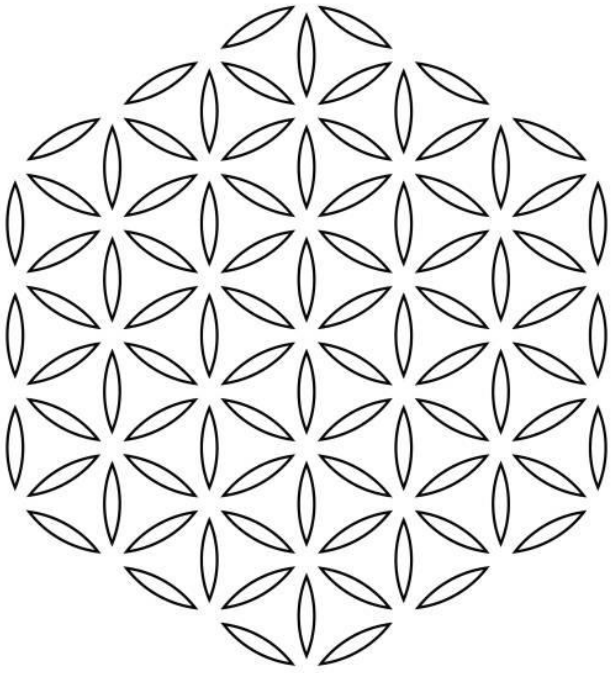
New Internet Common

EXTENDING THE MAGNA CARTA FOR DIGITAL PRIVACY TRANSPARENCY & CONSENT



V0.9.3: 24-12-2023

With good will for peace on earth through goodwill for all

This paper written for IEEE Digital Privacy Group

Digital Transparency Lab

ABSTRACT

There is a lot that is divisive about technology, it can be very isolating in its use, dis-intermediating the individual in context of it's use in invisible, often secret ways. In a globally accessible, media driven society where politics and information are often mis represented, with intent and bias. Digital Privacy Transparency (DPT) and the International ISO standards for digital notice and consent records, is what enable privacy to scale into digital privacy.

This paper introduces a digital common revealed with transparency and capable of digital consent. Introducing inclusive public privacy and cyber security with internet scalable data privacy vocabulary, digital law, and evidentiary privacy receipt standard for consent tokens. Embedding proof of knowledge, digital security, and privacy expectations in the governance of all digital interactions.

Transparency, notice, and consent is not currently connected to the operation of computer systems and their permissions by default. Instead they are static, non-dynamic, un-standardized and ultimately analogue privacy transparency tooling, outdated, in-sufficiently high risk for data protection and cyber security.

With international privacy and security, now is finally the time to enable the virtual and data driven digital realm to be governed with systems that respect, connect, enhance people and society. Where inclusion and provide of the physical rules, cultures, and capacities of people are embedded in data governance.

Over 40 years of international collaboration has produced a single international privacy regulatory framework through the development of international guidelines and standards. Standards matured through consensus in ISO/IEC JTC1 WG5, called 29100 Security and privacy standard, is used globally, developed with 51 participating countries and in conjunction with Council of Europe, Convention 108, the General Data Protection Regulation, and most significantly in 2024, Council of Europe Convention 108+, is expected to be ratified by a majority of countries in to law that is enforced.

Internationally harmonized privacy laws and standards, developed from the Commons, for the Commonwealth, comprised of 56 nations and 2.5 billon people.[1] Representing the scope of the new internet common for digital-enlightenment and collective digital wealth.

[1] The Commonwealth, Member Countries, [internet dec-23] https://thecommonwealth.org/our-member-countries

Digital Transparency Lab

Digital Transparency Lab

The Human Condition

Through our physical experience we reveal aspects of ourselves when engaging and communicating with others, this is captured in ways that increasingly are surveilled and tracked digitally. Without respect to the human condition, that transborder governance society requires for a common set of rules, standard and reliable practices, are required.

To confidently share personal details and trust the scope of this disclosure, for a specific purpose, data governance needs to be accessible regardless of the context, offline or on.

Digital Privacy requires security for the human condition, it requires transparency that is open, standardized clarity over the scope and breadth of digital surveillance in context.

