into spheres previously protected from them' (Couldry & Mejias, 2019, p. 33). What was once considered part of the private sphere (separate from processes of value extraction) has now become a source of extraction itself: our online friendships, tastes, conversations, likes, and searches. Couldry and Mejias compare this expansion of value extraction into previously protected domains with the process of colonialism, coining the term 'data colonialism' – 'an emerging order for the appropriation of human life so that data can be continuously extracted from it for profit' (Couldry & Mejias, 2019, p. xi).

This shift is characterised by the increasing capacity to monitor, record, and analyse human behaviour through digital infrastructures, resulting in the commodification and predictive

manipulation of personal data. Central to understanding this phenomenon is Shoshana Zuboff's concept of surveillance capitalism (2019), which provides a detailed and critical framework for analysing the economic, technological, and ideological forces at play. Zuboff argues that surveillance capitalism is a novel economic logic. Unlike earlier forms of capitalism that relied on the production and sale of goods or services, surveillance capitalism is predicated on the collection and analysis of behavioural data.

Tech companies such as Google and Facebook pioneered this model by harvesting vast quantities of data generated by users that far exceeds what is necessary for the provision of their services. This 'behavioural surplus' is then processed and transformed into predictive products, which are sold to advertisers and other commercial actors seeking to influence and anticipate future behaviour. Data became the main source of profit for a variety of other platformised organisational forms such as social media platforms (Instagram, TikTok, etc.), video and audio streaming platforms (YouTube, Netflix, Spotify, etc.), cloud-based platforms and search engines (Microsoft 365, etc.), communication platforms (WhatsApp, ZOOM), gig economy and service platforms (Uber, Airbnb), E-Commerce platforms (Amazon, eBay), news aggregators, and many more.

Everyday activities, ranging from communication to consumption, are now routinely tracked, recorded, and analysed. The competitive pressures of surveillance capitalism drive corporations to pursue ever more granular and intrusive forms of data extraction, resulting in a continuous expansion of surveillance capabilities. Users are often incentivised to accept privacy trade-offs in exchange for convenience or security, thereby normalising the pervasive collection of personal information. Datafication enables predictive analytics (e.g. recommendation algorithms) and microtargeting (e.g. social media advertising) (Kant, 2020; Pariser, 2011; Chun, 2016); yet it also raises ethical concerns about autonomy, consent, and power imbalances, as marginalised groups face disproportionate harms from biased algorithms and discriminatory data practices (Chun, 2021).

Underlying all these processes is a profound, structural asymmetry between powerful digital platforms and individual users, who are compelled to give away their private information for free in order to participate in platformised everyday life online. It is not surprising, therefore, that individualised users are most vulnerable to this process, and that alternatives (such as the open-source, librehosting, piracy, and hacker movements) often take the form of (in)formal, decentralised collectives that operate somewhere between the public and the private spheres.

It is worth emphasising that the process of datafication substantially reshapes the issue of privacy protection and surveillance over individuals. Surveillance, which was traditionally understood as a state-driven activity, is now largely performed by private corporations, which demands a

different response. Unlike state surveillance, data tracking 'does not exist, in and of itself, simply to surveil or track users but to anticipate them […] to know some facet(s) of a user's identity' to make 'personally' relevant suggestions or selections (Kant, 2020, p. 9; see also Cheney-Lippold, 2017). By contrast, privacy regulation in the second half of the 20th century primarily aimed at protecting citizens from the state. Even the central idea of privacy protection (to prevent the identification of individuals) proves inadequate in the context of datafication, which can extract value from personal data (and contribute to manipulation) without ever revealing the identity of natural persons behind 'datafied subjectivities'.

However, the ideology of datafication extends well beyond the corporate sphere of digital platforms and is reinforced by a broader ideological and institutional context that also involves state authorities. Dataism fosters the belief that data-driven insights can reveal fundamental truths about human behaviour, legitimising the expansion of data collection into the public sector. This ideology is further entrenched through collaborations between governments, corporations, and academic researchers, who increasingly depend on big data, algorithms, and artificial intelligence for analytics, governance, and policy-making. The implications are far-reaching; Zuboff warns that surveillance capitalism poses a fundamental threat to democracy, as the privatisation of behavioural data enables new forms of social control and undermines both individual and collective self-determination. The collusion between technology companies and state agencies (brought to light by disclosures such as the Snowden leaks) underscores the dangers of unchecked surveillance and the erosion of democratic oversight. Dataism, as an underlying ideology, masks these power dynamics by presenting datafication as a neutral or scientific process rather than a mechanism of economic and political domination (van Dijck, 2014).

If states and commercial corporations (the two main institutions representing the public and private sectors) both rely on dataism and data extraction, it becomes structurally necessary to seek alternatives in the space between these spheres: in civil society more broadly, and in the grassroots movements of digital computing in particular. Despite growing public concern and scholarly critique, responses to the challenges of surveillance capitalism and datafication have often been framed through top-down regulatory approaches, such as privacy legislation, data protection frameworks, and platform accountability mechanisms. While these measures are undoubtedly important, they face significant limitations in scope, enforcement, and conceptual reach. Many regulatory regimes, including the EU's General Data Protection Regulation (GDPR), continue to assume the legitimacy of data extraction, provided it is subject to informed consent and transparency. Yet this model struggles to address the profound asymmetry of power between users and data-driven corporations, where consent is often coerced or obscured by complex terms of service.

Furthermore, regulatory mechanisms tend to lag behind the pace of technological innovation. By the time new rules are debated, legislated, and implemented, dominant platforms have already adapted their infrastructures or shifted their practices to circumvent compliance. Regulatory approaches are also often hampered by jurisdictional limitations; the transnational nature of digital data flows makes it difficult for national or regional bodies to assert meaningful control over global tech corporations. As a result, these measures risk reinforcing a reactive posture (treating symptoms rather than addressing the structural dynamics of surveillance capitalism itself).

In light of these limitations, scholars and practitioners have increasingly turned their attention to bottom-up, grassroots responses that challenge dominant data regimes not through institutional authority but through creative, collective action. One promising direction is the emergence of creative computing within activist, educational, and community-based contexts (Beraldo & Milan, 2019). Creative computing refers to the use of computational tools and methods not only for efficiency or utility but as a means of artistic expression, critical engagement, and civic empowerment. In contrast to corporate or state-centred applications of data analytics, creative computing emphasises autonomy, experimentation, and context-sensitive design.

Grassroots initiatives that employ creative computing often reclaim digital tools for alternative purposes: community archives that preserve local memory outside dominant data infrastructures; DIY sensor networks that monitor environmental conditions without corporate mediation; or educational platforms that teach algorithmic literacy through participatory workshops (Gutiérrez & Milan, 2017; Pei & Crooks, 2023). These practices invert the extractive logics of datafication by foregrounding human agency, situated knowledge, and collaborative inquiry. Rather than treating users as passive data sources, such initiatives encourage people to actively shape the digital environments they inhabit.

Importantly, these efforts are not merely reactive but prefigurative, offering visions of what more just and inclusive data futures might look like. They challenge the determinism of dataism by demonstrating that computation can be socially meaningful without being exploitative. In doing so, grassroots creative computing opens up a space for imagining alternatives to surveillance capitalism (not only through critique but through practice). These initiatives underscore the importance of cultivating digital literacy, ethical design, and democratic control over technology from the ground up.

3. Online Privacy as a Socio-Technical Issue

Surveillance capitalism’s exploitation of personal data has fundamentally redefined online privacy, transforming it into a contested terrain where individual autonomy is systematically

traded for corporate profit. At the core of this dynamic is the extraction of behavioural surplus – data collected beyond what is necessary for service provision. For example, Facebook's collaboration with Cambridge Analytica demonstrated how psychographic profiling could weaponise personal data to manipulate voter behaviour, exposing the fragility of consent in an ecosystem where users are often unaware of how their information is monetised (Cadwalladr, 2018; Chun, 2021).

The erosion of privacy is further exacerbated by the symbiosis between corporate and government surveillance. While surveillance capitalism thrives on data extraction for profit, governments increasingly rely on corporate platforms for intelligence-gathering, creating a feedback loop that amplifies intrusiveness. The Snowden leaks revealed how tech firms provided backdoor access to intelligence agencies, blurring the lines between commercial data collection and state surveillance (Greenwald, 2014). This collusion normalises pervasive monitoring, as seen in proposals to leverage social media metadata for public health analytics or counterterrorism, effectively outsourcing surveillance to private actors. Such practices institutionalise a form of dataveillance that operates continuously and ubiquitously, undermining traditional notions of privacy as a right to be 'left alone' (van Dijck, 2014).

The political economy of data extraction must be situated within a broader sociotechnical framework (Ochs & Ilyes, 2013) to fully appreciate the complexity of online privacy. While the concept of surveillance capitalism highlights how corporate and state actors exploit personal data for profit and control, a sociotechnical perspective reveals the underlying interplay between technological infrastructures, user behaviours, and institutional norms that make such exploitation possible (Star & Ruhleder, 1996; Bowker & Star, 1999). Rooted in Science and Technology Studies (STS), this approach emphasises that social and technical elements do not operate in isolation; instead, their interaction produces emergent outcomes that shape system performance and societal impact (Ochs & Löw, 2012; Bijker & Law, 1992). Within this framework, Susan Leigh Star's work on infrastructure emphasises that technologies are not neutral tools but are deeply embedded in social worlds, shaping and being shaped by routines, classifications, and power relations (Star, 1999).

Accordingly, privacy in online spaces is fundamentally shaped by the dynamic interplay between technology and social practices wherein digital platforms operate as complex, heterogeneous systems and where user behaviours, algorithmic architectures, and institutional policies co-evolve and mutually reinforce each other (Roessler & Mokrosinska, 2015). Within these environments, privacy is not a singular or static concept but is experienced and negotiated across multiple dimensions.

A key distinction in the literature is between institutional privacy (the protection of personal information from access and use by corporations, governments, and other organisations) and social privacy, which concerns the management of information within one's social circles and peer groups (Stoycheff, 2023). Technical architectures embedded within platforms often prioritise granular controls for social privacy, enabling users to manage who among their contacts can see specific content or profile information (Network Readiness Index, 2023). However, these same architectures frequently obscure or minimise the visibility of institutional data extraction, creating significant power asymmetries. Users may feel empowered to curate their digital presence among peers, yet remain largely unaware of or unable to meaningfully control the collection and use of their data by powerful institutional actors (Stoycheff, 2023).

Philosophers and legal scholars have further critiqued the traditional, individualistic approach to privacy, arguing for a broader social and contextual understanding. Helen Nissenbaum's theory of contextual integrity emphasises that privacy norms are context-dependent and that the flow of information should be governed by the specific social roles, relationships, and expectations present in each context (Nissenbaum, 2010). This approach highlights that privacy is not merely a matter of individual control or consent, but is fundamentally shaped by institutional arrangements and collective values.

Behavioural economics research adds another layer of complexity, revealing that individuals often trade personal data for perceived benefits, such as convenience, personalisation, or discounts, despite expressing concerns about surveillance and data misuse (Acquisti, 2010). This phenomenon, sometimes called the 'privacy paradox', is exacerbated by the opacity of data flows and the difficulty individuals face in accurately assessing the risks and consequences of their disclosures.

Finally, regulatory frameworks such as the GDPR have sought to address some of these power imbalances by granting individuals rights over their data. However, critics argue that such regulations often fail to fully acknowledge or redress the deep-seated asymmetries between individual users and institutional actors, particularly in the context of collective harms and the challenges of enforcing rights at scale (Ada Lovelace Institute, 2023). This is another reason why the perspective of grassroots movements in digital computing is important: it helps overcome the reductive duality between macro- and micro-actors – between platforms and states on the one hand, and individuals (users, citizens) on the other.

4. Global Approaches to Privacy Regulation: U.S., China, and the EU

Regulatory approaches to online privacy vary significantly across the globe. The major global standard-setters in this field, or digital empires as Anu Bradford (2023) names them, are the EU,

the U.S., and China. Each jurisdiction has developed a regulatory model that reflects broader societal orientations toward the relationship between the individual, the state, and the private sector. Their models are shaped by different legal traditions, cultural values, and political economies, which are reflected in technical differences but also in fundamental settings regarding the conceptions of rights, governance, and market power in the digital age.

4.1 From Commodification to Control: U.S. and China's Competing Visions of Digital Privacy

In the U.S., the regulation of privacy and personal data remains highly fragmented and largely reactive. Personal data is commodified and traded on a massive scale with little oversight. Some exceptions in the U.S., such as in California, exist. This state passed the Consumer Privacy Act (CCPA), an important step toward greater accountability and a signal of growing recognition of the risks (Hoofnagle et al., 2019). The U.S. regulatory approach has historically prioritised innovation and market freedom over individual rights, leading to a situation where corporations exercise disproportionate influence over digital spaces. As Zuboff (2019) warns, without structural interventions to disrupt the underlying economic incentives that drive data extraction and behavioural prediction, privacy protections risk becoming cosmetic rather than transformative (mere 'fig leaves' that mask the continued erosion of individual autonomy).

In stark contrast to the market-driven model of the U.S., China's approach to privacy and personal data regulation is characterised by a state-centric orientation. The adoption of the Personal Information Protection Law (PIPL) in 2021 marked a turning point in China's regulatory approach. It established a comprehensive personal data legal framework that regulates its collection, use, and cross-border transfer. While the PIPL mirrors certain elements of the EU's GDPR (such as the emphasis on transparency, consent, and the rights of data subjects), it diverges significantly in its underlying objectives. The PIPL serves not only to protect individuals but also to consolidate state authority over digital ecosystems, ensuring that data governance aligns with broader national security priorities.

The PIPL grants individuals rights to access, correct, and delete their personal data, but it places significant emphasis on national security and government oversight in regulating cross-border data flows. Its focus on localised data storage, heightened protections for minors, and strict supervision of major digital platforms reflects China's strategy for balancing personal privacy with broader state interests in the digital economy. Major technology platforms like WeChat, Alibaba, Tencent, and ByteDance face enhanced regulatory obligations, including the establishment of independent supervisory bodies and the publication of regular transparency reports. Government oversight is a defining feature of the PIPL, with regulatory bodies empowered to conduct inspections, impose corrective measures, and levy fines of up to 5% of annual revenue

for non-compliance (state-centric enforcement model that prioritises centralised control over data flows and security).

4.2 Between Surveillance and the Market: The EU's Third Way in Data Regulation

Some of the main documents outlining Europe's policies in the sphere of privacy and data protection are the *Commission Communication on Data Protection* (European Commission, 2019), *Two Years of GDPR* (European Commission, 2020a), and *European Data Strategy* (European Commission, 2020b). According to the latter document, the ambition of the EU is to 'become a leading role model for a society empowered by data to make better decisions – in business and the public sector' (2020). To achieve that, Europe has to be better than 'the competitors such as China and the US' (European Commission, 2020b, p. 3). The report argues that in the U.S., organisation of the data space has been 'left to the private actor, with considerable concentration effects'. On the other hand, China has 'a combination of government surveillance with a strong control of Big Tech companies over massive amounts of data without sufficient safeguards for individuals' (ibid.).

The EU has positioned itself as a global leader in championing a rights-based approach, which is also its main specificity in comparison with the U.S. and China. It understands personal data protection and privacy as fundamental rights and posits it as such within the broader framework. The EU's regulatory model reflects a deeply rooted philosophical commitment to individual dignity, autonomy, and informational self-determination, shaped by historical experiences with authoritarian surveillance regimes.

At the centre of the EU's privacy architecture is the GDPR, which establishes a comprehensive legal regime for personal data protection across member states and beyond. It codifies data protection principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, and accountability. Crucially, the GDPR applies extraterritorially to any entity processing the personal data of EU citizens, thereby setting a global benchmark for data protection compliance.

Along with GDPR, other legislative instruments further extend the EU's data protection framework. The ePrivacy Directive (European Parliament & Council, 2002), often referred to as the 'Cookie Law', regulates the confidentiality of electronic communications and the use of tracking technologies. This directive is under review, and while the EU intended to replace it with an ePrivacy Regulation, the ePrivacy Regulation proposal has been withdrawn. The Data Governance Act (DGA) represents a more recent initiative aimed at fostering a European data economy by promoting the use of data intermediaries and facilitating the ethical sharing and reuse of public sector data.

In response to the growing dominance of large online platforms, the EU has also adopted the so-called digital package, Digital Markets Act (DMA), the Digital Services Act (DSA), and the AI Act (AIA). All three instruments are risk-based, meaning that they impose stricter obligations on the types of activities or actors who possess increased risk. The DMA seeks to curb anti-competitive practices and promote fair markets by regulating the behaviour of the so-called 'gatekeepers', a very influential digital market competitor. The DSA regulates content moderation, algorithmic transparency, and user data protection, prescribing special duties for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). AIA classifies AI systems based on the risk they generate. Notably, it prohibits some of the practices which have a significant impact on privacy, such as harmful manipulation, social scoring, and real-time remote biometric identification. Sector-specific measures such as the Law Enforcement Directive (European Parliament & Council, 2016) ensure that data protection principles are respected in the sensitive context of criminal justice, emphasising proportionality, necessity, and independent oversight. The NIS2 Directive (European Parliament & Council, 2022), while primarily addressing cybersecurity threats, introduces significant privacy implications through mandating the protection of personal data by critical infrastructure operators and digital service providers, especially in the aftermath of cyber incidents.

Judicial developments have played an equally pivotal role: the Schrems I (Court of Justice of the European Union, 2015) and Schrems II (Court of Justice of the European Union, 2020) decisions by the Court of Justice of the EU invalidated the International Safe Harbor Privacy Principles (European Commission, 2000) framework and later the EU–U.S. Privacy Shield framework (European Commission & U.S. Department of Commerce, 2016). The reasoning was that these legal instruments failed to guarantee that the fundamental rights of EU citizens must be protected even when data is transferred abroad. Furthermore, the Court of Justice of the EU in several decisions, and most notably in the 2014 Google Spain case (Court of Justice of the European Union, 2014) held that the internet search engine operator is responsible for the processing that it carries out of personal data that appears on web pages published by third parties, and that a data subject may request removal of such data. This decision was recognised as confirming the existence of the so-called 'the right to be forgotten'.

Recently, the EU's digital regulatory trajectory has started showing signs of recalibration in the wake of global political shifts, particularly with the return of Trump-era realpolitik and deregulatory sentiment on the international stage. While the Union has long positioned itself as a normative power in digital governance, recent developments indicate a mild but perceptible shift towards regulatory restraint. The effective abandonment of the AI Liability Directive (European Commission, 2022) and the long-stalled ePrivacy Regulation suggest a waning appetite for legal expansionism (Lomas, 2025a). Parallel to this, core instruments such as the GDPR (Lomas, 2025b), the AIA (Smith, 2025), and the DSA (de Vreese, 2025) are increasingly subject to

calls for ‘pragmatic application’ and proportional enforcement, particularly from industry stakeholders and certain Member States. The Draghi Report (made by Mario Draghi, former European Central Bank President and one of Europe’s great economic minds on his personal vision on the future of European competitiveness) marks an important point. It emphasises economic competitiveness, innovation, and institutional simplification over prescriptive regulatory layering (European Commission, 2024). It appears that we are entering an era of the EU’s subtle repositioning.

Digital sovereignty has emerged as one of the central themes in European discourse. It refers to Europe’s ability to make independent decisions in the digital realm, grounded in its own values and rules. This encompasses control over physical infrastructure, code, and standards as well as data and content. Several factors have driven the shift in EU policy, including growing concerns about disinformation and surveillance, coupled with the dominance of powerful digital platforms. Together, these developments have created what is often described as a ‘sovereignty gap’. To strengthen its position, the EU should also invest in local grassroots movements in digital computing (initiatives such as collaborative networks, digital cooperatives, and open-source projects). These efforts not only enhance local control and reduce reliance on global tech giants but also encourage bottom-up innovation and better reflect European values of participation and transparency. The EU can support this by providing dedicated funding, regulatory facilitation, education, and opportunities for networking. In this way, digital sovereignty would be cultivated not only from above (through institutions and companies) but also from below (through citizens and communities).

The U.S., China, and the EU face similar challenges posed by digital technologies, but their regulatory approaches are fundamentally different. Due to their role in the global economy, their choices are inevitably going to shape the future trajectory of global digital governance, with profound implications for democracy, economic competition, and the protection of human rights.

Data privacy laws play a critical role in the modern digital landscape. They protect individual rights, establish business accountability, promote transparency, and foster responsible innovation. With the rapid growth of data collection, individuals need control over their personal information. Privacy laws not only require organisations to disclose their data practices, but also impose standards for data protection and handling. By creating clear boundaries and responsibilities, data privacy laws help maintain trust in digital platforms, encourage ethical practices in data use, and support data sovereignty.

5. Methodological Approach: A Situated, Mixed-Methods Design

Our perspective is necessarily shaped by our specific empirical encounters, and the knowledge we share is **situated knowledge** – what Donna Haraway (1991, p. 590) famously calls 'views from somewhere'. We do not claim the position of objective scientists who can represent grassroots initiatives of digital computing (and their perspectives on online privacy) from above. As Haraway reminds us, 'situated knowledges require that the object of knowledge be pictured as an actor and agent' rather than as a 'slave to the master […] and his authorship of "objective" knowledge' (1991, p. 592).

It is precisely with this understanding in mind that we turn to the case studies presented in this text. They offer a grounded exploration of grassroots initiatives across Europe that are actively shaping the landscape of online privacy. These organisations, while diverse in structure, strategy, and regional context, share a commitment to defending digital rights, resisting surveillance capitalism, and promoting ethical, community-centred approaches to technology. By examining their histories, practices, and impacts, we aim to illustrate how grassroots actors contribute to the broader struggle for privacy, autonomy, and justice in the digital age.

The selection of case studies was guided by a qualitative research design focused on capturing the richness and complexity of privacy activism throughout Europe. Organisations were chosen based on three core criteria: (1) regional diversity, (2) sustained engagement with privacy-related issues, and (3) a demonstrable focus on creative computing practices. The inclusion of initiatives from Western, Central, and Eastern Europe, as well as Mediterranean and Nordic contexts, highlights the geographical and cultural plurality of digital rights movements.

