IEEE-Digital Forrest Transparency Charter, for Global Digital Privcy

Mark Lizar,
Global Privacy Rights, Montreal Quebec, Canada

Abstract

This paper introduces the **Digital Privacy Transparency Forest Charter**, to frame a meta-privacy transparency model, designed to address the urgent need for standardized, enforceable digital privacy governance in the era of ubiquitous surveillance and artificial intelligence. Drawing on centuries-old commons-based legal traditions, the Charter proposes a framework where every act of data processing must be transparently recorded, and where the identity, legal basis, and authority of any data controller must be presented to individuals—by default—before any digital service is used. This information should be either directly disclosed or posted in a public digital transparency registry, ensuring that all stakeholders, including non-personal and offline surveillance actors, are held to a standard of openness and accountability.

The Rationale for a New Charter

The challenges posed by digital surveillance and AI mirror those encountered in the historical development of democratic governance, trade, currency, and banking. These domains, once dominated by unchecked power and secrecy, evolved into transparently governed systems through the adoption of common rules and standards. The Digital Privacy Transparency Forest Charter seeks to catalyze a similar transformation in data governance, advocating for regulated, standardized transparency mechanisms—specifically, notice and consent receipts—that empower individuals and restore trust in digital ecosystems.

Core Principles of the Charter

- **Universal Notice and Consent:**
  Every individual, regardless of context, must receive clear notice before data is processed, enabling genuine consent and the management of permission-based relationships.
- **Transparency as Etiquette and Right:**
  In commons-based societies, providing notice is not only legally required but also a matter of basic etiquette and respect. This principle is embedded in international treaties like Convention 108+ and the GDPR, which recognize transparency and consent as foundational to privacy rights.
- **Meta-Data Governance:**
  The Charter advocates updating analogue privacy practices for the digital age, replacing outdated, context-dependent mechanisms with standardized, interoperable digital transparency protocols.

The Challenge: Outdated Regulation and Entrenched Interests

Most data protection regulations were conceived in an era before the internet, IP addresses, and digital identifiers. These analogue-rooted rules have been entrenched and, in some cases, actively protected from modernization by powerful technology interests—so-called "Techno-Barons." In physical contexts, notice and consent are often inherent and contextually signaled, with clear mechanisms for withdrawal. Online, however, service providers routinely fail to identify themselves, disclose their roles, or seek meaningful consent before collecting and trading personal information. This widespread violation of commons rules and human etiquette has enabled secret mass surveillance and eroded individual autonomy.

In the United States, the response has been to downgrade strong privacy laws to consumer protection statutes, shifting the focus from transparency and proactive rights to reactive remedies after privacy has already been compromised. Regulation has moved from privacy commissions to agencies like the FTC, and laws such as the CCPA offer only the right to opt out of tracking

—by which point the individual is already identified and their data processed. Non-U.S. citizens are left with even fewer protections, highlighting the inadequacy of current frameworks in a global digital environment.

Historical Context: Commons-Based Governance

The Charter draws inspiration from the evolution of commons-based governance, tracing a lineage from feudal lords and barons to the Magna Carta (1215) and the Forest Charter (1217). These historic documents established the principle that even the most powerful actors are subject to common rules, providing security and rights in shared spaces. Over centuries, these principles have shaped constitutions, national charters, and best practices, underpinning the development of the Commonwealth and other democratic institutions. The Digital Privacy Transparency Forest Charter seeks to extend this tradition into the digital realm, ensuring that the governance of personal data and digital identity is subject to the same standards of openness, accountability, and mutual respect.