Human Trust requires transparency to see and use consent-based controls, which an individual can trust, verify and self-validate as secure. Digital autonomy it's human entitlements, expressed as human rights are not a new topic.

Physical vs Digital; Privacy Transparency

Physical, analogue based privacy regulation were drafted when privacy was physical, paper based and face to face. Files needed to be kept confidential and secure, including access control, and this governance ported nicely to the mainframe computing environment.

Analogue privacy laws were written from best practices for physical privacy context, requiring data protection and minimization. Principles and privacy regulations to govern paper-based contexts were not written to govern digital privacy. It has been left up to services to innovate policy, while it has taken 40 years to develop enforceable privacy regulation and interoperable technical standards for digital privacy transparency to scale transborder.

For example, analogue privacy regulation is defined as "Data Protection", in which it is expected that personal data will a) be required b) that disclosing the data requires physical copy and transfer of data, c) that physical processes are required for privacy controls.

As a result, online today, no one controls their own records of digital relationships. Instead, cookies, rather than a consent receipt, track our personal information preferences and not for our benefit.

For most services online, people are required to create a 'username' and 'security profile' to identify themselves digitally, before access to services is granted, even without logging in identifiers are created by each service to track the service 'user'.

The most challenging component of data protection law is the analogue notice and transparency process that have not governed micro-data, referring to identifiers and related attributes services create to monitor and surveil by default. For example, providing digital services a 30 day response time to privacy information and access requests.

Digital Transparency Lab

Dynamic Data Control requires, reciprocal transparency, not provided with a term and conditions based agreement. Rather than privacy law, the interest of the business supersedes that of the individual, privacy is not treated as a right. In this data control architecture an individual, must ask 'permission' for their data to be deleted, accessed and managed. (thus the obligation is on the individual to govern the services permissions) rather than managing privacy with consent.

Digital privacy transparency has long since evolved past the 'clear and plain language requirement now. In Convention 108+ a record of processing activities, (Article 3) requires a record to be created, and consent requires a receipt, for the individual to be included. Clear language is not the only transparency modality required and alone is not suitable to scale digital privacy as a standard people can expect.

Anthropology of Common Consent

Throughout history, 'the common' approach, or method has represented our collective shared approach to governance of common resources. Central to public capacity for engagement and cultural expression is the space to express our collective selves in.

These spaces hold a significant place in the annals of our shared human experience, serving as a cradle for societal development. The Commons as a shared concept is extended with 'common law', evolved through case-by-case interpretations and collective iterations. Over time, we have co-created an infrastructure that embodies a shared authoritative history, of common law, with civil law and administration. This data infrastructure is used so that we are free to pro-actively govern our own common spaces, encapsulating human protocols and common sense, to foster commonwealth within shared engagements.

The whole is greater than the Sum of its Parts[2]

[2] Aristotle, 350 BCE "Meta-Physics"

As society developed greater common sense, extending beyond basic rules of thumb, this progress fueled a trust in the public's capacity to innovate. This trust has propelled generations of evolution and iteration, traces to the utility of the many working as a whole.

The Magna Carta and Forrest Charter, where a written record of rules were engineered the authority to govern common space and the rights (like consent) to use them,

In 1215, Magna Carta,[3] was published, accompanied by the Charter of the Forest in 1217,[4] both were used together to set precedent for public access and the rules for common stewardship of shared resources. This model of governance spread throughout the English-speaking world represented in principle in various constitutions. These documents, historical charters, are foundational for establishing common law that is enforced, which is crucial for governance in society.

The 1215, agreement between King John of England and his barons provided the foundation for English common law, which spread throughout the English-speaking world. Magna Carta is the first example of a king of England consenting to written limits on his power drafted by his subjects. The Magna Carta (or Great Charter) informs the legal system in English Canada, and the Canadian Charter of Rights and Freedoms.[5]

The Magna Carta was accompanied by the Forest Charter, which provided the commoner with the right to forage, hunt and eat off of crown land. Without formalizing this right to natural resources, the commons provided little food security.

The Magna Carta was accompanied by the Forest Charter, which provided the commoner with the right to use common land to forage and hunt. Without formalizing this right to natural resources, the commons provided little in security.