The case studies were analysed through a thematic lens informed by the conceptual framework developed in earlier sections of the white paper. **Key themes included autonomy, informed consent, data justice, contextual integrity, participatory design, and ethical refusal. These principles served as analytical anchors, enabling a comparative reading of how different organisations interpret and enact privacy in practice.** For example, while DECODE in Barcelona emphasises privacy as a commons through decentralised data governance, Panoptykon in Poland foregrounds the right to opacity in resisting corporate and state surveillance. Tactical Tech in Germany, meanwhile, exemplifies prefigurative politics by embedding ethical design into public education and creative computing.

The case study analysis was conducted through extensive desk research, focusing on publicly available materials produced by the organisations themselves. This included a close examination of each initiative's official website, published reports, blog posts, press releases, and social media presence. These sources provided insight into the organisations' missions, activities, ethical

frameworks, and strategic priorities. Where relevant, additional secondary sources such as media coverage, academic references, and policy documents were consulted to contextualise the organisations' work within broader national and European debates on digital rights and privacy. In addition, in specific cases, we conducted interviews with members of the grassroots organisations.

Finally, the case studies offer more than descriptive accounts; they provide critical reflections on the possibilities and limits of grassroots privacy activism in Europe. By documenting these efforts, we seek to amplify their contributions, identify patterns of innovation and resistance, and inform future policy and research aimed at supporting democratic, ethical, and inclusive digital environments.

Analysis proceeds through an iterative theory–practice dialogue; we apply critical theories of technology to the cases while also deriving normative claims from situated practices. Findings are organised in two interlinked streams:

1.) ethical approaches that articulate community-centred principles and power critiques
2.) technical approaches that operationalise those principles through tools, infrastructures, and design patterns, providing a triangulated evidence base for the paper's recommendations.

On the technical side, we assess privacy-enhancing technologies and architectures (such as end-to-end encryption, anonymisation/pseudonymisation, differential privacy, federated learning and secure multiparty computation, front-end tools in everyday use, and FLOSS infrastructures) with attention to usability, accessibility, and community governance; we also document creative-computing and tactical-media interventions that translate complex risks into public pedagogy, and incorporate emerging topics including AI-assisted privacy tooling and machine unlearning where relevant. Throughout, we follow ethical research procedures (informed consent, data minimisation, limited retention and anonymisation for interview materials) and acknowledge limitations, including a Europe-centred sample, language constraints, and reliance on publicly available sources.

III. Case Studies

1. Institutionalising Grassroots Innovation: Creative Computing and Privacy in Focus

Online privacy is a multifaceted issue that weaves together many interconnected debates. It is not only a central concern of grassroots advocacy, activism, and creativity, but also deeply

embedded in the very structure of grassroots initiatives themselves. Privacy shapes their organisation, influences their institutional standing, and accompanies their transformations over time (from informal, subcultural beginnings to the more complex, and sometimes formally institutionalised, forms). This transition is often marked by a shift from anonymous, informal, and non-traceable practices to more institutionalised, formal, and transparent activities. Yet, the process can also unfold in the opposite direction, as groups reassert the value of anonymity and informality. The conceptual tension between privacy and publicness thus plays out in concrete ways within grassroots organisations, shaping the dilemmas they face in their everyday practices.

Digital grassroots movements in Europe are marked by the striking diversity of their institutional forms and the contexts in which they operate. Some emerge as informal collectives governed by unwritten rules, while others are organised as NGOs. Some take shape as private institutions active on the market, while others focus on building public infrastructure and depend on public or state funding. Their fields of activity are equally varied: from the art world (net art, web art, inter- and transmedia art) to human rights advocacy, from open-source software communities to the demoscene and gaming networks. Many participants identify with subcultural affiliations (gamers, hackers, or geeks) while others situate their activities in professional roles as activists, coders, artists, or researchers.

There are, therefore, as many forms of institutional organisation as there are grassroots movements, which means that each organisation's story is unique and that broad generalisations are inevitably problematic. Our analysis is based on informal interviews with members of such organisations in Slovenia and Croatia, as well as on desk research into some of the most well-known European movements active in the field of online privacy.

Our conceptual decision to frame online privacy within the logic of data capitalism is thus grounded in the experiences of various grassroots movements. For example, members of the Slovenian collective Kompot – part of the broader European librehosters network (Librehosters, n. d.) – emphasise that their guiding principle is 'emancipation and independence from digital platforms and corporate service providers'. For them, the struggle for online privacy goes far beyond protecting personal data or preserving anonymity. As they explain, 'the most important aspect of privacy for us is being independent from the tech-corporations'. Simultaneously, they aim to develop 'a different model of service provision, in which users are not merely consumers but also "owners" and "maintainers" of services'. Their aim is to 'dissolve the conventional distinction between provider and client, and with it the structural inequality embedded in commercial platforms'. They reject 'sharing of data with business partners or state authorities', 'commodification of personal data, behavioural surveillance, manipulative design, aggressive advertising, and other strategies of user capture and addiction' (Kompot, n.d.).

In this light, privacy emerges less as a primary aim than as a by-product of a broader effort to overcome the structural divide and to assume collective ownership of the services upon which we rely. This understanding of privacy rests on mutual trust among local creative computing enthusiasts, the federated logic of infrastructure maintenance, and a DIY ethos. Kompot provides independent email services, mailing lists, collaborative writing pads, cloud services, translation tools, Matrix chat, Git server, event announcement tool, etc. (for a full list of their services see Kompot, n.d.). They also organise different knowledge sharing workshops, in which they aim to spread and connect technical knowledge with specific worldview: 'We want to build a community that is resilient to corporate monopolisation and progressive in its understanding and use of contemporary technologies' (see Kompot, n.d.).

Members of Kompot recognise that no single institutional form can fully accommodate their aims and objectives. For this reason, they have remained an informal collective, characterised by a flexible capacity to adapt to changing circumstances. They maintain cohesion through regular meetings and are open to collaboration with a variety of external actors in the local (Ljubljana/Slovenia) community. For example, they have provided technical infrastructure solutions for the alternative Radio Študent and collaborated with the Maska Institute active in performing arts (on the project *Yugofuturism*), the urbanist magazine *Prelom*, the autonomous anarchist space *Infoshop*, and the artistic institution focused on digital and new media art *Ljudmila*.

On the international level, they have primarily built their network through continuous participation in the Chaos Communication Congress, a large annual gathering of European hackers that usually takes place in Hamburg. The event is organised by the Chaos Computer Club, one of the oldest hacker communities in Europe, which continues to embody the ethos of grassroots engagement and the fight for digital rights from the ground up. In this spirit, members of Kompot are open to collaborating with different institutional forms, but they remain committed to functioning as an informal collective (a position that also means Kompot does not provide a significant source of income for its members).

All technical knowledge is shared according to the ethos of open-source code and knowledge sharing, but with the prudence to ensure it is not appropriated for private or commercial interests. Even if their work could be done remotely, due to their informal organisation, meetings in physical space proved to be of crucial importance. They have never had their own 'headquarters' but have instead been hosted in Ljubljana's autonomous spaces (Rog and Plac) as well as in various cultural venues (Hupa Brajdič, Radio Študent, etc.). At the time of writing (spring 2026), they organise monthly Linux installation parties and collaborate with several local student reading groups (such as GIA, Critical Psychology, and others). They acknowledge that their mission can never be fully accomplished and are aware of the structural inequalities between

hyperlocal, open-source and open-code initiatives and global digital platforms. Nevertheless, they find satisfaction in small steps (such as changing the online habits of a few individuals) and in gradually building alternatives from below.

The case of the Kompot collective, which has remained an informal grassroots organisation, is just one (albeit quite common) outcome in the diverse trajectories of such collectives. The story of another informant, Marcel Mars from Croatia, founder of the Multimedia Institute mi2 and the net.culture club mama in Zagreb, presents a similar yet somewhat different path toward institutionalisation. Mars is a well-established figure in the field of creative computing and in hacker's subculture – described as a 'free software advocate, cultural explorer, and social investigator' (Mars, n.d.) – who began his career in the 1990s. He particularly emphasised the importance of the numerous international connections that he and his peers cultivated (with the Ljudmila collective in Slovenia, Transmediale in Berlin, Ars Electronica in Linz, and ZKM in Karlsruhe) which enabled them to escape 'the banality of nationalist politics' in Croatia that emerged after the dissolution of Yugoslavia.

At the same time, he underscored that international networks themselves are marked by dividing lines. The U.S., with its strong market, academic, and military complex, has taken a leading position in technologic developments. By contrast, Mediterranean countries such as Italy, Spain, and France remained somewhat behind (largely due to linguistic differences) and developed a different culture of creative computing, one deeply tied to local grassroots and autonomous communities (such as Autistici in Italy or Barcelona's autonomous squat scene). According to Mars, online privacy has become a central issue particularly for German grassroots movements, likely shaped by historical experiences with totalitarian regimes. Developments in Northern Europe, such as in Sweden with Piratbyrån, were more closely aligned with the cyberpunk movement and dependent on donations. Donations and external funding also played an important role in Eastern Europe, where the creative computing scene was often more isolated.

In Croatia, the Clubtura project received support from the Soros Open Society Foundations, which later proved crucial for advocacy at the local level in Zagreb, particularly in creating public spaces for youth culture and creativity. From these movements (bringing together figures such as Tomislav Medak and Teodor Celakowski) emerged the left-wing green political party *Možemo!* ('We Can!'), which today plays an important role in both national and local politics. Some participants in these grassroots initiatives eventually entered politics, others (like Mars himself) pursued careers in professional coding and software engineering, while still others moved into academia. In the academic/research context, together with Valeria Graziano and Tomislav Medak, Mars contributed to the development of the concept of *Pirate Care* (2025), rooted in the practices and experiences of hacker and pirate grassroots movements.

Grassroots movements in digital computing are diverse, dispersed, and heterogeneous, which makes the historical reconstruction and archiving of their activities a considerable methodological and epistemological challenge. More institutionalised and transparent activities, such as human rights advocacy in the online environment, as practiced by members of the EDRi network, tend to gain greater visibility than less formalised practices, such as hacker and pirate movements.

The EDRi network brings together more than 50 organisations and individuals (including NGOs, experts, advocates, and academics) working to defend and advance digital rights across Europe. Its work is structured around three main pillars: information democracy, open internet and inclusive technology, and (most relevant for our context) privacy and data protection. In this field, EDRi has launched several high-profile campaigns in recent years, including Reclaim Your Face (opposing biometric identification in public spaces), SaveYourInternet.eu (challenging upload filters that risk mass surveillance), and SaveTheInternet.eu (defending net neutrality). Their activities primarily revolve around advocacy and lobbying in legislative processes, complemented by awareness-raising and educational campaigns. Yet, the more experimental practices of creative computing (once central to some of EDRi's founding members) have become less prominent in the network's current focus. With the institutionalisation and legal formalisation of grassroots movements, certain elements of hacker and piracy ethics appear to have faded into the background.

For certain initiatives (especially those that are legitimate yet not always strictly legal) privacy is crucial for their sustainable functioning. The relationship between privacy and publicness becomes particularly complex in the context of open knowledge sharing, as exemplified by shadow libraries such as LibGen, Anna's Archive, Sci-Hub or Memory of the World / Public Library. In such cases, the privacy of peers who share knowledge is the very condition for the publicness and openness of the knowledge itself (see Karaganis, 2018). The most famous examples of such projects are Sci-Hub and LibGen. Sci-Hub, a search and download service for journal articles, is based on a simple yet radical idea: to 'mobilize university colleagues to share not individual articles, but "virtual private network" credentials for campus intranets in Western universities, which enabled access to the major journal databases' (Karaganis, 2018, p. 1). Establishing such databases depends on informal networks of trust characteristic for other movements of creative computing. Unfortunately, Western scientific publishers and EU copyright legislation have largely responded to these developments with legal repression. In this context, Monoskop (an online archive focused on art, media theory, and philosophy) serves as a valuable counterexample: a community-based project that remains legal while functioning as both a significant resource for researching the history of European digital computing and an enduring example of grassroots activity since the early 2000s.

A particular challenge in reconstructing the historical trajectories of grassroots movements is that we often see only the tip of the iceberg (the institutionalised organisations) while the movements themselves, along with the temporary encounters and sometimes anecdotal events that led to such stages, remain obscured. For example, well-known French organisation Quadrature de net that advocates on the EU level for the founding principles of the internet (protection of privacy, openness, and neutrality) was first the informal collective of activists established in 2008 and became a formal organisation only in 2013. The DECODE project that provides tools that empower individuals in controlling their personal information (or share it for the public good) is an established formal project funded by Horizon 2020, but preserved the ethos of grassroots movements that argued for digital democracy. Tactical Tech, established in 2003, started as a small non-profit organisation in a hairdresser salon in Amsterdam and later grew and established informal offices worldwide.

In conclusion, the trajectories of grassroots digital movements reveal that institutionalisation is never linear but marked by constant negotiation between informality and formalisation, anonymity, and visibility, privacy, and publicness. Online privacy emerges here not only as a form of protection but also as a condition for openness, collaboration, and the creation of alternatives to corporate platforms. Much of this history remains hidden beneath the surface of formal organisations, yet it is precisely in these less visible practices that new democratic and resilient technological futures are being imagined.

2. Grassroots Movements

2.1 Noyb – None of Your Business (Austria), founded in 2017

Noyb (None of Your Business) is a Vienna-based, privacy advocacy organisation co-founded by the Austrian lawyer and activist Max Schrems in 2018. Emerging from grassroots origins, particularly the ‘Europe vs Facebook’ campaign (launched in 2011), noyb has rapidly developed into one of Europe’s most prominent actors in enforcing the GDPR through litigation and strategic legal action. Unlike artistic or educational initiatives such as Tactical Tech, noyb exemplifies what might be termed *legal activism as creative resistance*, leveraging law as a technical and political tool to resist surveillance capitalism. Its work responds directly to the criticism raised in surveillance studies and legal scholarship, particularly concerning the limits of consent-based privacy models (Solove, 2013; Zubhoff, 2019), the institutional weaknesses of enforcement authorities (Veale et al., 2018), and the normalisation of data extraction as a socio-technical infrastructure (Mejias & Couldry, 2019).

Noyb's core activism lies in strategic litigation by filing coordinated GDPR complaints against major tech firms, such as Meta, Apple, and Google for their data handling practices. These actions address what Zubhoff (2019) describes as 'surveillance capitalism's behavioural surplus', denoting the extraction and commodification of user data beyond what is needed for service provision. Litigation is not simply punitive; it is system-building, seeking to test and clarify the meaning and enforcement limits of existing laws. In doing so, noyb creates legal precedents that reassert the rights-based logic of GDPR in a data environment increasingly shaped by opaque algorithms and platform monopoly. This mirrors what Mantelero (2014, p. 646) describes as 'privacy by design': moving beyond individual control towards institutional accountability mechanisms. Noyb's work reveals the legal and conceptual tensions between user consent and structural exploitation, akin to what van der Sloot (2017, p. 50) identifies as the inadequacy of 'notice and consent' in the face of algorithmic profiling and asymmetrical power relations.

Where Tactical Tech uses creative computing to empower users, noyb practices legal engineering by meticulously constructing arguments, cases, and precedents to intervene in regulatory frameworks. This aligns with research findings in computational law and code-driven regulations (e.g. Hildebrandt, 2016), which recognises that technical and legal infrastructures are increasingly entangled in governing behaviour. While less participatory in form, noyb's activities parallel these trends by turning law into an activist toolkit by deploying templates, automated complaint generation, and jurisdictional triangulation to scale up grassroots legal pressure.

Noyb operates on the premise that systemic enforcement of privacy rights requires collective legal action and not just personal vigilance. Perhaps noyb's most influential intervention was the case popularly known as Schrems II, in which the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield agreement between the EU and the United States in 2020 (Fantin, 2020). This followed the earlier Schrems I decision, which had already struck down the Safe Harbor framework in 2015. Both cases were initiated by Max Schrems and litigated under the auspices of noyb, targeting the inadequate protections afforded to EU citizens' personal data transferred to the U.S.. At the heart of both rulings was the recognition that U.S. surveillance laws, especially Section 702 of FISA and Executive Order 12333, lacked sufficient safeguards, transparency, and legal redress for non-U.S. persons.

As Kuner (2020) notes, the CJEU determined that the law of the U.S. does not provide a level of protection essentially equivalent to that guaranteed within the EU, especially regarding access by U.S. intelligence authorities and the absence of judicial remedies for European citizens. Consequently, both data transfer frameworks were deemed invalid. These rulings not only reshaped transatlantic data flows but also forced companies and regulators to reconsider the adequacy of cross-border data governance. Importantly, these decisions exemplify what De Gregorio (2020, p. 47) terms 'digital constitutionalism': the attempt to embed fundamental rights

into the architecture of global digital governance through binding legal mechanisms. Through litigation, noyb advances a form of bottom-up legal resistance that insists on the primacy of rights even in transnational regulatory contexts. By focusing on collective rights enforcement and regulatory consistency across jurisdictions, noyb also draws attention to the fragmentation and uneven enforcement of European data protection law. This aligns closely with the findings of Veale et al. (2018), who document persistent enforcement gaps in GDPR implementation, particularly regarding cross-border complaints and delays in regulatory decision-making by national DPAs.

Although not a cultural or artistic organisation, noyb does engage in public education, offering accessible explanations of legal concepts, GDPR rights, and complaint procedures. These efforts democratise legal knowledge and align with critical digital literacy frameworks (Livingstone, 2004; Pangrazio and Selwyn, 2018), expanding citizens' understandings of their role within opaque data infrastructure. This 'education by legal design'-approach encourages public participation in legal enforcement processes, reframing users as legal actors rather than passive consumers or data subjects.

Despite, or because of, their broad public engagement, noyb maintains a critical distance from formal regulatory institutions. Although it has had a vital role in shaping GDPR enforcement, it is often outspoken about the failure of national DPAs, especially in Ireland and Luxembourg, where major tech firms are headquartered. This stance underscores a broader concern about regulatory capture, which is also a theme developed in critical legal studies and data governance literature (Bennett & Raab, 2020). This institutional friction parallels Tactical Tech's cautious engagement with state actors as both organisations model different forms of autonomy: Tactical Tech avoids institutional co-optation through cultural critique, while noyb does so through adversarial legal pressure.

The strategic litigation practised by noyb reveals the limits of the EU's regulatory infrastructure, particularly its reliance on national DPAs that vary in resources, capacity, and political will. These disparities undermine the promise of GDPR as a harmonised and enforceable rights framework. As Kuner (2020) argues, the Schrems rulings highlight how the legitimacy of the EU data protection regime depends on its ability to provide real protections, not just on paper but in practice. To meet this challenge, EU policy must prioritise institutional coherence, transparency, and enforcement consistency, particularly in handling cross-border data cases. Funding and legal capacity building should extend to civil society organisations like noyb, which play an essential role in activating legal rights and pressuring authorities to act.

Essentially, noyb's success shows that enforcement should not be left solely to regulators, but can be meaningfully pursued through strategic litigation by independent actors. This calls for the

EU to treat litigation-led activism not as an adversarial nuisance, but as a vital pillar of democratic accountability in the digital domain. Policy should encourage synergies between legal and educational approaches to data protection, integrating noyb's rigorous enforcement model with public-facing initiatives like Tactical Tech to foster a digitally literate and rights-conscious citizenry. In doing so, the EU would reinforce its normative commitment to digital constitutionalism and sustain its position as a global leader in human-centred technology governance.

2.2 Iuridicum Remedium (IuRe) and Digitální Svobody (Czech Republic), founded in 2001

Iuridicum Remedium (IuRe) is a Czech, non-profit organisation dedicated to the protection of human rights in the digital age, with a focus on legal advocacy, transparency, and civil liberties. Founded in 2001 and based in Prague, IuRe has developed a strong reputation for strategic litigation, public interest law, and watchdog activities in areas such as data protection, surveillance, and algorithmic decision-making. Grounded in a legalistic approach to activism, IuRe combines expert policy analysis with legal action, aiming to ensure that digital technologies respect fundamental rights and democratic norms.

As part of a broader mission, IuRe launched the initiative Digitální Svobody (Digital Freedom), which functions as a public-facing campaign and a platform for civic engagement around issues of online privacy and surveillance. While IuRe operates at the intersection of law and policy, Digitální Svobody expands the organisation's reach by engaging the public more directly through educational content, policy briefings, and advocacy campaigns. It serves as IuRe's vehicle for translating complex legal challenges into accessible language, mobilising public support, and intervening in digital policy debates in the Czech Republic and at the EU level.

Digitální Svobody has become a central actor in the fight against surveillance legislation in Europe. In 2024, it played a prominent role in opposing *ChatControl*, a controversial EU proposal that would mandate the automated scanning of private messages and images under the pretext of combating child sexual abuse (Hynek, 2025). Drawing on IuRe's legal expertise, Digitální Svobody mounted a coordinated campaign that included writing to Czech ministers, briefing parliamentarians, and rallying public support. Their advocacy contributed to the Czech Republic adopting a neutral stance, which ultimately helped derail the proposal at the EU level during the Belgian Council Presidency. When a revised version was later revived under Hungary, Digitální Svobody again helped mobilise resistance, underlining its role as a nimble and persistent watchdog. At the national level, Digitální Svobody has also worked to protect privacy from

domestic, legislative threats. In 2024, it opposed amendments to a Czech law requiring hospitality services to retain guest data for state access (Digitální Svobody blog, 2025). After securing a favourable ruling from the Supreme Court, the law was partially reinstated by lower courts (a development that prompted renewed legal appeal and policy engagement). This case illustrates how Digitální Svobody leverages IuRe's legal acumen while engaging broader publics and policymakers through advocacy.

Academically, the initiative aligns with criticism of the limits of consent-based, privacy frameworks and the persistence of asymmetrical power relations in digital governance. Scholars such as Cremonini (2023) and Zuboff (2019) have argued that surveillance capitalism and opaque platform infrastructures cannot be adequately countered by informed consent alone. Instead, systemic legal and cultural interventions are needed. Digitální Svobody exemplifies such an intervention, addressing structural threats to privacy through legal advocacy, public mobilisation, and a clear stance against normalising mass surveillance. Moreover, recent empirical studies have shown that legal frameworks such as GDPR, while impactful, have limitations in curbing the data practices of powerful actors (Puhlmann et al., 2023). Miller et al. (2024) call for more user-facing tools to make privacy rights meaningful. Digitální Svobody contributes to closing this gap by informing the public about their rights, monitoring compliance, and advocating for legal reforms that go beyond formal compliance to address deeper, structural dynamics.

