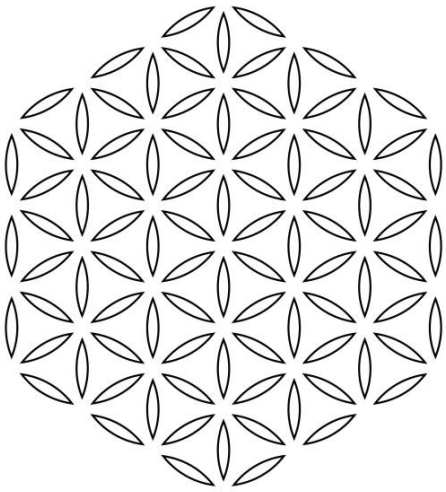
Digital Privacy Magna Carta

Extending the Magna Carta for Consent in the Digital Commons



v1 (draft)

Contributors/Supporters (add name)

- Mark Lizar
- Sal D'Agostino
- Paul Knowles

Digital Transparency Lab

Abstract

Many things are divisive, technology can be very isolating in its use, dis-intermediating the individual in context in invisible ways. In a global media driven society where politics and media are often divisive with intent and bias, digital transparency and standards for making notice and consent records enable privacy, to scale into digital privacy.

This paper introduces a digital transparency and consent commons, as an inclusive public privacy and security framework using internet scalable law and standards for digital privacy expectations to implement human interoperability, with consent as the security control. In Digital Commons, privacy is human and centric to the individual, law is legal centric, and code is defined by privacy and law, not by business and technical centric systems.

However, it is apparent that *virtual and data driven digital realm is not being governed with systems that respect the physical rules, cultures, and capacities of people.* Transparency, notice and consent is not connected to the operation of the systems, instead they are static, un-standardized and ultimately required in legislation to remain an analogue physical privacy tool of outsourced protection.

Which is why, for all of us to be included, digital privacy needs consent to make common sense and consent needs to be first and by default.

A consent receipt (decentralizes) digital governance as a standard, it is a record that people can used to control data and trust the use of PII across public data-spheres.

The Human Condition

Just as in our physical experiences, we reveal aspects of ourselves when engaging and communicating with others in the digital world. To facilitate this, we need reliable methods for identifying others and allowing them to identify and, *with our consent*, observe us.

To confidently share personal details and experiences, offline and online, we require privacy measures that scale across human conditions. Trust, established in face-to-face interactions, must extend seamlessly into the digital realm, to ensure robust governance in networked spaces. This

trust hinges on the assurance that personal identifiers are disclosed only with complete transparency and genuine informed consent.

Online proof of notice, and demonstration of knowledge is missing in governance systems today and yet required for Consent to scale beyond a single context. Systems keep no *record of notice for processing* in accordance with consent, and people have no record of digital relationships. than a record of consent, systems have.

Physical vs Digital Privacy

Physical, analogue based privacy regulation was crafted 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 first to access online service, even without logging in device id's web/wallet browsers, plugins and extensions, along with social media, track the 'user' for the service. Each identifier, and its attributes, give away elements of digital privacy in invisible ways, to first access an online privacy service.

The most challenging analogue component of data protection law is that it assumes services already have personal data, and it provides for services to have 30 days to respond to privacy access and information requests. Reciprocal and dynamic data control and transparency is not required, while a service might have instant access to personally identifiable information. Hence now, people must ask 'permission' for their data to be deleted.

There are no standard protocols for notice, notification, and disclosure, although all privacy regulation requires notice to be presented at the point of collection.

Digital Transparency Lab

Plain and clear language, as the only transparency requirement and it specific to physical privacy with analogue transparency mechanisms, which as a result is not digital privacy operational in the contextual use of the service.

Fundamentally a gap that digital privacy transparency and records of consent address by establishing proof of knowledge and evidence the providence of consent. In Digital Privacy, standardized records of processing activities mirrored with consent receipt, imagines a system in which data is minimized inherently in a receipt, that is encrypted as a credential required for the use of data, according to purpose, even after data is shared, disclosed and copywritten.

<snip> <snip>

Anthropology of Consent in the Commons

Throughout history, 'the commons' have represented our collective shared spaces, central to public engagement and cultural evolution. These spaces hold a significant place in the annals of human experience, serving as the cradle for societal development. The commons as a shared concept are extended into common law, evolving through case-by-case interpretations and collective iterations. Over time, we have co-created an infrastructure that embodies a shared authoritative history. This infrastructure actively regulates our common spaces, encapsulating human protocols and common sense, and aims to foster commonwealth within these shared environments.