In Clauses 39 and 40 and the accompanying Forest Charter that granted people common rights to use crown land, actively laid the foundation for these principles.

> *Clauses 39."No free man shall be seized or imprisoned, or stripped of his rights or possessions, or outlawed or exiled, or deprived of his standing in any other way, nor will we proceed with force against him, or send others to do so, except by the lawful judgement of his equals or by the law of the land."*
>
> *and*
>
> *40: "To no one will we sell to no one deny or delay right or justice.*[6]

3 Harris, C. (2015). Magna Carta. In *The Canadian Encyclopaedia*. Retrieved from https://www.thecanadianencyclopedia.ca/en/article/magna-carta

4 Harris, Carolyn. "The Charter of the Forest". *The Canadian Encyclopaedia*, 29 April 2015, *Historical Canada*. www.thecanadianencyclopedia.ca/en/article/the-charter-of-the-forest. Accessed 18 November 2023.

5 Foot, R. (2020). Canadian Charter of Rights and Freedoms. In *The Canadian Encyclopaedia*. Retrieved from https://www.thecanadianencyclopedia.ca/en/article/canadian-charter-of-rights-and-freedoms

6 Harris, C. (2015). Magna Carta. In *The Canadian Encyclopaedia*. Retrieved from https://www.thecanadianencyclopedia.ca/en/article/magna-carta

The establishment of legitimate authority to both protect democracy and enable mechanism for collective wealth is intertwined with epic tales of human adversity, battles for freedoms, autonomy, and the collective will of societies often has been required to evolve governance. While concepts like rights, justice, and freedom may easily be prescribed, their enforcement has historically been a challenge addressed with civic engagement.

Human rights, as we understand them today, can trace their origins to the Charter of the Forest, which first granted commoners the right to access and forage in the commons with the consent of the King.

This charter was almost unique in providing a degree of economic protection for free men who used the forest to forage for food and to graze their animals. it restored to the common man some real rights, privileges and protections against the abuses of an encroaching aristocracy. In this way standards for digital privacy transparency as well as records of consent represent a Charter to immortalize an authoritative consensus, to establish rights of access to resources, to forage for a Common resource.

The modern 'Forrest Charter' is likely best embodied in the 1948 Universal Declaration of Human Rights[7] as it first lays the foundation for rights to physical security and analogue privacy.

> *Everyone has the right to life, liberty and security of person.*
>
> *Article 3*

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*
>
> *Article 12*

In 1967, the Helsinki Declaration, published by the World Medical Association, significant milestone setting the standard for knowledge, transparency and what has been defined as informed and explicit consent, in 1with creating a gold standard for informed consent, and as a result has set the international adequacy bar for informed and explicit consent that has become the legal baseline for what is understood as valid consent today.

In this Declaration, the fundamental principle of respect for the individual is defined in (Article 8), his or her right to self-determination, and the right to make informed decisions[8] subsequently defined in (Articles 20, 21, and 22). Most notably,

> *The participant's welfare must always precede the interests of science and society (Article 5).*

[7] United Nations, Dec 10, 1948; 'Universal Declaration of Human Rights' [Internet] https://www.un.org/en/about-us/universal-declaration-of-human-rights

8 Informed Consent, Wikipedia [Internet] https://en.wikipedia.org/wiki/Informed_consent

Foundation of a Common Internet

The foundations are evident, when the USA was first formed the concept of common governance traces back to four of the early states, and three of the initial thirteen states, thereafter, beginning with; Virginia, Massachusetts, Kentucky, and Pennsylvania - which literally incorporated as a 'commonwealth' and related principles into their constitutions.

"According to the Massachusetts State Government, the term "Commonwealth" was incorporated into their constitution in 1780 and was used to express the ideal that "the people [of Massachusetts] ... form themselves into a free, sovereign, and independent body politic, or state."[9]

Subsequently, the rights of the free were entrenched for US citizens, notably through the 1791 Fourth Amendment, which safeguards American's rights against unreasonable searches and seizures, underlining the cornerstone of physical privacy and its security.

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Today, the expectation of privacy requires common governance, co-regulation, that which has evolved from the Magna Carta, been embedded in constitution, remains a crucial foundation for understanding the societal governance infrastructure we use to trust in each other. Physically security and control anchor our physical trust, through its extension into network technologies and used socially.