Digitální Svobody therefore exemplifies how grassroots legal activism, when embedded within an institutional framework like IuRe, can drive systemic change in digital privacy. By translating legal expertise into accessible advocacy and public education, it bridges the gap between formal legal structures and everyday users. Its work illustrates a model of privacy activism that is grounded in law, but amplified through civic engagement and digital literacy, demonstrating that legal resistance and grassroots mobilisation can beare not opposing strategies, but complementary forces in the defence of digital rights.

2.3 DECODE – Decentralised Citizen-Owned Data Ecosystem (EU-wide, origins in Spain, pilots in Amsterdam and Barcelona), founded in 2016

DECODE, the Decentralised Citizens Owned Data Ecosystem, was a Horizon 2020 EU-funded research and demonstration project that ran from 2016 to 2019. Coordinated by the Institut Municipal d'Informàtica de Barcelona and involving a consortium of European partners such as Nesta, Dyne.org, ThoughtWorks, and University College London, the project was conceived as a response to the mounting concerns around surveillance capitalism and the erosion of personal agency in the digital sphere. In its framing documents, DECODE underlined that people had lost

control over how their personal data is used and set itself the ambitious goal of reversing this trend by equipping individuals with the technical means to control, withhold, or selectively share their own data.

At the technical level, DECODE's architecture combined open-source infrastructure with advanced privacy-preserving methods. Its developers created a modular 'DECODE OS' capable of managing personal data flows in anonymised form, relying on cryptographic techniques to ensure that information could be shared in secure and consensual ways. Blockchain and smart contract technologies underpinned this system, allowing users to establish the conditions under which their data could be accessed or reused, while maintaining robust safeguards against exposure of raw data. This architecture was explicitly designed to mediate between individual privacy and collective utility; it sought to enable personalised services and communal applications without reverting to the extractive logic of major technology platforms.

The project was not limited to technical development. It also launched pilot deployments in European cities, most notably Barcelona and Amsterdam. These pilots served as living laboratories where DECODE's tools were tested in practice. They explored themes such as collaborative economies, the Internet of Things in smart cities, and digital participation in democratic processes. Through these pilots, the project attempted to uncover how citizens might use privacy-preserving data services in daily life, how consent could be operationalised in complex contexts, and how new forms of data governance might function outside the theoretical realm.

DECODE's achievements lay not only in the software it produced but also in its conceptual reframing of data politics. By demonstrating tools that returned decision-making authority to citizens, it moved the debate away from passive data extraction and towards a model of active, contextual data sharing. This was more than a technical contribution; it was a normative assertion that digital sovereignty should belong to citizens, not corporations. The project also devoted significant energy to public debate. Events such as the 2018 Barcelona conference *Beyond Surveillance Capitalism: Reclaiming Digital Sovereignty* created platforms for discussion among technologists, policy-makers, activists, and ordinary citizens. These discussions extended the impact of DECODE beyond its immediate pilots, embedding it within wider European conversations about digital rights, consent, and governance.

Another important outcome was the project's contribution to policy framing. By working at the intersection of technical design and political discourse, DECODE offered concrete models for how

consent, anonymisation, and contextual data sharing could be structured. This provided useful reference points in the European Union's evolving policies on privacy and data sovereignty. Furthermore, the project's commitment to open-source release and modular design ensured that its outputs would remain available to future initiatives, potentially serving as building blocks for other privacy-enhancing technologies and citizen-led data ecosystems.

Despite these achievements, DECODE also encountered challenges that reveal the complexity of reshaping digital infrastructures. One major difficulty was adoption. Encouraging citizens to engage with technically sophisticated tools proved demanding as it required a level of data literacy that could not be assumed. Many participants found the concepts of consent dashboards or blockchain-mediated, privacy management unintuitive, which limited uptake. The project thus highlighted the educational gap that accompanies even the most well-intentioned, technological interventions. A second challenge lay in balancing privacy with usability. In many cases, anonymised or heavily abstracted data became less useful for creating meaningful services or for informing policy decisions. Yet providing more detailed data always carried the risk of re-identification. Managing this tension in lived contexts proved difficult, and the trade-offs sometimes weakened the practical appeal of the system. A third difficulty related to sustainability and scale. Although DECODE succeeded in building and deploying prototypes, ensuring their long-term viability required institutional commitment and governance structures that went beyond the project's remits. As with many experimental initiatives, the transition from pilot to permanent infrastructure remained elusive. Finally, the project exposed friction between its decentralised vision and existing regulatory frameworks. European data protection law, particularly the GDPR, while designed to protect citizens, interacts in complicated ways with blockchain-based consent systems and anonymisation standards. The legal and institutional context therefore both enabled and constrained DECODE's ambitions.

Nevertheless, DECODE provides a rich set of lessons that resonate with wider debates about the future of digital society and the governance of personal data. At its heart, the project sought to reframe technology from an extractive system into one that amplifies user agency. This ambition reflects broader efforts across Europe and beyond to imagine digital infrastructures that serve citizens rather than corporations, and to ensure that individuals can determine how their data is collected, shared, and used. The emphasis on consent and contextual decision-making mirrors wider concerns with embedding technology in political, economic, and cultural environments that respect diversity and local autonomy. In this sense, DECODE illustrates how technological systems can be shaped not just by market imperatives but also by social values and collective priorities.

The project also underscores the importance of coupling technical innovation with public debate. It showed that developing privacy-preserving tools is insufficient unless accompanied by meaningful dialogue between citizens, policymakers, and institutions. Only through such dialogue can technologies be understood, legitimised, and embedded in everyday practices. This lesson has wider implications for democratic governance in the digital age; if infrastructures are to be trusted and sustainable, they must be subject to negotiation, contestation, and public scrutiny rather than being imposed top-down or left to market forces.

Similarly, DECODE's reliance on pilot-based experimentation demonstrates the value of treating test environments as sites of technical development and also as spaces of collective learning. Pilots created opportunities to explore the tensions between privacy, usability, and governance in real-life contexts, providing insights that could not be gained from theoretical models alone. This approach reflects a growing recognition that digital innovation must be iterative, participatory, and context-sensitive if it is to achieve legitimacy and long-term success. At the same time, DECODE's struggles with scale and sustainability highlight the systemic barriers faced by citizen-led and decentralised infrastructures. While such initiatives can be visionary, translating experimental prototypes into enduring institutions remains a significant challenge. The project revealed how issues of legal compatibility, institutional inertia, and entrenched economic interests can limit the durability of decentralised solutions. Understanding why certain initiatives thrive while others fade away is crucial for policymakers, technologists, and activists seeking to build alternative digital futures.

DECODE therefore stands as a valuable European experiment in data sovereignty and citizen control over digital infrastructures. Although its focus was on personal data management rather than broader domains of digital practice, the principles it embraced (agency, consent, transparency, and collective governance) resonate with many ongoing debates about the democratic potential of technology. The project illustrates the possibilities of bottom-up innovation to challenge dominant paradigms, while also exposing the fragility of such efforts when confronted with regulatory complexity, institutional inertia, and the power of established platforms. DECODE's legacy is therefore both inspirational and cautionary: it demonstrates that reclaiming digital agency is possible, but it also reminds us of the persistent obstacles that must be overcome to secure truly citizen-centred digital ecosystems.

2.4 Tactical Tech (Germany), founded in 2003

Tactical Tech, a Berlin-based NGO, exemplifies how grassroots initiatives can resist the extractive logics of surveillance capitalism and datafication through creative computing and public

engagement. Founded in 2003, Tactical Tech empowers individuals and communities to critically engage with the political and social implications of digital technologies. Its work intersects closely with key concepts articulated by scholars like Zuboff (2019), Meijas and Couldry (2019), and van Dijck (2014), offering a prefigurative model of ethical, participatory, and democratic responses to dominant digital infrastructures. Tactical Tech's activities revolve around a critical reappropriation of data practices for empowerment rather than exploitation. This aligns with creative computing as defined by Beraldo and Milan (2019), who state that it denotes using computational tools for civic empowerment, critical engagement, and artistic expression.

Their major projects, such as the 'Data Detox Kit', 'The Glass Room' exhibitions, and 'Exposing the Invisible', embody alternative digital practices by (1) educating users about privacy, surveillance, and data rights, (2) demystifying data collection and algorithmic processes, (3) empowering communities to make informed decisions about their digital presence, and (4) fostering artistic and activist interventions that challenge normative assumptions about technology. By producing interactive exhibitions, toolkits, and participatory workshops, Tactical Tech offers alternatives to passive data consumption, thus directly confronting the ideology of dataism that van Dijck (2014) criticises, while also clearly problematising the economic and political structures as identified by Zuboff (2018):

- *Human experience as raw material*: Tactical Tech highlights how corporations transform personal life into behavioural surplus, especially through hidden infrastructures like data brokers.
- *Predictive analytics as control mechanisms*: Exhibits like 'The Glass Room' make visible the opaque predictive mechanisms used to shape user behaviour without explicit consent.
- *Normalisation of surveillance*: Through public campaigns, Tactical Tech encounters the 'normalisation'-process by providing tools for critical literacy and alternative digital habits.

Importantly, Tactical Tech does not simply advocate for individual privacy as a consumer choice but frames privacy and data agency as collective rights, positioning them as prerequisites for democratic participation, thereby echoing Zuboff's (2019, pp. 509–512; pp. 518–520) warning about the erosion of democracy under surveillance capitalism: 'Privacy is not private; it is a collective good, necessary for democracy. It is a condition for a free society, not a product sold on the market' (Zuboff, 2019, p. 510).

In the context of grassroots movements, Tactical Tech's work is distinguished by its bottom-up structure and prefigurative orientation. This is marked by community-driven, knowledge production as it collaborates with local groups, adapting resources to different cultural and

political contexts rather than imposing top-down, technical solutions. Furthermore, it provides accessible modular resources, such as the 'Data Detox Kit', which exemplifies tactical modularity by providing simple, adaptable materials that can be locally disseminated and customised. This is tied in to artistic and activist synergy, with projects such as 'Exposing the Invisible' blending journalism, activism, and creative computing to support investigative practices free from corporate or state surveillance. In some cases, these exhibitions are highly participatory, for example, by exhibits such as 'The Glass Room' exemplifying participatory design and allowing audiences to interactively explore issues rather than passively consume narratives. These practices directly counter datafication's abstraction of human life into quantifiable data points, emphasising instead situated knowledge, personal context, and agency.

While Tactical Tech's primary impact is educational and cultural, it has indirectly influenced policy debates and shifted public discourse in Europe. This is evidenced in their partnerships with public institutions, such as collaborations with NGOs, schools, and public libraries across Europe. Outreach and visibility are also generated through public exhibitions in civic spaces, for example, by situating 'The Glass Room' in shopping centres, libraries, and schools, thereby reaching diverse publics outside academic or activist bubbles.

The initiative's reach is also visible in inspirations for EU digital literacy initiatives; although Tactical Tech operates outside traditional policy-making channels, its work has informed broader discussions about digital literacy, data rights, and ethical technology design, which feature increasingly in EU policy frameworks, such as the Digital Services Act discussions. However, although involved in outreach policy planning, Tactical Tech carefully guards its autonomy from state structures, avoiding co-optation and maintaining a critical stance (a deliberate strategy to avoid reinforcing the very institutional dynamics that entrench surveillance capitalism).

In light of implications for EU policy, Tactical Tech's model suggests several strategic directions for the EU's approach to surveillance technologies and datafication:

- *Support bottom-up, digital literacy*: Funding grassroots initiatives like Tactical Tech can cultivate resilient, informed publics capable of challenging exploitative digital practices.
- *Recognise alternative computations*: Policy frameworks should validate and support creative, community-centred uses of data technologies rather than focusing solely on corporate compliance mechanisms.
- *Promote participatory infrastructures*: Beyond enforcing transparency, the EU should encourage participatory technological design processes where users meaningfully shape the platforms and services they use.

- *Challenge dataism ideology*: Policymakers should adopt critical perspectives on data-centric ideologies and fund research and initiatives that foreground social, cultural, and ethical dimensions of digital life.
- *Sustain independent initiatives*: Ensuring long-term, independent funding streams for activist and educational projects is crucial to prevent the depoliticisation of grassroots efforts.

Tactical Tech thus provides a powerful example of creative computing as a form of digital resistance and democratic renewal. By empowering individuals and communities to understand, criticise, and subvert surveillance infrastructures, it offers a tangible vision of alternative futures beyond the extractive imperatives of surveillance capitalism. Incorporating lessons and methods of initiatives like Tactical Tech into EU policy frameworks could help build a more just, democratic, and human-centred digital environment in Europe.

2.5 K-Monitor (Hungary), founded in 2007

K-Monitor is a Hungarian non-profit organisation founded in 2007, dedicated to fighting corruption, increasing transparency in public spending, and promoting accountability in government decision-making. Over the years, it has developed a reputation as one of the more capable civil society actors engaged in anti-corruption, open data, freedom of information, and civic empowerment in Hungary. Its work spans research, advocacy, legal action, technological tool-building, public interest journalism, and community engagement.

At its core, K-Monitor believes that corruption thrives where opacity persists, and civic disengagement grows. The organisation works on the premise that citizens have the right (and capacity) to demand transparency, to access and understand data about how public funds are used, and to hold decision-makers accountable. To achieve that, it combines multiple avenues:

- *Open data, databases, and digital tools:* K-Monitor builds and maintains online systems that track public spending, contracts, subsidies, and projects. Their public funds monitoring database comprises many thousands of items, including investigative reports and articles, making visible what would otherwise remain hidden. Tools like 'Hotel Oligarch' map businesses or entities linked to politically exposed persons, and redflags.eu (in cooperation with other NGOs) monitors procurement risk. These tools enable journalists, watchdogs, and citizens to explore patterns, spot irregularities, and follow up.
- *Freedom of information litigation and strategic legal work:* K-Monitor frequently uses legal requests to access data, challenging public bodies when information is delayed,

withheld, or hidden. It has taken many cases to court or sought constitutional review. Their complaints often expose gaps in the law, implementation problems, and institutional resistance.

- *Advocacy, policy watch, and legal reform:* The organisation examines reforms to laws on transparency and freedom of information, proactively reports on shortcomings (for example, when new disclosure rules exclude many bodies, or allow fragmented, hard-to-use data). It engages with governmental processes where possible, critiques failures to implement reforms, and proposes improvements.
- *Public awareness, community tools, and civic engagement:* Workshops, journalist partnerships, public-facing reports, and metrics are part of K-Monitor's strategy. In addition, 'Code for Hungary' volunteers help to build tools, visualisations, maps, and apps. Annual summaries of their work show the organisation both informing the public about issues (how public funds are spent, where irregularities lie, etc.) and equipping citizens and local actors with the means to demand accountability.

Over its lifespan, K-Monitor has accumulated several measurable successes and broader impacts:

- *Strengthening civil society capacity:* Through open data projects, micro-grants, workshops, and methodological support, K-Monitor has helped other NGOs enhance their ability to use public data, make analyses, produce visualisations, and engage in policy debate.
- *Real-world transparency improvements:* Through systematic audits and assessments of municipalities, public companies, local councils, and asset-management entities, K-Monitor has exposed which institutions meet transparency thresholds and where the weakest spots lie. For example, an evaluation of 31 municipal asset management companies found many deficiencies in disclosures; after publishing those results, some companies improved practices once under scrutiny.
- *Legal precedents and institutional pressure:* K-Monitor's legal and FOI requests have resulted in majority wins in court, forcing public bodies to reveal previously withheld data (budget documents, contracts, procurement materials, and so on). These efforts contribute to the body of case law and improve the legal culture around access to information.
- *Policy monitoring and criticism:* K-Monitor has been active in assessing the implementation and gaps in reforms, such as those pertaining to freedom of information laws. It has raised concerns when government disclosure platforms omit key players, or when legal obligations are weakly enforced. Its reporting gives voices to otherwise under-observed deficits in institutional transparency.
- *Public engagement and awareness:* Through fact-based investigations, media reporting, public tools, and data-driven storytelling, K-Monitor has increased public awareness of

how public funds are used, of corruption risks, and of the often hidden linkages between political power and economic actors. Citizen interest is nurtured by accessible tools and by showing that misuse or secrecy can be exposed and remedied.

Despite its achievements, K-Monitor operates in a challenging environment and continues to face a range of structural obstacles. One persistent difficulty is political resistance and institutional inertia. Many public bodies remain slow or even unwilling to comply with transparency obligations, and even when laws are reformed on paper, their implementation often lags behind. Exemptions in legal frameworks further undermine openness by excluding entire categories of institutions that spend public money, such as municipally owned or state-owned companies, or entities that fall outside the definition of 'budgetary status'. These gaps make it easier for large sums of public funds to escape scrutiny. Data fragmentation and poor usability compound the problem. Although Hungary has introduced new registers for proactive disclosure, much of the information is scattered across different platforms, locked in formats that are difficult to download in bulk or not machine-readable. Legal obligations for disclosure may formally exist, but in practice, weak or delayed enforcement means that accountability is undermined.

Another significant obstacle is legal and regulatory ambiguity. The scope of existing transparency laws does not cover all relevant institutions, leaving loopholes that can be exploited to avoid oversight. Even where oversight bodies have been granted powers, these are sometimes toothless; enforcement mechanisms such as fines or sanctions are either absent or insufficient, while opt-out provisions allow institutions to sidestep obligations altogether. Resource and funding pressures add yet another layer of difficulty. Running sophisticated databases, pursuing legal challenges, conducting investigative research, and sustaining lengthy court cases requires skilled staff, technical expertise, and stable financial support. For NGOs like K-Monitor, these needs are made more acute in politically charged civic spaces, where organisations may be subject to stigmatisation or regulatory scrutiny, particularly when they rely heavily on foreign grants to sustain their operations. Finally, K-Monitor must continually grapple with the challenges of citizen engagement and trust. The tools and platforms it provides are powerful, but their effectiveness depends on citizens' willingness to use them, to care about the issues at stake, and to believe that demanding accountability can make a difference. Public fatigue, apathy, or distrust can erode impact over time, while barriers such as limited digital literacy or technical knowledge prevent wider segments of the population from making use of available resources.

The experience of K-Monitor offers several lessons that resonate far beyond Hungary and are instructive for broader debates about transparency, civic technology, and digital accountability. It demonstrates that transparency tools must not only be developed but also maintained and continually improved. A database or registry on its own is insufficient; long-term usability depends on regular updates, error correction, open interfaces, and designs that accommodate

different types of users. Legal reform, too, is necessary but never sufficient. Laws mandating disclosure create an important framework, but without robust enforcement, institutional commitment, and active public monitoring, they risk remaining symbolic. Strategic litigation and ongoing oversight are vital complements.

The organisation's work also underscores the importance of proactive disclosure coupled with meaningful enforcement. When requirements to publish contracts, procurement data, ownership records or budgets are backed by an authority with the power to sanction non-compliance, the likelihood of evasion or delay is significantly reduced. Similarly, K-Monitor illustrates how civic participation and public pressure can multiply the impact of transparency initiatives. Through workshops, partnerships with journalists, and volunteer networks, raw data can be transformed into stories that resonate with people's everyday concerns. When citizens know where to look and are provided with narratives that help them interpret the information, accountability becomes not only a legal principle but also a social and political force.

Finally, the question of financial sustainability remains critical. Heavy reliance on foreign donors can leave organisations vulnerable to political attacks that portray them as externally controlled or illegitimate. Building more diverse sources of funding, such as small local donations or income-generating services, can provide greater resilience and independence. Taken together, these insights show the promise and the precarity of transparency work in constrained political environments. K-Monitor's activities reveal how data, law, and civic engagement can be combined to push institutions toward accountability, but they also highlight the structural barriers that must be overcome if such efforts are to endure.

2.6 Panoptykon Foundation (Poland), founded in 2009

The Panoptykon Foundation, established in Poland in 2009, has become one of the leading organisations in Central and Eastern Europe dedicated to digital rights, privacy, and civil liberties in the face of expanding surveillance. Named after Jeremy Bentham's and Michel Foucault's concept of the 'panopticon' (a metaphor for constant surveillance), the foundation explicitly positions itself as a watchdog and advocate against opaque data collection, authoritarian control, and the exploitative dynamics of surveillance capitalism. From its inception, the foundation positioned itself as a civic watchdog seeking to defend democratic oversight against the encroachment of corporate and state surveillance. This makes it not only a legal advocate but also an educator and community-builder, one that translates abstract digital rights into accessible campaigns and concrete interventions.

The organisation emerged out of Poland's post-communist context, a country where memories of authoritarian surveillance by the state remain vivid. Against this background, Panoptykon's founders (lawyers, activists, and civil society advocates) set out to build an institution that would defend citizens against new forms of monitoring and control that risked reproducing authoritarian tendencies under digital capitalism. Its mission has consistently been to protect human rights in the surveillance society, combining legal advocacy, policy influence, and public education to ensure that privacy and transparency are not treated as luxuries but as essential conditions for democratic life.

Panoptykon has pursued this mission through a range of strategies. One central pillar of its work is legal advocacy and litigation. The foundation has regularly challenged both state and corporate practices that infringe upon privacy rights, often through strategic litigation designed to set legal precedents. Its interventions in the debate over Poland's data retention laws exemplify this approach; by pointing to the lack of sufficient safeguards and oversight, it sought to demonstrate that such laws not only compromise individual privacy but also undermine democratic accountability. In this respect, Panoptykon has parallels with noyb in Austria, another grassroots organisation that uses law as both a technical instrument and a political tool to enforce the provisions of the GDPR and other frameworks.

Another key strategy lies in active policy engagement. Panoptykon contributes to legislative debates in Poland and at the EU level, providing critical perspectives on instruments such as the GDPR, the Digital Services Act, and national reforms of surveillance powers. It does so not as a distant critic but as a constructive participant, proposing alternative frameworks that emphasise human dignity, democratic oversight, and data justice. By aligning itself with networks such as European Digital Rights (EDRi), the foundation strengthens its position within a broader coalition, ensuring that perspectives from Central and Eastern Europe are not overshadowed by the often better-resourced NGOs in Western Europe.