Commented [ML1]: Until recently services have not been required to keep track of who's personal data they process, big tech has taken advantage and worked to entrenched very permissive surveillance (e.g. data tracking, disclosure and use practices) that have not been regulated by an individual's consent. Instead, they have been un-regulated, governed by terms and conditions, unique to each provider, they can change any time are take it or leave it, assume consent has already been provided and accompany a privacy policy that is vague, and contract based, rather than specific to implementing privacy regulation.
Digital Commons Consent, is assured with privacy regulation and ISO/IEC security and privacy framework standard (ref) to make interoperable records of processing activities, which are mirrored as consent receipts. Just like a transaction receipt, which is inclusive of everyone, a consent receipt is created a logged and provided to everyone. All notice, notifications and disclosures required a receipt. The receipt can then be reused as a digital credential and identity claim where its use inherently minimizes data and reduces relying party liability. Key pair management for signing credential and encrypting tokens provide a secure exchange format for digital consent

Digital Transparency Lab

The whole is greater than the Sum of its Parts[1]

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 back to 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,

The Magna Carta,[2] accompanied by the 1217 Charter of the Forest[3] set a precedent for public access to and for common stewardship of shared resources. Which became a model of governance for English-speaking world. These historical charters are foundational for establishing a legal framework to govern common law and are crucial for scaling governance and 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.[4]

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

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

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

[3] 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.

[4] 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

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.[5]

The establishment of legitimate authority to enforce and protect democracy to enable commonwealth is intertwined with epic narratives of human struggles for freedom, autonomy, and the collective will of societies to evolve. While concepts like rights, justice, and freedom are easily defined, their enforcement has historically been challenging and requires civic engagement.

Deleted: require

Human rights, as we understand them today, can be traced back to the Charter of the Forest, which first granted commoners the right to access and forage in the commons.

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 and records of consent represent a Charter to access and forage the Common.

Commented [SD2]: to access and forage the commons

The modern 'Forrest Charter' is likely best embodied in the 1948 Universal Declaration of Human Rights[6] as it first lays the foundation for rights to security and privacy.

Article 3

Everyone has the right to life, liberty and security of person.

Article 12

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.

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

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

Digital Transparency Lab

A significant milestone was in 1967 with the World Medical Association's Helsinki Declaration, 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[7] 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).*
>
> *Ethical considerations must always take precedence over laws and regulations (Article-9)*

Modern Foundation of Digital Consent Commons

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."[8]

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 in the commons is derived from the Magna Carta and embedded in many constitutions, remains a crucial foundation for governing trust in each other

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

8 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

physically and by its extension into digital social settings. The modern challenge is to regulate physical and digital common spaces to avoid their misuse. 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 of Internet Governance Frameworks

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 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 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.

Evolution of Internet Governance Transparency: Records and Consent Receipts

Digital Transparency Lab

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 earliest physical artifact known as a transaction *Receipt* dates to 5000 BCE, representing the earliest form of written script.[9] 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.

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

The first notarized receipt documenting a gold transfer recorded in a banking ledger dates to medieval Florence. 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.

[9] 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

Digital Transparency Lab

The Future of Digital Commons Privacy

As the result of 42 years of security and privacy best practice harmonization the international privacy laws and ISO/IEC 29100 interoperable standards for consent can now be implemented and enforced.

Evidenced by the $1.2 billion-dollar fine regulators imposed on Facebook-Meta on May 23,[10] 2023. This fine marks a pivotal moment in officially recognizing the 'I Agree' checkbox as insufficient for legal consent, especially for secondary purposes like behavioral advertising. Such deceptive practices, often termed as consent fatigue is a 'dark pattern' called 'permission fatigue', and is fraudulent consent, which means most data processing online is without valid consent.

In response to this challenge, the European Data Protection Board (EDPB)[11] 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 practices, replacing privacy policies with privacy law to establish public, open, standardized and regulated, Digital Privacy Transparency.[12]

Conclusion

[10] 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

[11] 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.

[12] 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

People must govern their own digital privacy expectations, control their own data, to be digitally enlightened.

To accomplish this, standardized digital transparency over the state of security and privacy is required, and it is functionally required to be naturally interoperable with people, and applied as common protocol so we can instinctively understand its signal. Transparency must be inherent, digital privacy expectations require dynamic data trust between (parties, places, purpose, and we must all be able to see its performance. With our own records we can anchor our own trust, secure ourselves and with consent decide our own risk. Our own consent receipt, is our personal digital memory it presents the objective legal context for consent, if it is valid or not, and with consent by default, be required to validate it, or no matter what the purpose be informed of what the legal authority for the surveillance and processing of data personal data.

Once informed, the individual can provide directed digital consent for a secondary purpose. Regardless of what this legal justification is. In this way opening not only data portability, but also data control.

The lack of digital transparency governance, requiring transparency over data access and control, like we collectively track money in a bank, has enabled services to write their own data surveillance rules to monetize various aspects of our digital lives. Which is why the International Common's, privacy laws require a Records of Processing Activity, and Data Privacy Officers that keep 3rd party processing logs, when data is processed by a third-party Controller in another legal jurisdiction.

A Digital Privacy Framework must not only extend the security of the Magna Carta, but like in the Forrest Charter, the rights first bestowed for commoners wealth with royal consent. In the digital privacy future for privacy to scale digitally, not only must all data processing be recorded, but it must also be transparent (standardized), and an individual requires their own records, and source of knowledge to trust and control the state of consent. Secure digital consent can then be used to govern 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 scale technically.