Just as the Magna Carta marked the end of despotic rule in 1215, today's challenge is to address the violations of digital commons by services like Facebook and Google, where digital surveillance has become challenging to govern, in the absence of digital transparency and consent.

To adapt these principles to the digital age, we require international instruments to be interoperable, and standards that people can themselves operate, legally enforce to co-govern digital public spaces.

Evolution Privacy Rules

By the mid-1970s, privacy and data governance focused first on central database access. During this decade, the mainframe became widely used and in 1973 the USA developed robust privacy and security practices, in the form of the Fair Information Practice Principles (FIPP), which were used as a cornerstone for national

[9] Why States Are Called Commonwealths, 2019, Business Insider, https://www.businessinsider.com/why-states-are-called-commonwealths-explainer-2019-1?op=1#the-commonwealth-states-1

privacy regulations in the commonwealth and eventually industry best practices became international security and privacy standards.

Principles and best practices contributed to the 1980 OECD Guidelines on the Privacy of Transborder Data Flows, which later influenced the development of the ISO/IEC 29100 security and privacy standard, building upon the ISO/IEC 27001 security framework.

This socio-economic and legal innovation led to the creation of the Council of Europe's Convention 108, which became the first legally binding international instrument in data protection. Opened for signatures on January 28, 1981, it is now celebrated annually on the same day as International Privacy Day.

The OECD Guidelines were formally internationalized when internet growth started to skyrocket, in 1999 when European countries were allowed to join the convention upon implementing national legislation. Fifty-five countries in the Commonwealth later ratified this by enacting similar regulations.

In 2018, the General Data Protection Regulation (GDPR) came into force, over the next years several states in the USA pass privacy legislation.

Finally, in 2024, the Council of Europe Convention 108+, will come into force with the international framework, that largely mirrors the GDPR, for digital privacy transparency standards to be enforced internationally.

Privacy Records and Digital Consent Receipts

Privacy rules in the analogue world evolved with social governance and formalized with records. These methods included notarization, signatures, witnessing signatures, and similar practices, which, over time, have honed good and common practices.

Although these mature practices have not immediately been adopted in digital systems, the digital credential like commercial paper provide a secure vehicle for value based assets.

The earliest physical artifact known as a transaction *Receipt* dates to 5000 BCE, representing the earliest form of written script.[10] This receipt likely played a crucial role in boat-based goods transfers, allowing recipients to actively verify the accuracy of the delivered goods against their payments. This form of peer-to-peer trust technology minimized friction in third-party exchanges, fostering greater trust in trade. Such advancements facilitated economic growth across distributed geographic areas by making the exchange of goods more reliable and widespread.

[10] The Oldest Writing Ever Discovered Was an Ancient Receipt! (A Brief History of Receipts) https://hec.com/blogs/hillside-university/a-brief-history-of-receiptshttps://hec.com/blogs/hillside-university/a-brief-history-of-receipts

Photo: An ancient Mesopotamian receipt in Cuneiform, conveying the language of Akkadian (source: thebiblicalreview.wordpress.com)

The first notarized receipt replace a physical transfer of gold, recorded in a banking ledger dates to medieval times. While pin-pointing its exact date is challenging, evidence suggests it originated from early 14th-century Florence.

This innovation significantly enhanced (by more than tenfold) the security and efficiency of gold exchanges between Florence and Paris. Combining notarization, and receipt technology to secure the value of a currency in a commercial paper. With this new record system, the need to physically transfer gold, vulnerable to robbery, was eliminated. A single trusted intermediary could conduct transactions more quickly and with less risk, eliminating the need to transport heavy gold between cities. This advancement greatly expedited business dealings and improved the overall security of these transactions.

Digital Privacy for Common Expectations

As the result of 42 years of security and privacy standards development, best practice have become harmonized with Convention 108+ and the GDPR. The baseline for what to expect is clear, inclusive, comprehensive and provides governance framework for all stakeholders to use.