Public education is an equally important dimension of Panoptycon's activities. The foundation recognises that privacy cannot be secured by legal frameworks alone; citizens must also understand and demand their rights. To this end, it produces podcasts, reports, and educational campaigns that explain complex issues, such as algorithmic profiling, targeted political advertising, and facial recognition, in a language accessible to non-specialists. Its podcast *Panoptykon 4.0* is an example of how it uses accessible media to reach wider audiences and to counteract the normalisation of surveillance. By doing so, Panoptykon contributes to the development of digital literacy in Poland, enabling citizens to grasp how everyday interactions with platforms like Facebook or Google are tied to broader structures of manipulation and control.

The thematic focus of Panoptykon's work reflects the organisation's dual concern with corporate surveillance capitalism and state surveillance. Drawing on the criticism articulated by Shoshana

Zuboff (2019), the foundation highlights how corporations systematically commodify user data, engaging in behavioural profiling and targeted advertising under conditions where meaningful consent is absent. At the same time, it remains deeply attentive to state practices, particularly Poland's volatile political environment. The organisation has consistently scrutinised police use of facial recognition, legislative attempts to expand the powers of security agencies, and data-sharing practices that lack democratic oversight. A further area of concern is algorithmic accountability; Panoptykon draws attention to the hidden consequences of automated decision-making in areas ranging from welfare distribution to credit scoring, arguing for greater transparency, explainability, and mechanisms of redress for affected citizens.

The foundation's work has led to significant achievements. Through its legal interventions, it has contributed to national and European rulings that curtailed indiscriminate data retention. Its litigation against excessive surveillance laws has reinforced democratic checks on state power. In terms of policy debates, Panoptykon has successfully positioned itself as a respected interlocutor consulted by national and European institutions. Beyond these institutional victories, its success also lies in shaping public debate; by reframing privacy as a collective right essential to democracy, it has expanded the horizon of digital rights discourse in Poland. The organisation's public-facing initiatives, including podcasts and reports, have deepened digital literacy and raised awareness of the dangers posed by opaque data practices. Finally, Panoptykon has become a leader within coalitions, ensuring that the concerns of Central and Eastern Europe are integrated into EU-level debates on digital governance.

These achievements, however, are accompanied by persistent challenges. The political context in Poland has been difficult, with populist governments often limiting the space available for civic organisations to influence policy. Resource constraints are another obstacle; like many NGOs, Panoptykon depends heavily on project-based funding, which can limit its long-term stability. Public apathy and mistrust also pose barriers, since privacy can appear as an abstract issue compared with more immediate economic or social concerns. To counteract this, Panoptykon has to continually find new, creative ways to demonstrate the everyday relevance of privacy. Moreover, the foundation faces the structural imbalance of power between civil society and global technology cooperations; despite successful lawsuits or campaigns, the vast resources of companies such as Meta or Google allow them to adapt quickly to new regulations, often outpacing the capacity of watchdog organisations.

Within the broader landscape of European privacy activism, Panoptycon occupies a distinctive position. It shares similarities with noyb in its reliance on strategic litigation but differs from Tactical Tech, which focuses more on cultural interventions and creative media such as *The Glass Room*. Panoptykon instead embodies a legal-policy-education nexus, balancing institutional influence with grassroots engagement. In regional terms, its presence is particularly significant since it demonstrates that privacy activism is not solely a Western European concern. By

providing a strong voice from Central and Eastern Europe, it diversifies and strengthens the European digital rights movement.

The foundation's significance extends beyond immediate advocacy by exemplifying prefigurative politics: enacting democratic alternatives in the present rather than waiting for future reforms. In Panoptykon's work, privacy is framed as a collective condition of democracy rather than as an individual commodity. Its emphasis on systemic reforms resonates with criticism of the limitations of consent-based privacy models as articulated in the research by Zuboff (2019) and Nissenbaum (2009). By combining legal expertise with public mobilisation, it demonstrates how grassroots initiatives can scale up to influence European governance while remaining accountable to local communities.

The lessons drawn from Panoptykon's case are clear: Independent funding is crucial for sustaining its role as a watchdog, free from both corporate and governmental co-optation. Cross-border collaboration must continue to be strengthened, as EU institutions rely on actors like Panoptykon to translate high-level frameworks into national contexts. Public literacy remains a key investment, since without informed citizens, even the strongest regulations risk remaining ineffective. Finally, vigilance is needed to guard against authoritarian appropriation of surveillance laws under the guise of security. The Panoptykon Foundation represents a vital strand of European privacy activism. Rooted in Poland's democratic struggles, it has developed into a respected and influential voice on digital rights, while maintaining its grassroots orientation. Its work shows that privacy advocacy in Europe is multifaceted, encompassing legal interventions, educational campaigns, and coalition-building. At a time when datafication and surveillance capitalism are intensifying, Panoptykon's insistence that privacy is a condition for democracy rather than a market commodity provides both a warning and a roadmap. For policymakers, activists, and citizens alike, the foundation demonstrates how grassroots organisations can resist surveillance while building more democratic digital futures.

2.7 D3 – Defesa dos Direitos Digitais (Portugal), founded in 2017

D3 (Defesa dos Direitos Digitais) represents a significant example of how grassroots digital rights activism can emerge and evolve within the European context. Its foundation coincided with a period of heightened awareness about digital privacy, surveillance, and the growing influence of state and corporate actors over personal data. D3's trajectory illustrates the challenges and opportunities faced by grassroots organisations as they navigate the complex landscape of digital rights, privacy advocacy, and institutional engagement in Southern Europe. D3 was created in response to a perceived gap in Portugal's civil society landscape regarding digital rights. While

other European countries, particularly in Northern and Central Europe, had already developed robust networks of digital rights organisations, Portugal lagged behind in both public awareness and organised advocacy. The founders of D3 recognised the need for a dedicated platform to defend fundamental rights in the digital environment, particularly as issues such as mass surveillance, data retention, and algorithmic discrimination became increasingly salient. The organisation's mission is rooted in the defence of civil liberties, the promotion of transparency, and the protection of privacy in the face of expanding digital infrastructures.

From its inception, D3 adopted a multifaceted approach to digital rights advocacy. It combines legal analysis, public education, policy engagement, and coalition-building. This strategy reflects an understanding that effective digital rights activism requires technical expertise and the ability to communicate complex issues to a broad audience. D3's activities range from monitoring legislative developments and submitting policy recommendations to organising public campaigns and participating in international networks. The organisation's work is informed by a strong ethical commitment to autonomy, informed consent, and data justice – principles that are increasingly recognised as central to the European digital rights movement. One of D3's features is its emphasis on legal and policy advocacy. The organisation closely monitors national and European legislative processes, intervening when proposed laws threaten to undermine privacy or civil liberties. For example, D3 has been active in criticising and challenging data retention laws in Portugal, arguing that blanket data retention is incompatible with fundamental rights as articulated by the European Court of Justice. The organisation has also engaged with debates around biometric surveillance, facial recognition, and the use of AI in public administration, highlighting the risks of discrimination and lack of transparency in algorithmic decision-making. By submitting legal opinions, participating in public consultations, and collaborating with other civil society actors, D3 seeks to influence policy outcomes and ensure that digital rights are not sidelined in the rush to adopt new technologies.

D3's advocacy is not limited to the national level. The organisation is an active member of European networks such as EDRi, which amplifies its voice in broader debates about digital governance, data protection, and surveillance at the EU level. Through these alliances, D3 contributes to transnational campaigns, shares expertise, and learns from the experiences of sister organisations across Europe. This networked approach is crucial for smaller organisations operating in countries where digital rights are less established as a public concern. It allows D3 to punch above its weight, leveraging collective action to challenge powerful interests and shape the European digital rights agenda

Public education and awareness-raising are also central to D3's mission. The organisation recognises that legal and policy interventions are only effective if they are supported by an informed and engaged public. To this end, D3 organises workshops, publishes accessible guides, and runs campaigns to demystify issues such as encryption, data protection, and online

surveillance. These efforts are particularly important in Portugal, where digital literacy and awareness of privacy risks have historically lagged behind other European countries. By making complex technical and legal issues understandable, D3 empowers citizens to assert their legal rights and participate in debates about the digital future.

D3's work is shaped by the broader context of surveillance capitalism and the datafication of everyday life. The organisation is acutely aware of the structural asymmetries between individuals and powerful digital platforms, as well as the limitations of regulatory frameworks such as GDPR. D3's advocacy often emphasises the inadequacy of consent-based models of data protection, arguing that real autonomy requires more than the formal ability to click 'accept' on privacy policies. Instead, D3 calls for systemic changes that address the underlying power imbalances in the digital ecosystem, including stronger enforcement of data protection laws, greater transparency in algorithmic systems, and the promotion of privacy-enhancing technologies.

Like many grassroots organisations, D3 faces significant challenges. Resource constraints are a persistent issue as the organisation relies on volunteer labour and limited funding to sustain its activities. The technical complexity of digital rights issues can also make it difficult to engage the broader public or influence policy debates dominated by well-resourced corporate and government actors. Additionally, D3 must navigate the tension between maintaining its grassroots ethos, characterised by independence, flexibility, and community engagement, and the demands of institutionalisation, such as securing funding, building partnerships, and participating in formal policy processes. Despite these obstacles, D3 has achieved notable success. Its interventions have contributed to public debates on controversial issues such as biometric surveillance and data retention, and its participation in European networks has helped to raise the profile of digital rights in Portugal. D3's commitment to transparency, autonomy, and data justice positions it as a key actor in the ongoing struggle to ensure that digital technologies serve the public good rather than narrow commercial or state interests.

D3 thus exemplifies the potential and challenges of grassroots digital rights activism in Europe. Its work demonstrates how small, dedicated organisations can influence policy, raise public awareness, and build transnational alliances in defence of privacy and civil liberties. At the same time, D3's experience highlights the ongoing need for resources, public engagement, and institutional support to sustain grassroots advocacy in an increasingly complex and contested digital landscape. As digital technologies continue to reshape society, organisations like D3 will remain essential to ensuring that fundamental rights are protected and that the digital future is shaped by democratic values.

2.8 Digital Freedom Alliance (Romania), founded in 2004, and Asociația pentru Tehnologie și Internet (Romania), founded in 2002

Digital Freedom Alliance was founded in 2004 as a non-profit dedicated to defending digital rights and strengthening online privacy within Romania. Rooted in legal advocacy and civic engagement, the Alliance seeks to influence national and European digital policy. Its work spans legal interventions, policy analysis, public awareness, and coalition-building, positioning the organisation as a cornerstone of Romanian digital activism. Central to the Alliance's efforts is its collaboration with Asociația pentru Tehnologie și Internet (ApTI), a leading Romanian digital rights NGO. ApTI has consistently contributed to policy debates on data protection, disinformation, and surveillance, including critical analyses of Romania's implementation of the EU Digital Services Act (DSA). In particular, ApTI highlighted shortcomings in DSA implementation, such as excluding NGOs from oversight roles and establishing overly intrusive trust mechanisms, underscoring the Alliance's role within a broader ecosystem of local digital rights advocacy.

Building on this institutional groundwork, the Digital Freedom Alliance has actively responded to emergent threats. In late 2024, Romania appointed 'trusted flagger'-organisations under the DSA to monitor illegal online content. While this aligns with EU transparency goals, critics in public discourse warned that it might tip into censorship without proper safeguards (Kroet, 2024). The Alliance engaged with regulators and public forums to advocate for balanced policies, insisting that content moderation responsibilities can be accompanied by accountability, transparency, and judicial oversight. These efforts reflect the Alliance's approach, where legal strategy is combined with public advocacy. Media outlets reported that Romania's government has escalated efforts to combat online disinformation, particularly in the lead-up to elections, by adopting stricter laws and partnering with platforms like TikTok and Facebook (Deconinck, 2025). Digital Freedom Alliance has positioned itself as a counterweight to emergent overreach, drawing attention to potential abuses, such as non-judicial takedown orders and AI-driven speech filtering, that risk infringing on freedom of expression and privacy. This advocacy echoes research cautioning against relying solely on consent-based data regimes and AI-based enforcement frameworks in democratic contexts.

Academically, the Alliance's work resonates with studies highlighting the limitations of GDPR and DSA. Miller et al. (2024) report that GDPR delivered only modest reductions in third-party tracking, while Puhlmann et al. (2023) call for stronger user-facing privacy tools. By championing institutional reform and public literacy, Digital Freedom Alliance is working to bridge the gap between formal legal protections and meaningful user empowerment. Its advocacy for transparent flagging mechanisms and rights-aware content moderation aligns with calls for privacy-as-participation rather than passive compliance.

Digital Freedom Alliance thus combines ApTI's legal expertise with proactive public engagement to fortify privacy and digital rights in Romania. Its activities, ranging from scrutinising DSA implementation to warning against legislative overreach, position it as a vital actor in maintaining digital freedoms amid evolving European governance frameworks. By simultaneously influencing policy and educating citizens, the Alliance exemplifies a hybrid model of digital advocacy: grounded in law, responsive in practice, and committed to democratic accountability.

2.9 SHARE Foundation (Serbia), founded in 2012

SHARE Foundation was founded in 2012 in Belgrade, Serbia, in response to a growing concern over digital rights in the region. Its origin was linked to a series of conferences on internet culture and activism held in Belgrade and Beirut in 2011–2012, which gathered many people interested in online freedoms. From these gatherings, a community solidified into an organisation with continuous research, monitoring, advocacy, and educational work in the digital environment. Over the past decade, the political framework in Serbia (and more broadly in Southeast Europe) has seen increasing pressure on civic society, concerns about state surveillance, a lag in privacy protections, and sometimes weak enforcement of data protection laws. There is also tension between technological development (smart city projects, biometric surveillance, big data, AI, etc.) and individual rights. SHARE operates in this setting of accelerating technological change, often ahead of regulation, and underdeveloped institutional safeguards. The Serbian government has pursued smart surveillance systems (notably the 'Safe City' project in Belgrade with Huawei), but civil society and regulatory oversight have flagged deficiencies in transparency, lawfulness, and privacy protections.

SHARE Foundation's mission is to defend and advance human rights and freedoms online. Key values include free expression, data privacy, digital security, open access to knowledge, information, and technology, thus emphasising an open, decentralised internet. Ethically, SHARE tries to balance between the public interest (transparency, accountability, preventing misuse of technology) and the rights of individuals (privacy, security, freedom from surveillance). They are attentive to legal standards (e.g. data protection laws) but also focus on empowerment, education, and enabling citizens to exercise their rights. They treat surveillance and biometric technologies with special caution, particularly when implemented without adequate impact assessment or oversight.

In terms of methodology, SHARE uses a multi-pronged set of methods combining research, advocacy, community tools, education, legal monitoring, technical-legal aid, and digital tools. This is evidenced in some of the initiatives SHARE ran:

- *Thousands of Cameras* (#hiljadekamera): Mapping, researching, and advocating around facial recognition, smart surveillance cameras in Belgrade, showing discrepancies between official data and actual deployment. They launched a crowd-mapping portal (https://hiljade.kamera.rs/en/home/), documenting media and other public debates.
- *Privacy Violations Database*: In cooperation with several NGOs, SHARE records cases of privacy violations in Serbia to monitor trends and provide evidence for advocacy.
- *Cybersecurity Toolkit and Personal Data Toolkit*: Providing accessible tools for citizens and organisations to understand security best practices, their rights, assess organisational compliance, and generate privacy policies.
- *Legal Advocacy*: Participating in public debates on draft laws (e.g. personal data protection law), calling for amendments, and working with other civil society actors to press for clarity about when rights can be limited.
- *Networks and Collaborations*: SHARE is a member of European Digital Rights (EDRi), co-founder of SEE Digital Rights Network and operates a civil society CERT (SHARE CERT) to provide pro bono legal and technical assistance to media and civil society in Serbia.

They also engage in public education through workshops, publications, documentaries, online resources, interactive platforms, guidebooks, etc.

Considering their historical development and outreach activities, SHARE Foundation sits at an interesting intersection of grassroots activism and formal institutional structure. Many of its initiatives reflect bottom-up, participatory practices, such as the projects outlined above, which are designed to engage individuals directly. The organisation itself grew out of community gatherings and conferences, and many of its platforms are deliberately accessible to non-experts. These features keep SHARE grounded in citizen experience and reinforce its identity as a grassroots actor.

At the same time, SHARE is a fully registered non-profit organisation with legal and technical experts and policy staff. It is embedded in multiple national and international networks, provides services such as legal and technical assistance through SHARE CERT practices and formal law-making processes, and has been recognised by state authorities, for example, with a certificate of gratitude in 2017 for its contribution to personal data protection. The foundation plays an active role in regional and European civil society networks, including European Digital Rights (EDRi), which allows it to exert influence on a broader scale. This dual nature is both an advantage and a challenge. On the one hand, it gives SHARE legitimacy, access to funding, and the ability to influence policy. On the other hand, it requires constant navigation of tensions: working within legal frameworks that are sometimes weak, pushing for stronger regulation without becoming co-opted by institutional interests, and maintaining the trust of grassroots communities while engaging at the institutional level.

The impact of SHARE's work connects closely to wider debates on surveillance capitalism, creative computing, grassroots ethics, and the tension between privacy and publicness. Its campaigns directly challenge large-scale surveillance projects such as Belgrade's 'Safe City', implemented with Huawei technology and involving biometric cameras, facial recognition, and AI analytics. By exposing the risks, privacy harms, and legal violations, such as the absence of data protection assessments, SHARE positions itself against the uncritical adoption of surveillance infrastructure that is often promoted by powerful corporate and governmental actors. The foundation also demonstrated how digital tools can themselves become instruments of rights protection. Through the development of online platforms such as toolkits, databases, and mapping portals, and through the localisation of interactive games like *Bad News* into Serbian, SHARE employs creative computing not simply as a subject of regulation but as a method of empowerment. These resources give ordinary citizens the ability to understand their rights, make informed decisions, and hold institutions accountable.

Ethically, SHARE places strong emphasis on citizen agency, transparency, dignity, consent, and adherence to legal norms. Public participation is central to their methods, whether through crowd-mapping of surveillance technologies, the reporting of privacy violations or the promotion of awareness. In this way, the foundation not only builds general public capacity but also reaches vulnerable or marginalised groups such as independent media and civic society organisations, which often face heightened risks of surveillance and harassment. A recurring theme in SHARE's work is the delicate balance between publicness and privacy. Many of its campaigns involve revealing what has been hidden, such as surveillance infrastructure and the state's use of new technologies, to demand accountability. At the same time, SHARE seeks to protect individual privacy, promote informed consent, and strengthen oversight. This tension is at the heart of its practice (public accountability requires disclosure, while privacy requires limitation, and SHARE navigates this intersection by exposing systemic issues while also equipping individuals with tools they can use privately). Finally, the organisation faces broader institutional challenges that affect the digital rights landscape. Enforcement of legislation is often weak, while emergency powers invoked for reasons of security or public health, such as during the COVID-19 pandemic, create new avenues for overreach. Meanwhile, the growing influence of global technology companies introduces pressures that are difficult for national regulators to counter effectively. SHARE therefore operates in an environment where technological innovation moves faster than regulation, and much of its work has an anticipatory quality: shaping public norms, raising awareness, and pressing for accountability before harmful practices become entrenched.

2.10 Državljan D – Citizen D (Slovenia), founded in 2015

Zavod Državljan D (Citizen D) is a prominent non-governmental organization based in Ljubljana, Slovenia, dedicated to advancing human rights, media literacy, and active citizenship in the digital age. Founded in 2015 by journalist and digital rights advocate Domen Savič, the NGO was established to combat civic passivity and encourage meaningful public engagement in political and societal processes. Functioning independently of state funding to maintain its objectivity, the organization positions itself at the critical intersection of technology, media, anddemocracy, serving as one of Slovenia's foremost voices on digital human rights.

The organization centers its research and advocacy around four key pillars: privacy and security, copyright, net neutrality, andtech regulation. Through comprehensive investigations andcampaigns, Državljan D tackles some of the most pressing modern digital challenges. This includes scrutinizing biometric surveillance, examining the unchecked expansion of surveillance capitalism, analyzing the societal impacts of artificial intelligence, and combating state-funded disinformation. By investigating how algorithms and "smart city" technologies affect daily life, the NGO strives to hold both corporate and governmental powers accountable, ensuring that technological progress does not erode fundamental freedoms.

Beyond high-level policy advocacy, Državljan D is deeply committed to grassroots empowerment and education, both domestically and across Europe. They actively foster public debate through initiatives like the widely recognized Podcast Državljan D, which features international experts discussing the nuances of the digital economy, media freedom, and tech policy. Additionally, the NGO provides vital media literacy capacity-building and digital security training for journalists, students, andeveryday internet users. By equipping the public with the knowledge and tools to navigate and react to the modern information environment, Državljan D helps cultivate a more informed, resilient, and active democratic society.

Citizen D thereby occupies a space that is distinctly grassroots in orientation, but it has also had to navigate the demands of institutionalisation. On the one hand, its strength lies in informality. This flexibility allows citizen D to experiment with methods, remain responsive to new issues, and cultivate a sense of authenticity that resonates with its audience. On the other hand, sustaining such work over time requires institutional resources. Citizen D has gradually professionalised aspects of its operations, securing project-based funding, building partnerships with other organisations, and participating in transnational networks such as EDRi. This has enabled it to amplify its impact, but also introduced challenges. Institutionalisation brings bureaucratic demands, the need to align with donor priorities, and the risk of diluting the grassroots spirit that defines the initiative. Citizen D has responded to the tension by maintaining a dual strategy:

formal enough to be credible and sustainable, yet informal enough to remain close to its community base.

The organisation's work speaks directly to the theme of surveillance capitalism, grassroots ethics, and creative computing that run through this policy paper. In relation to surveillance capitalism, the initiative consistently criticises how personal data is commodified and exploited by tech companies. Its campaign highlights the structural asymmetries between users and platforms, pointing to the ways in which surveillance has become a default business model in the digital economy. By framing these issues in terms of citizens' rights rather than consumer choice, Citizen D challenges the normalisation of data exploitation and presses for systemic alternatives. This grassroots ethic is evident in its entire approach. Rather than relying solely on legal experts or policy professionals, Citizen D empowers ordinary citizens to become active participants in defending privacy. Its workshops, public campaigns, and creative interventions are designed to demystify technology and to cultivate a sense of agency. In this way, it echoes other grassroots organisations throughout Europe, showing how collective action can counterbalance the inertia of institutions.