The Solution: A Digital Forest Transparency Charter

Just as the original Forest Charter provided security and rights in physical commons, the Digital Forest Transparency Charter aims to secure individual rights in digital spaces. It calls for:

- **The Right to Choose Identification:**
  Individuals must have the ability to decide when and how they are identified online.
- **Control Over Data Benefits:**
  Individuals should have a say in who benefits from their data, ensuring that value generated from personal information is not extracted without their knowledge or permission.
- **Protection of Intellectual Property and Output:**
  The Charter demands protection against the unauthorized use of one's intellectual property, work, or creations—requiring legitimate purpose, permission, consent, license, or contract.
- **Standardized Notice and Consent Receipts:**
  Every digital transaction involving personal data must generate a notice record and a twinned receipt, providing verifiable, auditable proof of transparency and consent.
- **Public Transparency Registries and Data Notary Architecture for Trusted Transparency:**
  Controllers' identities, legal bases, and authorities must be accessible in public registries, enabling oversight and accountability across jurisdictions and technologies.

Broader Implications

By establishing a universal standard for digital privacy transparency, the Charter seeks to:

- **Restore Trust:**
  Rebuild trust in digital services by making data processing visible, understandable, and controllable by individuals.
- **Enable Effective Regulation:**
  Provide regulators with the tools and evidence needed to enforce privacy rights and hold violators accountable, regardless of their size or influence.
- **Foster Innovation:**
  Create a level playing field where innovation is not stifled by secrecy or exploitation, but is driven by respect for individual rights and transparent practices.
- **Support International Harmonization:**
  Align with existing international treaties and standards, such as Convention 108+ and the GDPR, to facilitate cross-border data flows while upholding high standards of privacy protection.

Conclusion

The Digital Privacy Transparency Forest Charter represents a necessary evolution in the governance of digital identiicaiton based surveillance, and its used to access and control personal data. By embedding standard digital transparency, notice, and consent as foundational requirements—mirroring the historical role of the Forest Charter in securing rights in common spaces—it offers a practical, principled framework for navigating the challenges of surveillance, AI, and the digital economy. The Charter calls on policymakers, technologists, and civil society to adopt and enforce these standards, ensuring that the digital commons remains a space of safety, dignity, and shared benefit for all.

contact mark@globalprivacyrights.org

References

- Article 29 Working Party, "Guidelines on Transparency under Regulation 2016/679"
- Council of Europe Convention 108+ (2025)
- EU General Data Protection Regulation (GDPR)
- EU Data Protection Regulation (DPR)
- Quebec Law 25 (2023)
- ISO/IEC 29100:2024 interoperable security and privacy framework
- ISO/IEC 29184:2020 Online privacy Notice and Consent
- ISO/IEC 27560:2023 Consent record information structrure
- ISO/iEC 27564: Privacy protection — Guidance on the use of models for privacy engineering
- ISO/IEC 27091 (Working Draft)
- W3C Data Privacy Vocabulary (DPV)
- ISO/IEC (Proposed) Canadian International Notice Record and Receipt information structure profile
- California Consumer Privacy Act, California Civil Code Section 1798.100, enacted January 1, 2020. Available at: California Department of Justice
- Kantara Initiative ANCR Transparency Performance Indicator Report (TPI-R), https://kantara.atlassian.net/wiki/spaces/WA/blog/2025/02/14/875200525/ANCR+WG+Introduces+Transparency+Performance+Indicator+Benchmark+for+Valid+Consent+to+Identification
- European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
- OECD. (2025). Enhancing Access to and Sharing of Data in the Age of Artificial Intelligence. Retrieved from www.oecd.org

Annex Meta Privacy Model for Glassbox Data Governance consists

The Model consists of,

1. Digital Privacy Forrest Charter for Transparency
2. Convention 108+ transparency as the privacy policy standard, (or code of conduct)
3. EU DPR (Mirrors the GDPR) - for Lawful Access and Consent (common/code of practice guideance)
4. ISO/IEC 29100 privacy framework as international standard which is free and open to access, required for transparency based interoperability
5. ISO/IEC 27560 consent record information structure, with the proposed Canadian-International Notice and Consent Record Structure Profile

6. National/Regional implmenetaiton of Commonwealth Adequate Rules