Its up coming enforcement is evidenced by the $1.2 billion-dollar fine imposed on Meta (Faceboo) on May 23,[11] 2023. This fine marks a pivotal moment in officially recognizing the 'I Agree' checkbox as insufficient for legal consent to ones identity(face), especially for secondary purposes like behavioral advertising. Such deceptive practices, often termed as consent fatigue is a 'dark pattern' technically, in fact this is a notice pop-up called 'permission fatigue', fraudulently represented as consent. As this is dominant process online today, this means that most (if not all) data processing online is without valid consent.

In response to this challenge, the European Data Protection Board (EDPB)[12] has introduced new legislation under the Digital Governance Act, the Digital Services Act, and the Digital Markets Act. The Digital Service Act enforce data sovereignty rules, on platform service providers across the EU starting March 16, when it comes into effect. And in this way, tackle deceptive digital privacy transparency

[11] EDPB, May 22, 2023, 1.2 billion euro fine for Facebook as a result of EDPB binding decision [Internet] https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

[12] EDPB European Data Protection Board: Established 2018, To ensure that the General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive are consistently applied in the EU countries, as well as Norway, Liechtenstein and Iceland.

practices, replacing privacy policies with privacy law to establish public, open, standardized and regulated, Digital Privacy Transparency.[13]

Digital Consent

Our own consent record, our personal digital memory, is a capture of the objective legal context relative to individual understanding of consent, whether consent is valid or not, and whether consent (or lack thereof) is informed from the default state of consent. AKA is digital privacy concentric?

Once informed, the individual can then direct consent digitally, in Quebec privacy law, for a secondary purpose. Regardless of what this legal justification is. In this all surveillance and data capture beco,es not only accountable, but digital consent operable. Opening not only data portability, but also data control portability, in which personal data is never transferred across the internet.

The lack of digital transparency, or digital governance that requires records for data processing diminishes the capacity of digital privacy. Transparency over personal data processing, its access and control, just bank records we keep to track money are critical to scale trust. No longer can service providers write their own technical rules, to govern surveillance in ways that monetize various aspects of our digital lives. In a New Internet Common, digital records of processing activities are required for adequacy, and 3rd party logs must be kept for high-risk assurance when data is processed by a third-party Controller without a direct relationship to the data subject.

[13] The Digital Services Act began enforcement in August 2023 and saw immediate action from the Norwegian Data Protection Authority. They imposed daily fines of one million kroner (approximately $97,000) on Meta for non-compliance with consent regulations for behavioral advertising, a practice often associated with surveillance capitalism. The law comes into full force on March 16, 2024.

Digital Transparency Lab

Digital Privacy Transparency must not only extend the security of a Magna Carta, but like in the Forrest Charter, the rights first bestowed for individuals to gain rights in the commons with royal *consent* of the King.

In our collective digital privacy future for real privacy to scale digitally, not only must all data processing be recorded, but it must also be transparent (standardized) with records, filled with clean data capturing the state of consent people can trust. Our own secure digital consent records can then be used to govern the use of our knowledge and all other intellectual property type of assets, intangible values and currencies. Once an individual consent can be digitally secure and authentic then it scales technically.

If advertisements can be delivered to an individual dynamically per session, then digital privacy and consent can work the same way, active state digital privacy transparency. Mis-information and fraudulent representation will become a transparent reputation for everyone to see, as we will all have a record of the controller id. So we can. All see the source of information and misrepresentation, compare information, for more and more dynamically operable transparency with our own AI.

Conclusion

People must be able to govern their own digital privacy expectations, to control their own records of relationships to be digitally enlightened.

To accomplish this, standardized digital transparency with records of the state of security and privacy is required to be dynamically operable. The use of notice receipts and consent records to imitate human centric exchange process enable natural interoperable with people. Making Digital Consent, Digital Freedom Technology.

Contributors

- Mark Lizar
- Sal D'Agostino
- Paul Knowles

About 0PN Digital Transparency Lab

Digital Surveillance, Privacy & Consent Standards have been the focus of the research and development culminating in 0PN, digital privacy transparency. 0PN is an evolution of efforts in common's orientated consensus technology, since the Identity & Trust group first started at Identity Commons in 2006. The work evolved the concept of Identity Trust, and Surveillance Registries. into efforts to standardized notice, replace agreements with consent. Iwt ht he Open Notice Initiative in 2012, before finding a home for this work at the Kantara Initiative in 2014.