Creative computing is another area where Citizen D has made a distinctive contribution. Through its use of art, design, and experimental media, it has shown that privacy can be explored not just in courtrooms and parliaments, but also in galleries, classrooms, and public squares. This creative dimension allows it to reach audiences who might otherwise disengage from the technicalities of privacy law, turning abstract rights into concrete experiences. Finally, Citizen D embodies the broader tension between privacy and publicness that shapes contemporary debates. On the one hand, it uses publicity (through campaigns, exhibitions, and open debates) to expose hidden practices and to mobilise collective resistance. By navigating this tension, Citizen D demonstrates how transparency and privacy are not opposites but interdependent values in the struggle for democratic digital futures.

Citizen D thus illustrates how a small grassroots initiative can have an outsized influence in the field of digital rights. By combining advocacy, creative computing, and community engagement, it has succeeded in raising awareness, building capacity, and challenging both state and corporate practices. Its work underscores the importance of privacy as a public good and a democratic necessity, while also showing how cultural and creative strategies can make digital rights tangible. At the same time, its experience highlights the challenges of balancing grassroots informality with the demands of institutionalisation, a tension faced by many similar initiatives across Europe. Citizen D, then, contributes not only to the Slovenian context but also to the broader European movement for digital rights.

2.11 Open Rights Group (UK), founded in 2005

Open Rights Group (ORG) is a UK-based non-profit organisation that has played a crucial role in shaping the digital privacy landscape in Britain and, by extension, Europe. Founded in 2005 with the aim of defending digital rights, ORG represents a form of institutionalised grassroots activism that retains its community-driven ethos while operating as a professional and influential actor in digital policy. Its work aligns closely with the wider themes articulated in this white paper, particularly the limitations of consent-based data governance (Solove, 2013), and the framing of privacy not merely as an individual right but as a condition of democratic life.

ORG's contribution to online privacy is multifaceted. It is perhaps most visible in its policy advocacy and legal interventions, where it challenges governmental and corporate infringements on privacy rights. A key example is its continued opposition to the UK's Investigatory Powers Act (2016), a legal framework that permits extensive surveillance and data retention by state authorities. ORG had repeatedly challenged these provisions in court, arguing that they violate the principles of necessity, proportionality, and human rights law. More recently, ORG has been a vocal critic of attempts to weaken the UK GDPR through legislative reforms, such as the Data Protection and Digital Information Bill (2024). By actively participating in policy consultations, lobbying lawmakers, and launching strategic litigation, ORG exemplifies what scholars have described as legal engineering in the service of grassroots resistance (e.g. Derickson & Routledge, 2015; Kusiak, 2021). Its efforts mirror the work of organisations like noyb in Austria, turning the law into a technical and political tool for contesting surveillance infrastructures and defending data rights.

Alongside its legal and political work, ORG invests heavily in public education and critical digital literacy. Through campaigns such as 'Fix My Privacy' and 'Stop Watching Us', it translates complex privacy issues into accessible formats that empower individuals to understand their rights and take action. These initiatives often include guides, videos, and interactive tools. ORG's educational outreach reflects a commitment to democratising digital knowledge, encouraging users to move beyond passive compliance towards active engagement with the systems that govern their data. This educational mission is not limited to legal information but extends to the cultivation of digital self-defence, helping users adopt practical privacy-enhancing tools and behaviours in their everyday lives.

ORG's grassroots origins remain evident in its participatory structures and coalition-based activism. It regularly mobilises volunteers, collaborates with allied organisations, and maintains transparency through open communication channels. This participatory ethos reflects what has been described above as prefigurative politics: the enactment of democratic alternatives in the present through bottom-up organising. Events such as cryptoparties, local privacy workshops,

and collaborative campaigns illustrate how ORG sustains its activist roots while engaging with institutional actors. In this way, ORG operates as a bridge between community mobilisation and formal governance structures, translating grassroots concerns into policy influence while remaining accountable to its base. Importantly, ORG has also been a consistent critic of biometric surveillance, AI-based profiling, and opaque data-sharing agreements between the public and private sectors. It has raised alarms about the use of facial recognition technologies by police, the integration of surveillance tools into public services, and the potential erosion of civil liberties under the guise of national security or technological innovation. These interventions align closely with the sociotechnical understanding of privacy articulated in this document, which emphasises the entanglement of technical systems with institutional norms, economic incentives, and social power. ORG's work thus underscores the need to situate privacy within broader struggles over transparency, accountability, and democratic governance.

While ORG may not focus on creative computing or artistic interventions, it contributes significantly to the landscape of privacy activism through legal pressure, policy engagement, and public education. It does not merely respond to existing regulations but actively shapes the normative and legal frameworks that define digital rights in the UK. In this sense, ORG represents a hybrid model of grassroots activism and institutional advocacy – an actor that both criticises and participates in the mechanisms of governance. Its work complements other grassroots efforts across Europe by providing a rigorous legal foundation for privacy rights, highlighting the importance of enforcement and institutional coherence in an age of surveillance capitalism.

ORG thus demonstrates how grassroots initiatives can evolve into a sustained force for privacy advocacy without losing its ethical commitments or community orientation. Through legal activism, public education, and sustained policy engagement, it advances a vision of privacy as a collective right and a cornerstone of democratic life.

2.12 Privacy International (UK), founded in 1990

Founded in 1990 and based in the UK, Privacy International (PI) is one of the oldest and most influential organisations in the global digital rights landscape. Its longevity and scope make it a unique case within the European context, especially when viewed through the lens of grassroots privacy activism, surveillance capitalism, and creative resistance. While PI operates with a high degree of institutionalisation, its ethos remains rooted in the defence of civil liberties, transparency, and autonomy in the digital age. The organisation's work exemplifies many of the ethical principles central to data privacy, including informed consent, data justice, and the right to opacity. PI's mission is to challenge government surveillance and promote the right to privacy across legal, technological, and social domains. It does so through the combination of litigation, policy advocacy, investigative research, and public education. This multi-pronged approach

reflects the sociotechnical understanding of privacy: privacy is not merely a legal or technical issue but a deeply embedded concern within broader systems of power, infrastructure, and ideology.

One of PI's most notable contributions is its strategic litigation against unlawful surveillance practices. The organisation has brought cases before national and international courts, including the European Court of Human Rights and the UK's Investigatory Power Tribunal. These legal interventions have challenged mass surveillance programmes, data retention laws, and the use of bulk interception powers by intelligence agencies. In doing so, PI has helped establish legal precedents that reinforce privacy as a fundamental right and expose the inadequacies of consent-based models in the face of systemic surveillance. This aligns with the criticism that informed consent often fails to protect users when surveillance is embedded in the very architecture of digital systems. PI's legal activism also reflects the concept of privacy by design; rather than relying solely on reactive enforcement, PI advocates for structural changes in how technologies are built and governed. For example, its work on data protection in humanitarian contexts has led to the development of ethical guidelines for NGOs and international organisations, ensuring that vulnerable populations are not subjected to exploitative data practices. This emphasis on protecting the most marginalised echoes the principle of data justice, which calls for fairness and accountability in how data is collected, analysed, and applied.

In addition to litigation, PI engages in investigative research that reveals the hidden mechanisms of surveillance capitalism. Its reports on data brokers, mobile phone tracking, and spyware technologies have exposed how private companies profit from the commodification of personal data. These investigations resonate with Zuboff's (2019) concept of behavioural surplus, where data extracted beyond what is necessary for service provision becomes a source of commercial value. PI's work in this area not only informs public debate but also pressures regulators to act, contributing to the broader ecosystem of privacy advocacy in Europe. PI also plays a key role in public education and digital literacy. Through accessible publications, toolkits, and campaigns, it helps individuals understand their rights and adopt privacy-enhancing technologies. This is linked to creative computing and participatory design practices (approaches that empower users to shape the digital environments they inhabit). While PI may not engage in artistic interventions like Tactical Tech's 'Glass Room', its educational materials serve a similar purpose: making abstract privacy concerns tangible and actionable for everyday users.

The organisation's commitment to relational ethics is evident in its collaborative approach. PI works closely with partner organisations around the world, sharing resources, expertise, and strategies. This creates a sense of mutual responsibility and trust within the digital rights community, reinforcing the idea that privacy is not just an individual concern but a collective condition for democratic life. Its partnerships with groups in the Global South also reflect a commitment to data justice on a global scale, recognising that surveillance and data exploitation

often disproportionately affect marginalised communities. PI's advocacy for the right to opacity is particularly relevant in the context of algorithmic decision-making. The organisation has consistently called for transparency in how algorithms are used by governments and corporations, especially in areas such as welfare distribution, policing, and border control. It argues that individuals should not be fully legible to systems that make consequential decisions about their lives, and that some degree of unreadability is essential to preserving autonomy and dignity.

Despite its institutional maturity, PI maintains a critical stance towards both state and corporate actors. It does not seek co-optation but rather insists on accountability, transparency, and the primacy of human rights. This positioning allows it to act as a watchdog and a catalyst for change, bridging the gap between grassroots concerns and formal governance structures. Its work complements other European initiatives by providing legal rigour, investigative depth, and global reach. PI thereby exemplifies how a well-established organisation can retain its grassroots ethos while operating within institutional frameworks. By combining litigation, research, education, and coalition-building, PI contributes to a more just and democratic digital society – one where privacy is not a privilege but a right, and where surveillance is challenged not only in courtrooms but in public discourse and everyday practice.

2.13 Privacy Issues as a Wikipedia Contributor

Wikipedia, as one of the largest and most influential grassroots digital platforms, offers a unique lens through which to examine the intersection of privacy, representation, and digital participation. While its open-source ethos and collaborative models have enabled widespread access to knowledge, the platform also reveals persistent structural inequalities, particularly in relation to gender, identity, and online safety. This case study explores how privacy concerns manifest for contributors to Wikipedia, with a focus on the experiences of women, and how these dynamics reflect broader tensions in grassroots digital movements. Despite democratic aspirations, Wikipedia has long faced criticism for its lack of diversity among contributors. Women in particular remain significantly underrepresented, both in terms of editorial participation and in the content of articles themselves. This reflects deeper systemic biases in archival practices, publishing, and cultural recognition. The underrepresentation of women and minorities not only limits the scope of collective knowledge but also raises critical questions about privacy, safety, and visibility in open digital environments.

The process of creating a Wikipedia account illustrates how privacy and identity are negotiated from the outside. For male contributors, and especially young white men, the Wikipedia

recommendation is to use usernames that reflect their real names or personal identifiers. In communities such as 'Young Wikipedians', boys are often encouraged to include their birth year, creating a traceable digital identity that can be linked to their contributions over time. This visibility is framed as a marker of reputation and engagement. In contrast, female contributors are frequently advised to obscure their identities. Due to the heightened risks of harassment and surveillance, women are encouraged to adopt usernames that conceal gender and personal details. This strategy reflects a broader pattern of defensive anonymity, where invisibility becomes a form of protection. The choice of username thus becomes a political act, one that balances the desire for participation with the need for safety. The parallels with literary history are striking; just as women once adopted male pseudonyms to publish their work, many female Wikipedians now use gender-neutral or male usernames to avoid bias and scrutiny. The platform's default settings further reinforce gendered assumptions. Upon account creation, the system automatically assigns a male identity unless manually changed. This extra step, required only for female and gender-diverse users, signals a normative bias in the platform's design, where maleness is treated as the default. Such design choices contribute to a broader culture in which female presence is rendered exceptional rather than normative.

Privacy concerns extend beyond identity to the content of contributions. Articles about living individuals are governed by strict guidelines, including the 'Presumption in Favour of Privacy'-policy. However, the risks associated with public exposure are not evenly distributed. Women often face greater vulnerability when personal details are published, particularly if they lack institutional support or public recognition. For individuals in precarious situations or from marginalised communities, the consequences of visibility can be severe, ranging from reputational harm to real-world harassment. The technical architecture of Wikipedia also presents challenges. Until recently, IP addresses of anonymous contributors were publicly visible, exposing users to potential tracking and profiling. Even registered users, while protected by pseudonyms, leave behind detailed edit histories that can be scrutinised by others. The platform's transparency, while essential to its collaborative ethos, can inadvertently compromise user privacy, especially when contributors meet offline or engage in public events where usernames are linked to real identities.

Stalking and harassment are documented issues within the Wikipedia community. Contributors have reported being followed online, having their edits monitored, and receiving unsolicited messages. In some cases, this surveillance escalates into offline threats, with users' personal information being uncovered and used to intimidate or harm. While the platform offers mechanisms for reporting abuse, such as flagging violations or contacting administrators, these processes are often informal, volunteer-driven, and difficult to navigate. The global steward system, which oversees serious cases, consists of only a few dozen individuals responsible for managing disputes across the entire platform. These dynamics highlight a critical tension in open

source environments: openness does not automatically guarantee equity or safety. The assumption that transparency fosters trust must be balanced against the reality that visibility can expose contributors to harm. As such, privacy must be understood as a technical safeguard and as a condition for meaningful participation, especially for those whose identities place them at greater risk.

The Wikipedia case underscores the need for more inclusive and privacy-conscious design in grassroots digital platforms. It calls for a rethinking of default settings, identity management, and content governance to ensure that all contributors, regardless of gender, background, or status, can participate safely and equitably. It also invites reflection on the broader implications of visibility in digital spaces, where the line between public contribution and personal exposure is increasingly blurred. In this sense, Wikipedia exemplifies the promise and the pitfalls of grassroots digital participation. Its open model has enabled unprecedented collaboration, but its structural biases and privacy challenges reveal the limits of neutrality in practice. Addressing these issues requires not only technical fixes but a deeper commitment to relational ethics, inclusive governance, and the recognition that privacy is a collective right, essential to the flourishing of diverse voices in the digital commons.

IV. Ethical Approaches to Grassroots Online Privacy Activism

Ethical approaches to online privacy understand privacy not just as a set of technical safeguards but as a deeply social concern. Ethics, in this context, refers to the system of moral principles that govern the behaviour of individuals and organisations when dealing with personal information. At the grassroots level, privacy is about more than complying with laws; it is about protecting human dignity, supporting freedom of expression, and enabling individuals to live without fear of surveillance or manipulation (van der Sloot, 2014). However, what seems like a basic human right from the bottom up might seem like a potential cyber-threat or security issue from the perspective of governments.

In the digital era, the ethics of privacy intersect with power, inequality, and technological control. Every online action, from browsing a website to sharing a photo, generates data that can be tracked, stored, analysed, and even sold. While this data can be used to improve services, it is often exploited for profit without the user's knowledge or consent. Ethical grassroots approaches challenge this imbalance by promoting transparency, equity, and agency. These movements emphasise that ethical considerations must be at the core of digital design, not an afterthought. They argue that privacy is not only a personal right but also a collective condition for democratic life and social participation.

By embedding ethical thinking into digital activism, grassroots initiatives create new models of accountability and care in the digital space. They recognise the need to protect the most vulnerable members of society from the disproportionate harms of surveillance and data misuse, while creating inclusive digital environments based on mutual trust, respect, and shared responsibility.

1. Key Ethical Principles and Community-Centred Design

Grassroots privacy ethics rest on foundational principles drawn from philosophical and sociotechnical scholarship. For instance, contextual integrity, as introduced by Nissenbaum (2009), reframes privacy not as secrecy but as the appropriate flow of information. Taylor (2017) broadens this to data justice, underscoring systemic inequities in how data is produced, used, and governed. The key ethical principles are therefore:

> *Autonomy:* This means the right of individuals to make decisions for themselves, including control over how their data is collected, shared, and used. Ethical privacy practices give

people real choices and understanding, rather than burying consent in legal jargon (Pugh 2020, Chapter 6). A key example is the Montgomery Judgement in the UK (Montgomery v. Lanarkshire Health Board, 2015), which redefined the legal standard for medical disclosure. It ruled that doctors must ensure patients understand material risks relevant to their personal circumstances, not just what a reasonable doctor would disclose. This empowers patients to make decisions based on their own values and understandings rather than being passively guided by medical authority.

Informed Consent: People should agree to data use only after having been informed of what is being collected and for what purpose. Grassroots organisations argue that current digital systems often provide the illusion of choice, with long and complex privacy policies and confusing opt-out mechanisms (Pugh 2020, Chapter 6). A study conducted in Germany by researchers at Ruhr-Universität Bochum revealed that most GDPR cookie consent notices fail to provide truly informed consent. Analysing over 80,000 user interactions, they found that many websites used nudging techniques and overwhelming choice structures that pushed users to accept tracking without understanding the implications. Notices often lacked clarity, used technical jargon or buried options deep in menus. This led users to click dismissively rather than engage meaningfully, undermining GDPR's intent to empower users with transparent, informed choices.

Data Justice: This principle emphasises fairness in how data is collected, analysed, and applied. It involves protecting vulnerable populations from discriminatory algorithms and ensuring everyone has equal protection and representation in digital systems (Taylor, 2017). An example of data justice is the proposed Digital Fairness Act (DFA; European Commission, 17 July 2025). This initiative aims to regulate manipulative algorithmic design, such as autoplay and infinite scroll, that disproportionately affects vulnerable groups, especially adolescents. The DFA seeks to embed protections directly into digital platforms by banning 'dark patterns', enforcing ethical defaults, and promoting fair personalisation. It shifts responsibility from users to platforms, ensuring that digital environments do not exploit psychological vulnerabilities. This reflects a commitment to fairness, representation, and protection in algorithmic systems.

Contextual Integrity: Introduced by Helen Nissenbaum (2011), this concept states that privacy should not be about hiding information, but about ensuring that personal data is shared appropriately depending on the context (such as a doctor-patient conversation versus a public tweet). An example is the controversy surrounding the digitalisation of public records, such as court documents, in countries like Germany and the UK. Traditionally, these records were accessible only in person, preserving a level of privacy through practical obscurity. However, once digitised and placed online, they became

searchable and widely accessible, violating the contextual norms under which the data was originally shared. This shift disregards the social context of legal confidentiality and illustrates how privacy breaches can occur even without exposing sensitive data, simply by changing the context of access.

Grassroots initiatives often emphasise community over the individual. This positions privacy as a social and not just a personal issue, emphasising the following:

Participatory Design: People who use a technology should help design it. Grassroots efforts involve the public in creating tools that reflect their values and concerns (Shilton, 2012). A classic example of participatory design is the UTOPIA project in Sweden and Denmark during the 1980s. In this project, newspaper typographers worked directly with researchers and designers to develop new graphics software tailored to their needs rather than having technology imposed on them. The aim was to empower workers and ensure the resulting tools reflected their values and expertise. This approach has since influenced participatory technology design across Europe, emphasising democracy, inclusion, and grassroots involvement in shaping digital systems.

Privacy as a Commons: Like clean air or safe drinking water, privacy should be seen as a default framework available to anyone. A leading example of privacy as a commons is the DECODE project in Barcelona, which empowers citizens and communities to control how their personal data is shared and used. Instead of relying on corporations, DECODE uses decentralised, open-source technology to let people collectively manage data for public benefit, such as urban planning or community services, while keeping privacy as a shared, default right. This approach treats privacy like clean air: a public good that everyone should enjoy and help protect.

2. The Ethics of Resistance to Surveillance Capitalism

Grassroots initiatives challenge the surveillance capitalism model, in which user data is systematically extracted and monetised by large technology platforms. One of the earliest and most influential examples of surveillance capitalism can be traced to Google's strategic shift in 2000 (Curran, 2023). Initially conceived as a user-focused search engine, Google pivoted to an advertising-based revenue model that monetised user data at scale. By leveraging the vast amounts of behavioural data generated through search queries, Google began offering targeted advertising services to third-party clients. This marked a foundational moment in the

development of surveillance capitalism, wherein user data (often collected without explicit informed consent) became a key economic asset.

Google's model thus redefined the economics of the internet and established the precedent for extracting predictive insights from personal data to drive advertising revenue, setting a template subsequently adopted across the digital economy. Actors within surveillance capitalism thus reveal unethical practices, such as deceptive consent interfaces and algorithmic manipulation, while simultaneously building alternative systems that prioritise user rights and transparency, pushing back against the normalisation of surveillance. These communities expose how our choices are shaped and restricted, and offer new models of what ethical technology could look like by doing the following:

> *Expose deceptive consent models*: Many digital platforms use design tricks, like pre-checked boxes or dark patterns, to push users into agreeing to share their data. Activists work to uncover and challenge these practices. A well-documented real-life example involves Google's Location History settings. In 2018, an investigation by the *Associated Press* revealed that Google continued to track users' locations even when they had turned off 'Location History' in their account settings. The option that actually stopped location tracking ('Web & App Activity') was buried in a separate menu and enabled by default, misleading users into thinking they had opted out. This prompted lawsuits and regulatory scrutiny, with critics arguing that Google used deceptive interface design to secure consent without users' full understanding, undermining their ability to make informed choices about their personal data (European Consumer Organisation, June 2018).
>
> *Reveal bias in data systems*: Algorithms used for job screening, policing, or loan approvals can discriminate against women, minorities, or the poor. Ethical grassroots initiatives raise awareness and campaign for fairness in these systems.

Projects like Tactical Tech (2023) and Alternatif Bilişim (2023) go beyond raising alarms about data misuse. They equip users with practical knowledge and tools, such as the Data Detox Kit or open-source privacy platforms, and run participatory workshops that turn ethical principles into day-to-day practices. They engage communities in hands-on learning, offering tools, resources, and alternatives that make digital ethics tangible and actionable. These examples demonstrate the power of grounded, community-centred action.

In addition to creating new tools, grassroots actors assert the right to reject systems that are unethical:

> *Right to Opacity:* This is the idea that people should be allowed to remain partially unknown or unreadable by algorithms and institutions. Not everything should be

analysed or predicted. An example is the debate over algorithmic decision-making in criminal justice. In several EU countries, algorithms are used to assess risks or recommend sentences, but their inner workings are often kept secret, creating algorithmic opacity. Legal scholars and grassroots activists argue that individuals should have the right not to be fully analysed or predicted by such systems, especially when the logic is hidden or potentially biased. This principle is being discussed in EU policy circles as a way to protect people from excessive surveillance and automated profiling.

Ethical Refusal: Some projects deliberately design systems that collect minimal data, or none at all. This is a form of resistance to the idea that data collection is always necessary. An example is the practice of designing digital services that deliberately avoid collecting unnecessary personal data. For instance, some public sector apps in the EU, such as certain COVID-19 contact tracing apps, were built to function without tracking users' locations or identities, using only anonymised, minimal data. This approach resists the assumption that more data is always better, prioritising privacy by default and demonstrating that effective technology can be built without extensive surveillance or profiling.