If advertisements can be delivered to an individual dynamically per session, then digital privacy and consent can work the same way. Digital consent is conformance and compliant address digital challenges around providence. For example, mis-information and fraudulent representation will become transparent, a reputation for everyone to see, as we will all have a record of the controller id, and we will all be able to see the source of misinformation and misrepresentation, compare information, for more and more dynamically operable transparency.

<snip>

Commented [SD3]: Was the Magna Carta about security? More about access no?

Commented [SD4R3]: Access to rights for the common wealth.

Commented [ML5R3]: More Security of the state – as oppose to security for the person to live

Commented [ML6]: (a token suite) that notarize, authorize, authenticate, account for, and administrate for the individual at scale.
The design and architecture for this has to be consent by default> , With this digital privacy expectations scale consent, not run counter to it. These expectations can then provide a basis for anyone when applied to the Digital Commons.

Digital Transparency Lab

Next Steps: Transparency Code of Conduct for Digital Consent

Towards a future of Dynamic Data Controls Governance.

A code of conduct must provide a record to prove the legal providence in order for digital consent be put in place, based on current laws and standards it includes:

1. All processing requires digital transparency:
    a. all notice, notifications, and disclosures
        i. 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.
        ii. 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.
3. Consent is specified by the purpose of use for a device or service, not to the technical permissions or related security preferences.
    a. 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.
4. 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.

Next generation consent is a digital record, a legal notary, for authentic, authoritative and notarized receipts. These records are the critical component for social-economic micro-data trust, with emerging standards for digital credentials, and their use to sign receipts so they can be used as micro-claims. Providing people with the power to be the issuer and reverse the data control paradigm.

Consent by default addresses providence security and enhances cyber security address common digital privacy challenges by encapsulating PII in consent tokens, this way those most knowledgeable and motivated can use cyber security and manage their own data control.

0PN Labs is working with Surveillance Trust Registry (to create a token suite) that notarize, authorize, authenticate, account for, and administrate consent for the individual to administrate at scale.

Digital Transparency Lab

About 0PN Digital Transparency Lab and the Kantara Initiative

The 0PN project first started as a work group at Identity Commons in 2006, the work evolved into Identity Trust, Surveillance Trust, and then the Open Notice Initiative, before finding a home at the Kantara Initiative in 2012, before becoming adopted as a ISO/IEC Standard in 2023.

A lot of the work for this is underway at the Kantara Initiative and in the 0PN Transparency Lab, with a Roadmap to Launch 0PN.ORG Digital Commons Privacy Policy, Transparency Index and open source PII Controller Credential for Commons Registration, March 2024.

Kantara ANCR WG - Digital Consent Standards

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

The Roadmap for 2024, continues development on digital commons standard infrastructure with consent by default specifications for digital privacy transparency.

- Digital Privacy Transparency Compliance and Conformance Scheme[13]
- PII Controller Notice Credential
- ANCR Record information structure[14]
- AuthC: Digital Identifier Exchange and Interoperability Protocol for Authorization from Consent
    - Consent Receipt v2, Consent Tokens

Get involved @0PN,

<snip>

of one million kroner ($97,000) per day of non-compliance under an order issued by the Norwegian data protection agency Datatilsynet. https://techxplore.com/news/2023-08-meta-behavioral-norway.html

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

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

Commented [ML7]: Abstract
What we collectively call "humanity" – in as much as it marks the extent of our lived experiences – our diverse languages, cultures, societies, laws, arts, industries, histories, and myriad ways of life throughout the ages, has evolved and adapted within an overwhelmingly *physical and material* realm.
However, it is apparent that *virtual and data driven digital realm is not being governed with systems that respect the physical rules, cultures, and capacities of people.*
Transparency, notice and consent is not connected to the operation of the systems, instead they are static, un-standardized and ultimately required in legislation to remain an analogue physical privacy tool.
Which is why, for all of us to be included, digital privacy needs to make common sense.
Digital Privacy Transparency and personal data control is the human governance and trust framework presented in this paper, it is for humans and refers from an individual's self-expressed identity and engagement in the digitally public data-sphere. ** Old **
Introduction
Many things are divisive, technology can be very isolating in its use, dis-intermediating the individual in context in invisible ways. In a globalized media driven society where politics and media are often divisive with intent and bias, digital transparency, and standards for making notice and consent records enable privacy, to scale into digital privacy.

This paper introduces digital transparency and consent commons, as an inclusive public privacy and security framework using internet scalable law and standards for digital privacy expectations to implement human interoperability. In Digital Commons, privacy is human and individual centric, law is legal centric, and code is defined by privacy and law, not by business and technical centric systems.
Digital Privacy in the Digital Commons focuses on the use of standardized digital transparency (notice and consent) records. Specified with the appropriate international standards that implement a public privacy transparency and record management program, all stakeholders can use for governance interoperability in an international 'Commons'.
A digital privacy transparency governance model that plugs all the digital holes, in the privacy bucket, would require a record of processing activity for every digital privacy notice, notification and disclosure to be provided as a digital privacy receipt by default.