Where the Consent Receipt v1 was championed, written in conjunctions with ISO 29100 and 29184, to provide an international standard consent record information structure. This has now published becoming ISO/IEC 27560 Consent record information structure in Aug, 2023.

A lot of the work for this is underway at the Kantara Initiative ANCR WG and in the 0PN Transparency Lab, has ben developed through this project efforts over time.

0PN: Digital Privacy Transparency Semantics

- **0PN**: This refers to being open about both a) the legal compliance, b) and conformance of a record to determine the performance in standard way. 0PN = 0pen²
- **Digital**: references specifically cyber security, its data control and protection design gov architecture
- **Digital Privacy** – Consent by Default, surveillance online
- **Digital Transparency** - transparency over the security design and data control defaults, context settings relative to consent
- **Digital Privacy Transparency** – Privacy by design that enables consent by default embeds personal security by design

About ANCR @ the Kantara Initiative

All the invested time and effort from many people, work groups and communities have now evolved into the current Kantara Initiative ANCR WG.

ANCR Roadmap for 2024

- Consensus Collaboration Protocol
- Digital Privacy Transparency Compliance and Conformance Scheme[14]
- PII Controller Notice Credential

[14] ANCR Compliance and Conformance Scheme https://kantara.atlassian.net/wiki/spaces/WA/pages/301564731/ANCR+Digital+Privacy+Transparency+Compliance+and+Conformity+Assessment+Scheme

- ANCR Record information structure[15]
- AuthC: Digital Identifier Exchange and Interoperability Protocol for Authorization from Consent
  - Consent Receipt v2, Consent Tokens

[15] https://kantara.atlassian.net/wiki/spaces/WA/pages/304480257/ANCR+Record+Information+Structure+v0.7#[inlineExtension][inlineExtension][inlineExtension]Notice-Record-Security

ANNEX: Transparency Code of Conduct (for Digital Consent tokens)

Towards a future of Dynamic Data Governance.

In 2024, 0PN Digital Privacy Transparency project starts hosting a meeting to build a public digital privacy policy. Which will entail a Digital Transparency Code of Conduct for Digital Consent, for Transparency Modalities, Chapter 1 of both GDPR and Conventional 108+, this will be specified with a Digital Privacy Code of Technical Practice, which are specified with the ANCR WG, Specifications, specific to the laws and standards in this document.

To this end, a code of conduct for micro- records, their control, the ability to aggregate these records at the heart of the digital commons, is about ethical and dynamic access to data, legal providence provides the authority that Must be presented, verified, validated, and accountably assured, for digital consent to be validated:

The same Digital Transparency rules for privacy apply to everyone, secret surveillance, break the glass, must be governed, transparent to the regulator and use the front door of democracy.

Equal access to justice, means everyone has a right to be heard, to control their own data, construct their own digital identifiers, be their own data intermediary, not be surveilled without digital privacy transparency that is meaningful and consent by default.

For this code of conduct, 0PN Digital Transparency Lab works on the implementation of a digital privacy transparency code of digital identity practice, where people can go from anonymous, to fully transparent with autonomous personal data control.

BEST 0PN-DIGITAL PRIVACY PRINCIPLES AND PRACTICES

1. All networked data processing requires digital transparency:
    a. all notice, notifications, and disclosures
    b. require a record of processing activity and a consent notice receipt, to be provided, to provide a systematically inclusive identity to enable anonymous/pseudonymous access to digital privacy services.
    c. a notice controller identity to be provided prior to collecting personal data
2. Consent is a human control that an individual can modify to an individual's condition.
    a. Legally, A human manages consent and systems manage permissions.
    b. Consent is specified by the purpose of use for a device or service, not to the technical permissions or related security preferences.
    c. any new purpose for consent is either directed through individual action, or in digital contexts, permission to present secondary purposes for consent is first explicitly provided.
3. Authentication can be provided with notarized, signed and encrypted receipts, used as claims, rather than with the transfer of raw personal information, which according to 0PN Model has 4 levels of digital privacy risk assurance, across 3 vectors of governance.