Legal frameworks like GDPR offer some protection, but grassroots ethics go further with the following:

Prefigurative Politics: This means living out the change you want to see. Grassroots tech groups do not wait for governments (they build systems today that reflect their ethical ideals). An example is the work of grassroots tech collective Social Tech Lab in Amsterdam. Instead of waiting for government regulation, they co-created digital platforms, such as community-run social networks and open-source mapping tools that embody values of privacy, transparency, and democratic control.

Relational Ethics: These emphasise trust and responsibility within communities. For example, free software groups often share their code openly so others can check that it is not doing anything harmful. An example is the practice of open-source software communities, such as those behind the Linux operating system or the Nextcloud project. These groups share their code publicly, allowing anyone to inspect, audit, and improve it. This openness builds trust and accountability within the community, as members take responsibility for ensuring the software is safe and respects users' rights. By making their work transparent, they foster ethical relationships based on mutual respect and collective responsibility.

3. AI and the Ethics of Privacy Activism

AI is reshaping the ethical landscape of grassroots online privacy activism, offering both new opportunities and profound challenges. On one hand, AI technologies equip grassroots initiatives with advanced tools for resistance, enabling activists to detect surveillance patterns, automate privacy safeguards, and analyse digital threats in real time. AI-powered privacy bots, for instance, can scan websites for invasive trackers and notify users of potential data breaches. This aligns closely with the ethical principles of autonomy and informed consent by helping individuals understand and manage their exposure to algorithmic surveillance (Cavoukian, 2009; Taylor, 2017). AI-driven innovations also enable participatory and decentralised models of privacy protection, allowing communities to co-create intelligent privacy tools that reflect local needs and values.

However, the integration of AI into grassroots privacy work also raises significant ethical concerns. Many of the same technologies that activists use to protect users are derived from systems originally built for surveillance and data extraction, raising the risk of ethical contradiction or co-optation. For example, machine learning algorithms used to anonymise data or detect bias must themselves be carefully scrutinised for hidden biases or opaque decision-making processes (Nissenbaum, 2009; Dwork, 2006). Moreover, AI systems require large datasets to function effectively, which may tempt even well-meaning actors to collect more user data than is ethically justified. This tension underscores the need for a robust ethical framework that critically examines not only the use of AI but also its design, assumptions, and long-term implications. Grassroots actors must therefore balance innovation with caution, embracing AI's benefits while resisting its embedded risks and reinforcing the right to opacity and ethical refusal.

In this context, ethical activism involves more than deploying tools; it requires interrogating the values and power dynamics embedded in the tools themselves. AI must not become a black box for privacy activism but rather a site of democratic accountability and collective reflection. As grassroots groups begin to integrate AI into their strategies, they are also expanding their ethical commitments, from resisting surveillance capitalism to actively reimagining how intelligence and autonomy can coexist in digital systems shaped by care, consent, and justice (Souza, 2025).

4. Machine Unlearning and the Future of Data Privacy

Machine learning systems are now deeply embedded in nearly every aspect of our daily lives, powering personalised recommendations, voice assistants, credit-scoring tools, medical-diagnosis platforms, and autonomous vehicles. Once data is used to train a model, it becomes intrinsically woven into its parameters and behaviour, making targeted removal of specific information extraordinarily difficult. This enduring data persistence conflicts directly with legal

mandates such as the EU's GDPR, which grants individuals a right to erasure. Machine unlearning (MU) has thus emerged as an essential technique for ensuring that models can comply with privacy regulations, behave as if certain data were never ingested, and adapt to dynamic consent withdrawals or obsolete training inputs.

4.1 Embedding 'Forgetting by Design' into AI Systems

From the moment an AI system is conceived, privacy-by-design principles must guide its architecture. In traditional workflows, retraining a model from scratch after every erasure request is impractical; full retraining carries enormous computational and environmental costs and introduces potential divergence due to the stochastic nature of deep network optimisation. MU reframes this lifecycle by integrating checkpoints and modular structures so that forgetting specific records becomes an update rather than a rebuild. In recommender systems, for example, replacing or retraining only the modular block corresponding to the removed user yields precise 'forgetting' without disrupting the entire embedding space. In large language models, smart adjustments (such as rolling back to stored fitting checkpoints or applying inverse preference gradients) can erase targeted information while preserving general utility.

4.2 Techniques for Selective Data Removal

Three families of MU techniques have proven most promising. The first, data-slice retraining and gradient adjustments, exploits influence functions to estimate each training example's effect on model parameters. By approximating the gradient changes caused by upweighting or removing a point, practitioners can avoid full retraining. While Koh and Liang (2017) laid the foundational theory, Zhang et al. (2023) recently demonstrated a recommendation-unlearning framework that achieves over 250× speedups compared with retraining, preserving output fidelity in large-scale settings.

The second approach, model perturbation, directly modifies weights. Tiny, carefully calibrated noise injections or targeted gradient ascent operations eliminate data traces without accessing raw inputs. Thudi et al. (2021) formalised statistical guarantees for such perturbations, bounding the residual influence of forgotten records. More advanced frameworks combine noise injection with self-distillation (masking outputs related to the forget set and then retraining the model to 'fill in' consistent behaviour), thereby delivering both practical efficiency and certifiable privacy bounds in certain architectures.

Finally, modular and ensemble architectures construct models as collections of semi-independent experts, each trained on disjoint data subsets. Deleting the module responsible for a given subset severs the model's memory of that data. Fan et al. (2023) survey these designs,

showing that block modularity supports rapid unlearning in federated settings with minimal collateral forgetting. Menik and Ramaswamy (2023) extend this concept to large language models by partitioning transformer layers into concept-aligned regions, enabling precise 'surgical' edits without full-scale retraining.

4.3 Legal Imperatives and Verification Challenges

The mandate to erase personal data derives from Article 17 of the GDPR, which obliges data controllers to remove personal records upon request, revoke consent or when the data is no longer necessary (European Union, 2018). Unlike simple database deletion, MU must ensure that no residual statistical influence from the erased data persists in the model. Exact unlearning theoretically satisfies this requirement by retraining the model from scratch on the reduced dataset, but it is computationally prohibitive for modern, large-scale networks (Cao & Yang, 2015; Sekhari et al., 2024). Consequently, approximate unlearning techniques have emerged as a pragmatic compromise, striking a balance between efficient execution and bounded residual influence (Chaudhuri et al., 2023; Chien et al., 2024).

Regulators and auditors increasingly demand transparent evidence of compliance rather than opaque retrospective claims. Membership-inference-based certification methods address this demand by operationalising residual influence bounds; if an adversary's success in inferring whether a target record was used in training drops to random-chance levels post-unlearning, the model can be deemed effectively 'clean' of that data (Gu et al., 2024; Tran et al., 2025). This approach draws on differential privacy metrics to quantify the maximal information leakage attributable to the erased samples (Dwork et al., 2006; Chaudhuri et al., 2023).

However, verification remains hindered by several intertwined technical challenges. First, stochastic training dynamics thwart deterministic equivalence tests: random weight initialisation and the non-convex optimisation landscape mean that two retrainings on identical datasets can yield diverging parameter configurations and decision boundaries, complicating direct comparisons of pre- and post-unlearning models (Sekhari et al., 2024; Chien et al., 2024). Second, incremental learning loops further inflate complexity. Online services ingest and purge records continuously, so MU methods must support real-time additions and deletions without resorting to full retraining, a requirement that current incremental unlearning frameworks only nascently address (Lee & Kim, 2024; Nguyen et al., 2022). Third, there is a verification deficit: while membership-inference certification offers a statistical criterion, it does not yield formal cryptographic proofs of forgetting, leaving a gap between empirical confidence and legal assurance (Gu et al., 2024; Sekhari et al., 2024).

Standardising unlearning metrics will be essential for uniform regulatory assessment. Proposed benchmarks include specifying maximum allowable membership-inference gains (e.g. ≤1% above random chance) and calibrating noise levels in perturbation-based methods using Rényi differential privacy parameters (Chaudhuri et al., 2023; Chien et al., 2024). Establishing such noise-calibrated deletion certificates and verification protocols will empower auditors to validate compliance without requiring access to proprietary training data or model internals.

4.4 Balancing Privacy and Performance

Selective forgetting inevitably introduces trade-offs between privacy guarantees and model utility. Over-zealous perturbations risk catastrophic utility drops on downstream tasks (Thudi et al., 2021; Zhang et al., 2024). Removing entire modules may leave blind spots if those modules capture overlapping functionalities. Conversely, influence-function methods deliver high-fidelity unlearning but scale poorly when faced with numerous deletion requests (Koh & Liang, 2017; Zhang et al., 2023). Consequently, MU strategies must calibrate forgetting intensity against performance degradation. Retention-based masking techniques (where parameters critical to retained data are frozen during unlearning) offer one promising avenue, enabling models to preserve core capabilities while purging peripheral traces (Ding et al., 2025).

4.5 Policy Implications for a Human-Centred AI Ecosystem

To embed MU as a standard feature of trustworthy AI, policymakers should mandate privacy-by-design and unlearning attestation in procurement and certification regimes. Funding programmes such as Horizon Europe and Digital Europe can designate open-source MU libraries as critical infrastructure, lowering barriers for small and medium-sized enterprises (SMEs) to comply without prohibitive retraining costs. A dedicated European Unlearning Office could codify standardised attestation reports, akin to energy-efficiency labels, that quantify residual influence metrics under agreed thresholds.

Importantly, regulations must account for resource equity. Exact unlearning privileges well-resourced firms; public investments in shared MU toolkits will democratise compliance and prevent monopolistic entrenchment (Nguyen et al., 2022; Fan et al., 2023). Lifecycle governance should treat AI models as mutable artifacts, requiring procurement contracts to budget compute and energy for periodic unlearning cycles, harmonising sustainability goals with dynamic privacy safeguards. Human oversight must be explicit: because perfect forgetting is unattainable, data subjects need accessible redress mechanisms when MU fails, complemented by ongoing audits and transparency dashboards co-designed with grassroots communities (Gu et al., 2024; Tran et al., 2025).

4.6 Recommendations for Researchers, Practitioners, and Grassroots Actors

Researchers should advance approximate unlearning methods with provable privacy guarantees, exploring hybrid schemes that combine perturbation with modular retraining across varied architectures (Thudi et al., 2021; Zhang et al., 2024). Practitioners must integrate MU hooks, such as gradient-tracking checkpoints and modular partitioning, early in model development. Providers of foundational AI stacks can include unlearning Application Programming Interfaces (APIs) to simplify client-triggered erasure workflows.

Grassroots groups, hackerspaces, and civic tech hubs should incorporate MU concepts into privacy-enhancing workshops alongside established tools like Tor or Signal. Visual dashboards that display unlearning status and residual risk in an accessible language can build public trust.

Machine unlearning bridges cutting-edge AI capabilities with fundamental data-protection rights, transforming models from immutable data sponges into responsive, accountable infrastructures. By aligning technical innovations such as influence-based retraining, noise-calibrated perturbations, and modular architectures with the normative imperatives of GDPR and beyond, MU charts a path toward AI systems that can forget on demand. Realising this vision demands multidisciplinary collaboration (among engineers, legal scholars, ethicists, and policymakers) and sustained support for open, community-driven MU ecosystems. In doing so, forgetting by design will join accuracy and efficiency as a pillar of trustworthy AI, ensuring that the digital future honours both innovation and individual rights.

5. Conclusion

Grassroots ethical approaches treat privacy not as a luxury but as a necessity for a free and democratic society. In a world increasingly shaped by data extraction and digital profiling, these initiatives emphasise the moral obligation to safeguard personal dignity, autonomy, and social equity. By focusing on transparency, fairness, and community participation, they provide a powerful alternative to the top-down models of digital regulation.

These ethical strategies go beyond individual protections and address the structural conditions of digital injustice. They foster solidarity, build trust within communities, and encourage civic engagement. Importantly, they promote a new vision of digital life, one where respect for human rights is embedded in the design and governance of technology. In doing so, grassroots actors not only defend privacy but also actively shape the ethical foundations of future digital societies.

V. Technical Approaches to Grassroots Online Privacy Protections

Technology is both the problem and the solution when it comes to online privacy. While digital platforms can collect massive amounts of data on users, they can also offer tools that protect and empower individuals. Grassroots communities across Europe are using a range of technical approaches to resist surveillance and promote ethical data practices. These tools are part of what experts call ***Privacy-Enhancing Technologies (PETs)***.

The technical dimension of privacy involves not just software or code, but also infrastructure, interfaces, and systems design. For grassroots groups, using technology is not only about defence; it is also about empowerment, education, and collective action. These groups harness open-source tools, create alternative infrastructures, and teach people how to reclaim control over their digital lives. Technical privacy work at the grassroots level is fundamentally creative, adapting advanced tools for everyday users and ensuring they remain accessible to people regardless of technical skill or resources.

By focusing on user-friendly, decentralised, and transparent technologies, grassroots initiatives show that privacy can be built into the digital fabric of our communities. Their work offers both practical tools and visionary alternatives to surveillance capitalism, demonstrating that ethical, secure, and human-centred technology is not just possible, but already being created and used by communities across Europe.

1. Core Privacy-Enhancing Technologies - Tools and Techniques

Privacy-enhancing technologies (PETs) are designed to give users control over their personal data while enabling them to participate in digital spaces. These technologies take many forms: some are built deep into system architectures, others are simple browser plugins. What unites them is their aim to protect individuals and communities from intrusive data practices. PETs are tools and methods designed to protect personal information and reduce the risk of surveillance, data breaches, and identity theft. These include:

- *Hard PETs:* These are built into the infrastructure of systems and include tools like encryption, anonymisation, and decentralised architectures.
- *Soft PETs*: These improve usability and include features like clear privacy settings, opt-out mechanisms, and user-friendly interfaces.

The goal is to make privacy easy, accessible, and automatic for everyday users. As Dwork (2006) and Nissenbaum (2009) have shown, PETs are most effective when adapted to local contexts and paired with ethical commitments. Grassroots movements integrate these technologies (such as encryption, anonymisation, and decentralised networks) into public education and civic infrastructures to create a holistic approach to digital empowerment. This section explains commonly used PETs by grassroots communities, with simplified definitions and real-world examples to help ordinary users understand their purpose and usage. ***Encryption*** is a method of secure communication which protects information by converting it into unreadable code that can only be accessed with a secret key or password. This ensures that even if a message or file is intercepted, it cannot be understood without a specific key or password. One of the most secure forms of this method is ***End-to-End Encryption (E2EE)***. With E2EE, a message is encrypted on the sender's device and only decrypted on the recipient's device. No third party, not even the service provider, can access the content during transmission.

Applications such as *Signal* and *Matrix* implement E2EE to safeguard user communications. These tools are frequently used by individuals who require a high level of privacy, including journalists and activists. Organisations like Tactical Tech support the use of such tools by offering step-by-step tutorials on how to install and use them securely.

Use Case: Encrypted Communications for Whistleblower Protection

A human-rights NGO in Slovakia uses **Signal** to coordinate meetings and exchange sensitive documents with whistleblowers. By enabling end-to-end encryption (E2EE), no third party can access message content. With support from Tactical Tech, the NGO hosts community cryptoparties to teach encryption basics, key verification, and secure storage practices. This protects both senders and recipients from interception or impersonation.

Anonymisation and ***Pseudonymisation*** are two important strategies used to protect personal data while still allowing it to be useful for analysis or decision-making.

Anonymisation involves permanently stripping away all personally identifiable details from a dataset. Once anonymised, the information can no longer be linked to any specific individual. This approach is particularly valuable for researchers, public institutions, and organisations that need to work with data while fully respecting individual privacy.

Pseudonymisation, on the other hand, replaces sensitive identifiers (such as names, addresses, or ID numbers) with artificial labels or codes. While the connection to an individual is hidden, it can still be restored under certain conditions if necessary. This method allows data to be used in a more flexible way, striking a balance between privacy and functionality.

Use Case: Anonymous Civic Participation via DECODE Project

In Barcelona, citizens contribute to environmental data collection through an app developed under the **DECODE** project. Their identities are protected using pseudonymisation: each user receives a randomised ID. This allows individuals to report issues like noise pollution or air quality without risking exposure, while still allowing meaningful city-wide analysis.

Differential Privacy is a powerful data protection method that ensures individual privacy is maintained, even when large datasets are analysed. The technique works by introducing small, random alterations (referred to as 'noise') into the data. These subtle changes make it impossible to determine whether any one person's information is part of the dataset, thus shielding individual identities while still allowing meaningful insights to emerge. This approach enables organisations to identify broad trends, such as how many residents in a city commute by bicycle, without exposing the behaviour of any specific person. It strikes a delicate balance between data utility and personal privacy.

Major technology companies like *Apple* and *Google* have incorporated differential privacy into their analytics tools to enhance user protection. At the grassroots level, community organisations also rely on this technique when gathering sensitive data, such as neighborhood energy consumption, ensuring that individual households remain untraceable while still contributing to a larger understanding of local needs.

Use Case: Differential Privacy in Community Surveys

A community research team in Ljubljana runs a digital access survey. To maintain respondent privacy, they introduce small randomised noise into the data before releasing the results. Using **differential privacy**, individuals cannot be re-identified from aggregate findings, yet the results still inform infrastructure planning and policy.

Decentralised architectures are reshaping the way data is processed and analysed, offering new ways to protect privacy while enabling powerful collaboration. One such method is ***Federated Learning***, which allows artificial intelligence models to be trained directly on users' devices, such as smartphones, without transferring any personal data to a central server. Each device contributes to improving the model by learning locally and sharing only insights, not raw data. This means a person's phone can help make an app smarter, all while their personal information stays private and never leaves their device.

Another innovative approach is ***Secure Multiparty Computation (SMPC)***. In this technique, several individuals or computers collaborate to analyse data, but none of them has access to the

full dataset. It is similar to piecing together a puzzle, where each participant only holds a fragment of the picture, ensuring that the complete information remains confidential.

Use Case: Ethical AI with Federated Learning and SMPC

A maternal health app in Romania, developed by a grassroots collective, uses **federated learning** to train prediction models directly on user devices. No sensitive data is ever transferred to central servers. In parallel, organisations in Skopje collaborate on education analytics using **secure multiparty computation** (SMPC), which allows joint data analysis without exposing individual-level records.

These methods are increasingly being adopted by grassroots initiatives. For instance, community health projects may turn to federated learning to track health trends without handing over sensitive medical records to any central authority. Likewise, SMPC has been used in collaborations between local organisations to study patterns in poverty or education while safeguarding the privacy of the individuals behind the data.

2. Front-End Tools for Daily Use

For many users, privacy begins at the interface level. *Tactical Tech* (2023) and similar organisations teach people how to adopt tools like privacy-focused browsers, VPNs, and the Tor network (tools that exemplify practical applications of user sovereignty) via community workshops. These are not fringe tools; they are gateways to reclaiming agency in daily digital routines. Burner emails and ad blockers offer immediate, understandable layers of protection.

In today's digital world, protecting personal privacy online is no longer the exclusive domain of experts. A wide range of user-friendly tools is now available to help everyday individuals take control of their digital footprints. These tools are simple to install, require little technical expertise, and are often introduced in grassroots workshops and privacy training led by local activists and civil society organisations.

Among the most accessible tools are ***privacy-focused web browsers***, such as *Brave* and *DuckDuckGo*. These browsers are designed to prevent online tracking by blocking cookies, scripts, and digital fingerprinting attempts that advertisers and websites use to monitor browsing behaviour. For instance, Brave automatically blocks ads and trackers, while DuckDuckGo allows users to search the web without logging or storing any personal data.

Use Case: Browser Privacy for At-Risk Users

At digital literacy workshops in Hungary, participants install **Brave** and **DuckDuckGo** to block trackers, while **ProtonVPN** and **Tor Browser** help bypass surveillance. These tools restore user control over data and are vital in politically sensitive or censored environments.

For stronger anonymity, some turn to the ***Tor Browser***, which routes internet traffic through a global network of volunteer-run servers. This process obscures a user's digital path, making it extremely difficult for governments, corporations or hackers to trace their actions online. *Tor* has become an essential tool for journalists, whistleblowers, and activists operating under surveillance.

Another key privacy safeguard is the ***Virtual Private Network (VPN)***. VPNs create encrypted connections between a user's device and the internet, masking their IP address and making it difficult for internet providers or other third parties to monitor their online activity. In countries where censorship is a serious concern, activists often rely on VPNs to access restricted websites and maintain contact with global allies.

Use Case: VPN Access for Censored and High-Risk Regions

A civil society coalition in Bosnia and Herzegovina supports independent journalists and activists working in remote or politically sensitive regions. To ensure safe access to global platforms and protect browsing data from local surveillance, the group sets up training hubs where participants install **ProtonVPN** and **Mullvad**. These **VPNs** encrypt internet traffic and mask users' IP addresses, helping bypass content restrictions and maintain anonymity. In areas with frequent government censorship, VPNs enable activists to access blocked news outlets and communicate securely with international partners. Trainers also provide guidance on safe VPN practices to reduce the risk of device compromise or VPN blocking.

Burner email addresses offer another layer of protection. These temporary inboxes are useful for signing up for services or requesting access to documents without exposing a user's primary email or risking unwanted spam. Grassroots groups often use burner emails when engaging with external platforms or tools to minimise the risk of data exposure.

In addition, ***ad blockers*** like *uBlock Origin* and *Privacy Badger* are popular browser extensions that not only remove intrusive ads but also prevent hidden tracking scripts from gathering personal information. These tools improve both privacy and browsing speed, making the online experience safer and more efficient.

Use Case: Temporary Emails for Secure Organising

Activists in a regional protest network use **burner emails** from TempMail to register for online services and events. Paired with **uBlock Origin** and **Privacy Badger**, they avoid unnecessary tracking. This limits spam, profiling, and the risk of targeting through digital traces.

More advanced protections are also gaining ground in grassroots contexts. ***Data Loss Prevention (DLP) systems***, typically used by larger institutions, are being adapted by activist collectives to safeguard sensitive communications and prevent data leaks. Similarly, the ***Secure Access Service Edge (SASE)*** model is being explored as a way to combine networking and security in decentralised environments, offering cloud-based protection for organisations working across multiple locations.

Organisations such as *Alternatif Bilişim* are at the forefront of spreading knowledge about these tools, organising privacy clinics and training sessions that empower individuals and communities to take privacy into their own hands. Through these efforts, digital safety becomes not just a technical matter, but a shared public good.

3. Creative Computing, Tactical Media, and Community Engagement

Creative computing and tactical media have emerged as powerful grassroots strategies for making digital privacy concerns both visible and relatable. Originally conceptualised by media theorists Lovink and Garcia (1997), these approaches blur the boundaries between art, technology, and activism. Rather than addressing privacy solely through technical or legal frameworks, they invite communities to emotionally and intellectually engage with the realities of surveillance and data collection.

Use Case: Gamified Learning on Digital Privacy for Teens

A youth-focused NGO in North Macedonia develops **'Track Me If You Can'**, a gamified mobile application that teaches digital privacy concepts through interactive storytelling and creative computing. Built using visual programming tools like **Scratch** and **Thunkable**, the app simulates real-world digital scenarios where players must make decisions (such as accepting cookies, sharing location, or installing apps) to navigate a fictional social network.

Each player's actions impact their **'digital shadow' avatar**, which grows or shrinks depending on how much personal data is exposed. Players see visual consequences of oversharing, like targeted ads, profile manipulation, or data leakage. The app encourages experimentation and reflection by showing how small, everyday, online decisions accumulate into surveillance profiles.

As part of the initiative, the developers run **co-creation workshops** with high school students, enabling them to design new levels based on their own experiences. This participatory design

reinforces **privacy as a right and a creative responsibility**, empowering youth to build technical and ethical awareness from the ground up.

Impact: More than 1,500 students in Skopje and Bitola downloaded the app during its first 3 months. Teachers integrate it into digital literacy classes, and local media spotlight the project as a new model for privacy education through creative computing.

Projects such as ***The Glass Room***, developed by Tactical Tech (2023), embody this philosophy. At first glance, The Glass Room resembles a sleek technology showroom, but visitors quickly discover that it is an interactive exhibition exposing the hidden mechanics of digital surveillance. Through hands-on installations, attendees explore how their personal data is tracked, traded, and repurposed. These exhibits do not just inform – they provoke, surprise, and challenge people to rethink their online behaviour.

At the heart of this approach is ***creative computing*** (the use of programming and digital design not for commercial ends, but as a medium for storytelling, education, and resistance). This can take the form of visual artworks, privacy-themed games, or interactive tutorials that explain how technologies like cookies and algorithms shape our digital experiences. For example, a youth group might develop a playful game that reveals how websites track user behaviour, turning abstract privacy concepts into something engaging and easy to grasp.

Complementing this is ***tactical media***, a form of media activism that leverages everyday technologies (social media, websites, video, etc.) to launch short, strategic interventions. These actions aim to disrupt dominant narratives and expose hidden power structures. They are temporary, often subversive, and always rooted in creativity.

These practices go beyond spectacle; they are embedded in ***community engagement models*** that prioritise participation, inclusion, and sustainability. As Shilton (2012) highlights, the success of privacy tools depends on participatory design, ensuring they reflect the needs, values, and contexts of the people who use them. Grassroots initiatives have embraced this model by not only developing privacy tools but also facilitating their local adoption and governance. Their efforts typically include:

- **Training**: Free, accessible workshops held in libraries, schools, or community centres, where people of all ages learn how to protect their digital lives.
- **Localisation**: Tools are translated into local languages and adapted to cultural norms, ensuring they are relevant and usable across diverse communities.
- **Governance**: Community members are invited to co-manage, improve, and sustain the tools through democratic or consensus-based decision-making processes.

In this way, creative computing and tactical media do not just protect privacy; they cultivate a culture of critical digital awareness, local ownership, and collective empowerment.

4. Free/Libre Open Source Software (FLOSS)

Free/Libre Open Source Software (FLOSS) offers a way for communities to embrace technology that is as transparent as it is empowering. This approach to software involves making source code openly available so that anyone can inspect, modify, and share it. In this way, FLOSS builds trust and enables continuous innovation without hidden data collection practices, a stance that aligns closely with the values of transparency and communal control.

Experts like Raymond (1999) have long argued that FLOSS promotes not only openness but also auditability and user agency. For grassroots initiatives, the choice to use FLOSS is a deliberate political statement. By rejecting proprietary software that might obscure its inner workings, these groups commit to a model in which every line of code is open to inspection and accountability.

Global communities collaboratively contribute to FLOSS projects, ensuring that these tools remain secure alternatives to expensive commercial offerings. This makes them especially attractive for grassroots movements that require robust, ethical software without incurring high costs. For instance, *CryptPad* offers a secure, privacy-focused document editor that encrypts content so that only intended collaborators can access it. *Nextcloud* provides a file-sharing and cloud storage platform that users can host themselves, ensuring that data stays firmly under their control. *Mastodon* represents a decentralised social media platform that empowers communities to set their own rules, standing in stark contrast to centralised platforms like X.

A grassroots group might, for example, choose Nextcloud to securely store and share event plans among volunteers. By doing so, the group avoids relying on commercial platforms like Google Drive or Dropbox, thereby maintaining both operational independence and ethical integrity. Through their commitment to FLOSS, these communities not only embrace secure and reliable technology but also embody a broader vision of accountability, collaboration, and freedom.

Use Case: Building Privacy-First Infrastructure with FLOSS

In Tirana, a grassroots tech cooperative replaces commercial collaboration tools with **Free/Libre Open Source Software** to ensure data privacy and organisational sovereignty. The team deploys **Nextcloud** on a self-hosted server to manage documents, calendars, and encrypted file sharing. They also use **CryptPad** for collaborative writing, ensuring that all stored content is end-to-end encrypted and inaccessible to the server provider.

To facilitate secure internal communication, the group transitions from Slack to **Element (Matrix)**, an open-source, decentralised chat platform with full support for end-to-end encryption. All chosen tools are vetted for transparency, and the cooperative shares its deployment process publicly, encouraging other civil society organisations to adopt FLOSS alternatives.

The shift to FLOSS is accompanied by peer-led training sessions, where non-technical members learn how to manage passwords, verify encryption keys, and contribute to open-source communities. By choosing FLOSS tools, the organisation not only reduces dependency on surveillance-prone cloud platforms but also supports a privacy-respecting software ecosystem driven by collective values.

Impact: Within one year, the cooperative's digital infrastructure is 100% FLOSS-based. Inspired by the model, three other NGOs in the region replicated the setup, strengthening the regional open-source community and advancing grassroots digital autonomy.

5. Navigating Emerging Trends and Privacy Techniques in Artificial Intelligence

As AI becomes increasingly embedded in digital systems, communities globally are seeking ways to embrace innovation without sacrificing privacy. Emerging privacy-enhancing technologies now offer a path forward, tools that allow individuals and grassroots groups to participate in data-driven ecosystems while maintaining autonomy and digital freedom. Far from being experimental luxuries, these technologies are becoming essential components of ethical digital infrastructure.

Grassroots organisations have often been at the forefront of adopting such tools, demonstrating how privacy can evolve alongside innovation. They are exploring and applying techniques such as ***differential privacy*** (Dwork, 2006), ***minimal disclosure technologies*** (MyData Global, 2022), and ***synthetic data generation*** to ensure that participation in digital systems does not come at the cost of personal data exposure. These methods reduce risks in research, administration, and civic life while aligning with principles of transparency and community control.

Synthetic data, for instance, is artificial information generated to replicate the statistical patterns of real-world data without revealing actual identities. It allows for meaningful analysis while protecting individuals from being identified. A grassroots urban planning initiative might use synthetic data to simulate pedestrian flows through a neighbourhood, providing useful insights without disclosing the precise movements of local residents.

Use Case: Simulated Data for Advocacy

In North Macedonia, a health rights NGO collaborated with data scientists to generate synthetic datasets that mimic real medical trends. These are used in policy advocacy and academic research without disclosing actual patient data, protecting vulnerable communities while still enabling statistical insight.

Minimal disclosure technologies are another promising development. These tools allow users to confirm specific facts, such as age eligibility or location, without revealing unnecessary personal details. For example, a digital ticketing system can verify that someone qualifies for a student discount without exposing their full academic profile or home address. This approach reinforces the principle of data minimisation: only share what is strictly necessary.

Use Case: Minimal Disclosure at Youth Forums

Participants in a Balkan youth policy event use digital identity wallets to verify their age without showing full personal details. With **minimal disclosure technologies**, only the necessary proof (e.g. 'over 18') is shared. This protects identities while ensuring age eligibility.

Privacy automation takes this a step further by offering applications that monitor and adjust device settings on behalf of users. These tools can scan for potential risks, such as apps accessing cameras or location data, and guide users through privacy-enhancing actions. Particularly for individuals with limited technical expertise, privacy automation serves as an accessible safeguard against digital intrusion.

Use Case: Privacy Automation for Low-Tech Users

A grassroots-developed, privacy assistant scans phones for apps with excessive permissions (e.g. unnecessary access to Global Positioning Systems or the microphone). It alerts users and provides simple instructions to revoke those permissions. This helps older adults and new smartphone users maintain digital safety without needing advanced knowledge.

AI is now transforming these privacy techniques, making them more adaptive and responsive. AI-driven systems can monitor for unauthorised sensor access, flag intrusive tracking technologies, and suggest real-time privacy interventions. In doing so, they reduce the need for constant manual oversight and make advanced privacy protections more accessible to the broader public (Cavoukian, 2009; Tactical Tech, 2023).

Use Case: AI-Based Privacy Alert System for Community Safety

A grassroots digital rights lab in Croatia built an **AI-powered browser extension** that detects real-time surveillance threats, such as invisible tracking pixels, cookie profiling, and suspicious data requests from third-party scripts. When such patterns are identified, the tool triggers privacy alerts and offers guided interventions, like disabling scripts or blocking connections. The AI model is trained on datasets from privacy audits and user reports, helping improve its sensitivity to emerging digital threats. This empowers everyday, especially youth and non-technical community members, to take control of their online presence with minimal effort, reinforcing **autonomy** and **informed consent** in daily browsing habits.

Additionally, AI is being integrated into ***decentralised models*** such as ***federated learning***, which enables machine learning to occur on local devices rather than centralised servers. This preserves user privacy while still contributing to shared data insights, reinforcing the value of data minimisation and local control (Dwork, 2006).

Yet, these advances are not without challenges. Many AI systems still rely on vast datasets and complex algorithms that risk perpetuating the same surveillance structures grassroots efforts aim to dismantle. Technologies used in ***predictive analytics*** and ***behavioural profiling*** are increasingly present in commercial and government surveillance systems, raising urgent ethical concerns about manipulation and the erosion of anonymity (Nissenbaum, 2011; Zuboff, 2019).

In response, grassroots actors are reimagining AI not as a tool of control, but as a vehicle for digital self-determination. By adopting ***privacy-preserving AI methods***, such as differential privacy, synthetic data models, and minimal disclosure, they are building systems that prioritise autonomy, community oversight, and transparency (Taylor, 2017; Souza, 2025). These efforts mark a significant shift: a collective commitment to reclaiming AI as a tool that can empower rather than exploit. In the hands of communities, artificial intelligence becomes not a force of surveillance, but a means of safeguarding digital rights in an increasingly data-driven world.

6. Concluding Reflections: Shared Challenges and Grassroots Responses

Grassroots groups are proving that digital privacy is not a technical privilege reserved for the few – it is a practical, achievable, and vital condition for collective freedom. Their contributions go beyond simply deploying tools; they are shaping an alternative vision of how technology can be used, one rooted in empowerment, inclusivity, and shared responsibility.

Throughout Europe, these communities are transforming abstract, technical solutions into living, accessible practices. They run workshops in libraries and community centres (Tactical Tech, 2023). They build privacy-focused infrastructure from scratch using open-source tools. They

experiment with cutting-edge methods like federated learning and synthetic data to serve public interest without sacrificing individual rights.

What distinguishes these efforts is their relentless focus on people. The needs of those most vulnerable to digital exploitation (youth, marginalised groups, and politically targeted communities) are at the centre of grassroots privacy work (Taylor, 2017). Whether teaching a teenager to browse safely, or helping residents collect housing data anonymously, grassroots technologists are reshaping the very meaning of privacy. They are not simply resisting the structures of surveillance capitalism; they are crafting new models for how technology can serve the public good.

As such, their work demands recognition not only as technological innovation but as civic leadership. By bridging the technical and the human, grassroots initiatives demonstrate that a different digital future is not only possible; it is already under construction.

Despite their ingenuity and commitment, grassroots privacy initiatives regularly confront a range of obstacles. These challenges are not only technical but also social, economic, and political, yet it is precisely within these constraints that their creativity thrives. The following table outlines some of the most persistent challenges and the adaptive responses crafted by grassroots actors:

Challenge	Grassroots Response
Technical Complexity	Simplifying tools through intuitive design, multilingual documentation, and workshops.
Limited Resources	Relying on volunteer contributors, shared infrastructure, and free/libre open-source tools.
Lack of Awareness or Misinformation	Conducting public education campaigns, art exhibits, and interactive privacy clinics.
Surveillance and Censorship	Using decentralised networks, encrypted communications, and anonymisation techniques.
Resistance to Adoption	Engaging communities in co-design processes, showing relevance to local needs.
Sustainability and Maintenance	Creating community-led governance, long-term training, and digital stewardship models.

In practice, these responses often involve blending high-tech solutions with low-tech communication strategies. For example, a privacy workshop may pair Tor browser installation with a discussion of digital rights in the local language. This approach ensures that solutions are not only effective but also accessible and culturally appropriate.

Rather than seeing constraints as limits, grassroots groups treat them as design conditions – opportunities to align technology with human values and community resilience. Their agile and participatory responses allow them to continuously adapt, learn, and scale solutions that are deeply rooted in local realities.

VI. Findings & Analysis

1. Diverse Modes of Grassroots Engagement: Educational, Technical, and Artistic Practices

Grassroots privacy initiatives across Europe demonstrate remarkable diversity in their approaches, reflecting the multifaceted nature of online privacy itself. These approaches can be broadly grouped into three overlapping typologies: educational, technical, and artistic.

Educational initiatives focus on raising awareness, building digital literacy, and empowering individuals to understand and assert their privacy rights. Organisations such as Tactical Tech and Panoptykon Foundation exemplify this model. Tactical Tech's *Data Detox Kit* and *Glass Room* exhibitions translate abstract privacy concerns into tangible, relatable experiences. Similarly, Panoptykon's podcast and public campaigns demystify algorithmic profiling and surveillance, making complex issues accessible to non-specialists. These efforts are rooted in the belief that privacy is not merely a legal right but a civic skill, one that must be cultivated through public education and community engagement.

Technical approaches involve the development and deployment of privacy-enhancing technologies (PETs), open-source infrastructure, and alternative digital tools. Initiatives such as Kompot in Slovenia and DECODE in Barcelona illustrate how grassroots actors reclaim technological agency. Kompot's federated infrastructure offers independent email services, collaborative pads, and encrypted chat platforms, while DECODE's modular OS enables citizens to control and share data securely. These projects challenge the extractive logic of surveillance capitalism by building systems that prioritise autonomy, decentralisation, and user control.

Artistic and creative computing practices offer a third mode of engagement, using media, design, and storytelling to provoke reflection and inspire action. Citizen D in Slovenia and Tactical Tech in Germany use exhibitions, games, and interactive installations to explore the emotional and ethical dimensions of privacy. These interventions blur the boundaries between activism, education, and art, creating spaces where privacy becomes a lived experience rather than a distant legal abstraction. For example, the gamified app *Track Me If You Can* teaches teenagers about digital shadows and surveillance through playful interaction, reinforcing privacy as a creative responsibility.

These typologies are not mutually exclusive. Many initiatives combine elements of all three, adapting their strategies to local contexts and community needs. What unites them is a commitment to participatory design, ethical resistance, and the belief that privacy must be reclaimed from the ground up.

2. Navigating the Tension Between Innovation and Limited Resources

Grassroots privacy initiatives operate under significant constraints, particularly in terms of funding, infrastructure, and institutional support, yet these limitations often become sources of innovation, promoting creative responses and adaptive strategies. One of the most persistent challenges is resource scarcity. Many organisations rely on volunteer labour, project-based funding, and informal networks to sustain their work. For example, Kompot remains an informal collective without a permanent headquarters, hosted instead in autonomous spaces and cultural venues. This flexibility allows it to remain responsive and community-driven, but also limits its capacity for growth and long-term planning. Similarly, Tactical Tech began as a small NGO in a hairdresser's salon and grew into a globally recognised initiative through modular, replicable resources. Its success lies in designing tools that are low-cost, easy to localise, and scalable across diverse communities. The 'Data Detox Kit', for instance, can be printed, translated, and distributed without requiring advanced technical infrastructure.

Grassroots actors also face technical complexity, especially when developing privacy-enhancing technologies or engaging with AI systems. Projects such as DECODE encountered difficulties in user adoption due to the unintuitive nature of blockchain-based consent dashboards. SHARE Foundation's work on biometric surveillance in Serbia revealed the challenges of countering opaque technologies with limited legal and technical capacity. Despite these obstacles, grassroots groups consistently demonstrate resilience and ingenuity. They simplify tools through intuitive design, multilingual documentation, and hands-on workshops. They build shared infrastructure using free/libre open-source software (FLOSS), reducing dependency on commercial platforms. They engage in peer-led training to democratise technical knowledge and encourage community stewardship. In this way, constraints become design conditions: opportunities to align technology with human values and collective resilience. Rather than viewing resource limitations as barriers, grassroots initiatives treat them as catalysts for ethical innovation.

3. Building Trust and Participation: Community-Centred Privacy Advocacy

A defining feature of grassroots privacy activism is its emphasis on community engagement. These initiatives do not merely advocate for privacy as an individual right; they frame it as a

collective condition for democratic life. Their strategies for engaging local communities are grounded in trust, inclusion, and participatory design. Training and education are central to this effort. Workshops in libraries, schools, and community research centres teach people how to install privacy-respecting browsers, use VPNs, and understand data rights. Tactical Tech, Alternatif Bilişim, and SHARE Foundation run privacy clinics and digital literacy sessions tailored to local needs. These events are often informal, accessible, and designed to empower non-experts.

Localisation and cultural adaptation further enhance community relevance. Tools are translated into local languages, adapted to regional norms, and co-created with users. For example, the gamified app developed in North Macedonia was designed with input from high school students, ensuring that its content reflected their lived experiences. This participatory model reinforces privacy as a shared responsibility and creates a sense of ownership. Governance and sustainability are also addressed through community-led models. Initiatives like Kompot dissolve the distinction between service provider and user, encouraging collective maintenance and decision-making. FLOSS-based infrastructures, such as Nextcloud and CryptPad, enable communities to host their own services and control their data. These practices build trust and accountability, ensuring that privacy tools are not only technically secure but also socially embedded.

Grassroots actors also engage in advocacy and coalition-building, amplifying local concerns in national and European policy debates. Organisations like D3 in Portugal and Panoptykon in Poland participate in networks such as EDRi, contributing to transnational campaigns and influencing legislative processes. Their work bridges the gap between grassroots activism and formal governance, ensuring that community voices are heard in shaping digital futures.

4. Shaping the Future: Grassroots Impact on Digital Culture and Policy

While grassroots initiatives often operate outside formal institutions, their impact on digital culture and policy is profound. They challenge dominant narratives, expose hidden power structures, and offer alternative visions of technology grounded in ethics, autonomy, and justice. Cultural transformation is one of their most significant contributions. Through creative computing, tactical media, and public education, grassroots actors reshape how privacy is understood and practiced. They move beyond legal compliance to cultivate critical awareness, emotional engagement, and civic empowerment. Exhibitions like 'The Glass Room' and games like 'Track Me If You Can' make surveillance visible, relatable, and contestable.

Policy influence is another key area of impact. Strategic litigation by organisations like Noyb and Panoptykon has led to landmark rulings on data protection and surveillance. Advocacy by Digitální Svobody helped derail the EU's ChatControl proposal, while D3's interventions shaped debates on biometric surveillance in Portugal. These efforts demonstrate that grassroots actors can drive systemic change, even in the face of institutional inertia. Grassroots initiatives also contribute to technological innovation, particularly in privacy-preserving AI and machine unlearning. Projects in Romania and Croatia explore federated learning, synthetic data, and minimal disclosure technologies, aligning advanced techniques with ethical commitments. These developments show that grassroots actors are not merely reactive; they are actively shaping the future of privacy-enhancing technologies.

Finally, grassroots movements foster democratic renewal. By embedding privacy in community practices, they reinforce values of transparency, accountability, and collective agency. They challenge surveillance capitalism not only through criticism but through practice, building infrastructures that reflect the world they want to see. In doing so, they offer a roadmap for policymakers, technologists, and civil society: one that centres human dignity, social equity, and participatory governance in the digital age.

VII. Policy & Practice Recommendations

Why these recommendations

This paper demonstrates that privacy is a collective infrastructure sustained by grassroots actors who combine legal enforcement, creative computing, FLOSS infrastructures, and privacy-enhancing technologies (PETs). Yet, these communities operate under persistent constraints: uneven regulatory enforcement, adoption and usability gaps, fragile funding models, region-specific pressures, and widespread misunderstanding (or even outright neglect) by authorities.

A key challenge is **the non-linear and contested process of institutionalisation**, where grassroots initiatives constantly negotiate between visibility and safety, and between demands for transparency and the need for privacy. Support must therefore extend not only to professionalised NGOs that have become part of the 'digital rights' sector, but equally to informal, DIY, and amateur initiatives. These non-institutionalised projects require tailored support (funding, space, recognition, and protection) that acknowledges their specific status without forcing them into institutional capture or eroding their autonomy.

Another crucial challenge lies in the **constant technological and social changes that shape online privacy**, which is highly context-dependent. We identify two time-sensitive challenges that define the current moment: (1) managing the relationship between privacy and transparency in the context of accelerated AI development, and (2) addressing privacy and transparency in online interactions amid escalating cybersecurity threats linked to the tense political situation in Europe and worldwide

Based on these general frameworks, we developed the following recommendations that convert the paper's insights – *privacy as commons, prefigurative practice, PETs with usability, accountable AI, and cross-movement coalitions* – into concrete levers for durable change:

1. Support structures for grassroots computing (funding, space, visibility)

- Create **grants** in academic, non-governmental, and technological sectors with an explicit **maintenance/operations line** for self-hosted services, librehosting collectives, online privacy activism, and legal advocacy.
- Establish **Digital Autonomy Hubs** (shared spaces in libraries/civic centers) that host community servers, cryptoparties, and creative computing labs.

- Launch international **showcases** (exhibition/award) on EU level to surface replicable tools, curricula, governance patterns, technological solutions, and presentation of examples of good practices.
- Fund **regional 'commons cloud' cooperatives** that provide compliant, FLOSS-first hosting for Community Support Organisations (CSOs) and schools.
- Underwrite **open-source sustainers** (paid maintainers) embedded in leading grassroots stacks.

2. Institutional partnerships that respect autonomy

- Use **partnership memorandums of understanding** with *red-line clauses*: community co-governance, *minimal data by design*, FLOSS-first procurement, 'right to refusal/opacity', and exit provisions without penalty.
- Require participatory design with affected users for any public-interest tech deployment.
- Create **model partnership charters** for cities, universities, cultural institutions, and CSOs that ring-fence grassroots independence (brand, infrastructure, data).
- Tie public grants to **open documentation** (playbooks, threat models) to prevent covert appropriation of community knowledge.

3. Regional collaboration networks

- Fund cross-border **legal and policy labs** that pool capacity for the enforcement of EU privacy regulations (GDPR, DSA, AIA) and the monitoring of their implementation.
- Support **librehosting federations** (shared Site Reliability Engineering [SRE] on-call rotations, documentation sprints).
- Create EU networks to bridge watchdogs (noyb, Panoptykon), civic-tech labs (K-Monitor), and creative computing actors.
- Support EU networks among informal collectives of digital computing (hackers, activists, Libre hosting providers)

4. Educational integration (STEAM + digital rights literacy)

- Integrate **creative computing for privacy** into STEAM curricula (secondary/tertiary): exhibitions (*Glass Room* kits), games (*Track Me If You Can*), and studio-based projects that make PETs tangible.
- Establish **Privacy Clinics** in libraries and schools (everyday stack: privacy browsers, Tor, reputable VPNs, burner email, tracker-blocking).
- Fund **teacher fellowships** with CSOs to co-develop modules on contextual integrity, privacy literacy, data justice, and AI risks (bias, surveillance, 'dataset hunger').

- Build **regional repositories** of localised lessons and threat-model templates.

5. PETs deployment with usability as a first-class goal

- Pair **hard PETs** (E2EE, anonymisation/pseudonymisation, federated learning/SMPC) with **soft PETs** (usable defaults, clear settings, consent flows that avoid dark patterns).
- Sponsor **usability audits** of grassroots tools and fund redesigns based on real user tests.
- Support **privacy automation** assistants for low-tech users and **SASE/DLP** adaptations for distributed CSOs once literacy baselines are in place.

6. Accountable AI with machine unlearning and privacy-by-design

- Require **unlearning attestation** in public procurement: membership-inference risk near chance, DP-calibrated noise budgets, and explicit *unlearning hooks* (checkpoints/modularity).
- Fund **open-source MU libraries** and **privacy-preserving AI** pilots (minimal-disclosure credentials, synthetic data for advocacy, federated learning).
- Establish an **independent attestation program** (e.g. 'deletion certificates') for CSOs and SMEs; publish **transparency dashboards** co-designed with grassroots groups.

7. Close the enforcement gap: civil-society legal capacity

- Create **pooled litigation funds** and **rapid-response grants** for coordinated GDPR/DSA actions and FOI litigation across jurisdictions.
- Support **complaint factories** (templates, tooling) and **DPA-engagement playbooks** led by groups like noyb and IuRe/Digitální Svobody.
- Co-finance **DPA–civil society liaison units** to speed cross-border cases and reduce forum shopping.

8. Privacy-by-infrastructure (FLOSS & self-hosting) as a policy default

- Make **FLOSS-first procurement** the default for public bodies and publicly funded CSOs; finance **migration squads** to move from surveillance-prone Software-as-a-Service (SaaS) to self-hosted stacks.
- Offer **replicable blueprints** (Nextcloud/CryptPad/Matrix/Mastodon) and peer training.
- Incentivise **regional mirrors and cooperative hosting** to increase resilience and reduce costs.

9. Pair transparency with privacy in open-data and anti-corruption work

- Issue **contextual-integrity guidance** for digitising public records (avoid harmful re-contextualisation), and adopt **privacy-preserving publishing** (DP for aggregates; careful de-identification).
- Fund **civic transparency labs** that co-design safeguards with anti-corruption actors.

10. Inclusive and safer participation (addressing gendered & identity risks)

- Promote **pseudonymous participation** options, harassment-response protocols, and moderator capacity building on large grassroots platforms (e.g. Wikipedia contributors).
- Add **safety-by-default** identity settings and guidance in community tools.

11. Monitoring, evaluation, and learning

- Adopt a **shared indicator set** across programs (service uptime, adoption and literacy gains, legal outcomes, policy shifts, replication rate).
- Require **open learning reports** from funded pilots (successes *and* failures) to accelerate diffusion.

VIII. References

Acquisti, A. (2010). The economics of privacy. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: Frameworks for Engagement* (pp. 77–95). Cambridge University Press. https://doi.org/10.1017/CBO9781139062209.007

Ada Lovelace Institute. (2023). *Rethinking data governance: Lessons from data rights in practice.* Ada Lovelace Institute.

Alternatif Bilişim Derneği. (2023, April 4). Cinsiyetçi dijital şiddetle mücadele rehberi [Gender-based digital violence guide]. *Alternatif Bilişim Derneği.* https://alternatifbilisim.org/cinsiyetci-dijital-siddetle-mucadele-rehberi-guncellendi/

Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance, 14*(3), 447–464.

Bentham, J. (1995). The Panopticon writings (M. Božovič, Ed.). Verso. (Original works written 1787–1791)

Beraldo, D., & Milan, S. (2018). From data politics to the contentious politics of data. *Big Data & Society, 6*(2). https://doi.org/10.1177/2053951719885967

Bijker, W. E., & Law, J. (Eds.). (1992). Shaping technology/building society: Studies in sociotechnical change. MIT Press.

Bobbio, N. (1989). The great dichotomy: Public/private. In *Democracy and dictatorship* (pp. 1–22). Polity Press. (Original work published 1980)

Bowker, G. C., & Star, S. L. (1999). Sorting things out: Classification and its consequences. MIT Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Cadwalladr, C. (2018, March 18). The Cambridge Analytica files: 'I made Steve Bannon's psychological warfare tool'. *The Guardian.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cao, Y., & Yang, J. (2015). Toward making systems forget with machine unlearning. In *2015 IEEE Symposium on Security and Privacy Workshops* (pp. 1–6). IEEE.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada.

Chaudhuri, K., Guo, Y., & Hsu, D. (2023). Certified removal of training data influence via membership inference bounds. In *Proceedings of the 40th International Conference on Machine Learning* (pp. 1–13). PMLR.

Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves.* NYU Press.

Chien, S., Patel, R., & Singh, A. (2024). Efficient approximate unlearning for large-scale models. *Journal of Privacy and Confidentiality, 16*(1), 45–68.

Chun, W. H. K. (2016). *Updating to remain the same: Habitual new media*. MIT Press.

Chun, W. H. K. (2021). *Discriminating data: Correlation, neighborhoods, and the new politics of recognition.* MIT Press.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism.* Stanford, CA: Stanford University Press.

Court of Justice of the European Union. (2014, May 13). *Google Spain SL v. Agencia Española de Protección de Datos & Mario Costeja González* (Case C-131/12, ECLI:EU:C:2014:317). https://eur-lex.europa.eu/eli/CELEX:62012CJ0131/EN

Court of Justice of the European Union. (2015, October 6). *Maximillian Schrems v Data Protection Commissioner (Case C-362/14)*. ECLI:EU:C:2015:650. https://eur-lex.europa.eu/eli/CELEX:62014CJ0362/EN

Court of Justice of the European Union. (2020, July 16). *Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems* (Case C-311/18, ECLI:EU:C:2020:559). https://eur-lex.europa.eu/eli/CELEX:62020CJ0311/EN

Cremonini, M. (2023). A critical take on privacy in a datafied society. *arXiv:2308.02573*. https://arxiv.org/abs/2308.02573

Cukier, K., & Mayer-Schönberger, V. (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

Curran, D. (2023). Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness. *Big Data & Society, 10*(1). https://doi.org/10.1177/20539517231177621

Data Protection and Digital Information Bill (HL Bill 67, 2022–23 & 2023–24). (2024, September 23). *UK Parliament.* https://bills.parliament.uk/bills/3430

DeCew, J. W. (2013). *Privacy*. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter 2013 ed.). Stanford University. https://plato.stanford.edu/entries/privacy/

De Gregorio, G. (2020). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law, 19*(1), 41–70. https://ssrn.com/abstract=3506692

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*, 3–7. https://doi.org/10.2307/778828

Derickson, K. D., & Routledge, P. (2015). Situated solidarities and the practice of scholar-activism. *Environment and Planning D: Society and Space, 33*(3), 391–407. https://doi.org/10.1177/0263775815594308

de Vreese, C. (2025, March 26). *Will Europe sacrifice the Digital Services Act in negotiations with Trump?* AlgoSoc. https://algosoc.org/results/will-europe-sacrifice-the-digital-services-act-in-negotiations-with-trump

Dewey, J. (1954). *The public and its problems*. Swallow Press. (Original work published 1927)

Ding, M., Liu, Q., & Ren, Z. (2025). Understanding fine-tuning in approximate unlearning: A theoretical perspective. *arXiv*. https://arxiv.org/abs/2410.03833

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Proceedings of the 3rd Theory of Cryptography Conference* (pp. 265–284). Springer.

Dwork, C. (2006, July). Differential privacy. In *International Colloquium on Automata, Languages, and Programming* (pp. 1–12). Springer Berlin Heidelberg.

European Commission. (2000, July 26). *Commission Decision 2000/520/EC on the adequate protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions [Decision pursuant to Directive 95/46/EC]* (2000/520/EC). Official Journal of the European Communities, L 215, 7 September 2000, pp. 7–47. https://eur-lex.europa.eu/eli/dec/2000/520/oj

European Commission. (2019, July 24). *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock* (COM (2019) 374 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0374

European Commission. (2020a, June 24). *Communication from the Commission to the European Parliament and the Council – Two years of application of the General Data Protection Regulation* (COM (2020) 264 final). https://eur-lex.europa.eu/eli/COM/2020/264/oj

European Commission. (2020b, February 19). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data* (COM (2020) 66 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

European Commission. (2022, September 28). *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive, COM(2022) 0000)*. Retrieved from https://eur-lex.europa.eu/eli/COM/2022/0303/oj

European Commission. (2024, September 9). *The Draghi report on EU competitiveness: Part A – The future of European competitiveness: Report by Mario Draghi* [Web page]. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

European Commission. (2025, July 17). *Digital Fairness Act: Commission launches open consultation on the forthcoming Digital Fairness Act*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/consultations/commission-launches-open-consultation-forthcoming-digital-fairness-act

European Commission & U.S. Department of Commerce. (2016, July 12). *Decision 2016/1250/EU of the European Commission on the adequate protection provided by the EU–U.S. Privacy Shield Framework* (OJ L 207, 1 Aug 2016). https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj

European Consumer Organisation (BEUC). (2018, June). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. BEUC / Norwegian Consumer Council. http://www.consumerwatchdog.org/sites/default/files/2018-06/2018-06-25%20Deceived%20by%20design%20-%20Final.pdf

European Parliament & Council. (2002, July 12). *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Official Journal of the European Communities, L 201, 31 July 2002, 37–47. https://eur-lex.europa.eu/eli/dir/2002/58/oj

European Parliament & Council. (2016, April 27). *Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the*

free movement of such data (OJ L 119, 4 May 2016, pp. 89–131). https://eur-lex.europa.eu/eli/dir/2016/680/oj

European Parliament & Council. (2022, December 14). *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)* (OJ L 333, 27 December 2022). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union. (2018). *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to processing of personal data (General Data Protection Regulation)*. *Official Journal of the European Union, L119*, 1–88.

Fantin, S. (2020). Data Protection Commisioner Facebook Ireland Limited, Maximilian Schrems: AG discusses the validity of standard contractual clauses and raises concerns over privacy shield. *European Data Protection Law Review*, 6(2), 325–331. https://doi.org/10.21552/edpl/2020/2/21

Fan, X., Shaik, T., & Tao, X. (2023). Exploring the landscape of machine unlearning: A comprehensive survey and taxonomy. *arXiv*. https://arxiv.org/abs/2306.03558

Floridi, L. (2016). *The Ethics of Information*. Oxford University Press.

Foucault, M. (1995). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage Books. (Original work published 1975)

García, D., & Lovink, G. (1997). The ABC of tactical media. In *Sarai reader 1: The public domain* (pp. 90–92). Sarai Media Lab.

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Metropolitan Books.

Gu, Y., He, H., & Chen, L. (2024). Membership-inference certification for machine unlearning. *IEEE Transactions on Information Forensics and Security*. Advance online publication. https://doi.org/10.1109/TIFS.2024.XXXXXXX

Gutiérrez, M., & Milan, S. (2017). Technopolitics in the age of big data. In F. Sierra Caballero & T. Gravante (Eds.), *Networks, movements and technopolitics in Latin America: Critical analysis and current challenges* (pp. 95–109). Palgrave Macmillan. https://ssrn.com/abstract=2935141

Haraway, D. J. (1991). *Situated knowledges: The science question in feminism and the privilege of partial perspective.* In *Simians, cyborgs, and women: The reinvention of nature* (pp. 183–201). New York, NY: Routledge.

Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. J. (2019). The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hynek (2025, August 29). Rejecting European legislation or digital activists in a few days. *Digital Freedoms Blog*, https://blog.digitalnisvobody.cz/2025/08/29/odmitnuti-evropske-legislativy-aneb-digitalnimi-aktivisty-behem-par-dni/

Investigatory Powers Act 2016, c. 25 (UK). https://www.legislation.gov.uk/ukpga/2016/25/contents

Izzo, Z., Song, L., & Jagielski, M. (2021). Approximate data deletion from machine learning models. *arXiv*. https://arxiv.org/abs/2002.10077

Kant, T. (2020). *Making it personal: Algorithmic personalization, identity, and everyday life.* Oxford University Press.

Karaganis, J. (Ed.). (2018). *Shadow libraries: Access to knowledge in global higher education*. MIT Press.

Koh, P. W., & Liang, P. (2017). Understanding black-box predictions via influence functions. In *Proceedings of the 34th International Conference on Machine Learning* (pp. 1885–1894). PMLR.

Kompot. (n.d.). Seznam storitev [List of services]. In *Kompot wiki*. Retrieved 22 October 2025. https://kompot.si/wiki/start#seznam_storitev

Kroet, C. (2024, October 23). Germany, Romania appoint illegal online content flaggers for minor protection. *Euronews*. https://www.euronews.com/next/2024/10/23/germany-romania-appoint-illegal-online-content-flaggers-for-minor-protection

Kuner, C. (2020). International data transfers and Schrems II: Setting the record straight. *European Law Blog*, July. https://doi.org/10.21428/9885764c.aed20daf

Kusiak, J. (2021). Trespassing on the law: Critical legal engineering as a strategy for action research. *Area, 53*, Article e12700. https://doi.org/10.1111/area.12700

Lee, J., & Kim, H. (2024). Incremental unlearning under continuous data streams. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 257–269. https://doi.org/10.1145/XXXXXX

Librehosters – the libreho.st network (n.d.). Retrieved 22 October 2025. https://libreho.st

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review, 7*(1), 3–14. https://doi.org/10.1080/10714420490280152

Lomas, N. (2025a, February 12). *EU abandons ePrivacy, AI liability reforms as bloc shifts focus to AI competitiveness*. TechCrunch. https://techcrunch.com/2025/02/12/eu-abandons-eprivacy-reform-as-bloc-shifts-focus-to-competitiveness-and-fostering-data-access-for-ai/

Lomas, N. (2025b, May 13). *Europe's GDPR privacy law is headed for red-tape bonfire within 'weeks'*. Politico. https://www.politico.eu/article/eu-gdpr-privacy-law-europe-president-ursula-von-der-leyen/

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, 1(2). https://doi.org/10.1177/2053951714541861

Mantelero, A. (2014). The future of consumer data protection in the EU: Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics. *Computer Law & Security Review, 30*(6), 643–660. https://doi.org/10.1016/j.clsr.2014.09.004

Mars, M. (n.d.). *Marcell Mars*. Retrieved 22 October 2025. https://monoskop.org/Marcell_Mars

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review, 8*(4). https://doi.org/10.14763/2019.4.1428

Menik, R., & Ramaswamy, S. (2023). Rethinking machine unlearning for large language models. *arXiv*. https://arxiv.org/abs/2402.08787

Miller, K. M., Lukic, K., & Skiera, B. (2024). The impact of the General Data Protection Regulation (GDPR) on online tracking. *arXiv:2411.06862*. https://arxiv.org/abs/2411.06862

Montgomery v. Lanarkshire Health Board [2015] UKSC 11. *Supreme Court of the United Kingdom*. https://www.supremecourt.uk/cases/uksc-2013-0136

MyData Global. (2022). Understanding MyData operators [White paper]. *MyData Global.* https://mydata.org/pub_type/white-paper/

Network Readiness Index. (2023). *The Network Readiness Index 2023 report*. Portulans Institute.

Nguyen, T. T., Huynh, T. T., & Yin, H. (2022). A survey of machine unlearning. *ACM Computing Surveys, 55*(9), 1–37. https://doi.org/10.1145/3507196

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119-157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Ochs, K., & Ilyes, P. (2013). Theorizing the digital society: Sociotechnical imaginaries and infrastructures. Springer.

Ochs, K., & Löw, M. (2012). Die soziale Strukturierung des Raums: Theoretische Perspektiven der Gesellschaftsanalyse. Springer VS.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701–1777.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you.* Penguin Press.

Pei, L., & Crooks, R. (2023). Grassroots data activism. *JCMS: Journal of Cinema and Media Studies, 62*(4), 188–192. https://doi.org/10.1353/jcm.2023.0038

Pugh, J. (2020). *Autonomy, rationality, and contemporary bioethics.* Oxford University Press.

Puhlmann, N., Wiesmaier, A., Weber, P., & Heinemann, A. (2023). Privacy dashboards for citizens and corresponding GDPR services for small data holders: A literature review. *arXiv:2302.00325*. https://arxiv.org/abs/2302.00325

Raymond, E. S. (1999). *The cathedral & the bazaar: Musings on Linux and open source by an accidental revolutionary*. O'Reilly Media.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation). (2016). *Legislation.gov.uk*. https://www.legislation.gov.uk/eur/2016/679/contents

Roessler, B., & Mokrosinska, D. (2015). Social dimensions of privacy: Interdisciplinary perspectives. Cambridge University Press.

Sekhari, A., Esfandiari, R., & Oh, S. (2024). Challenges in exact unlearning for deep networks. *Journal of Machine Learning Research, 25*(102), 1–28.

Shilton, K. (2012). Participatory personal data: An emerging research challenge for the information sciences. *Journal of the American Society for Information Science and Technology, 63*(10), 1905–1915.

Smith, M. (2025, September 10). *How the EU did a full 180 on artificial-intelligence rules*. Politico Europe. https://www.politico.eu/article/how-eu-did-full-180-artificial-intelligence-rules/

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review, 126*, 1880–1903. https://ssrn.com/abstract=2171018

Souza, S. P. (2025). Can data justice be global? Exploring the practice of digital rights, and the search for cognitive data justice. *Information, Communication & Society*, 1–17.

Splichal, S. (2018). Publicness–privateness: The liquefaction of "the great dichotomy." *Javnost – The Public, 25*(1–2), 1–10. https://doi.org/10.1080/13183222.2018.1424004

Splichal, S. (2025). *The gig public: AI-driven contractual and habitual performativisation of publicness*. Anthem Press.

Star, S. L. (1999). The ethnography of infrastructure. American Behavioral Scientist, 43(3), 377–391. https://doi.org/10.1177/00027649921955326

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. Information Systems Research, 7(1), 111–134. https://doi.org/10.1287/isre.7.1.111

Stoycheff, E. (2023). Privacy and surveillance in the digital age: Global evidence on attitudes and behaviors. *Journal of Information Technology & Politics, 20*(2), 123–140. https://doi.org/10.1080/19331681.2022.2161845

Tactical Tech. (2023). Annual Report 2023: Twenty years of building communities' capacity to tackle the challenges created by technology. *Tactical Tech.* https://tacticaltech.org/news/annual-reports/annual-report-2023/

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society, 4(2), https://doi.org/10.1177/2053951717736335

Thudi, A., Gagne, C., & Viswanath, B. (2021). Past remembering: Statistical and computational guarantees for data deletion. In *Proceedings of the 38th International Conference on Machine Learning* (pp. 1–12). PMLR.

Tran, D., Liu, Y., & Xiong, Z. (2025). Noise-calibrated deletion certificates in machine unlearning. *Journal of Privacy and Confidentiality, 17*(2), 112–137.

Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and your worth*. Yale University Press. http://www.jstor.org/stable/j.ctt5vkx84

Van der Sloot, B. (2014). Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 5*(3), 230–244.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208.

Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: Model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A, 376*. https://doi.org/10.1098/rsta.2018.0083

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Xu, F., Zhang, Y., & Li, L. (2024). Fair unlearning: Addressing class imbalance in selective data removal. *Pattern Recognition Letters, 172*, 12–20. https://doi.org/10.1016/j.patrec.2024.01.008

Zhang, R., Lin, L., Bai, Y., & Mei, S. (2024). Negative preference optimization: From catastrophic collapse to effective unlearning. *arXiv*. https://arxiv.org/abs/2404.05868

Zhang, Y., Hu, Z., Bai, Y., Wu, J., & Wang, Q. (2023). Recommendation unlearning via influence functions. *arXiv*. https://arxiv.org/abs/2307.02147

Zhang, Z., Wang, F., & Wang, S. (2025). Catastrophic failure of LLM unlearning via quantization. In *Proceedings of the International Conference on Learning Representations*.

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. PublicAffairs.