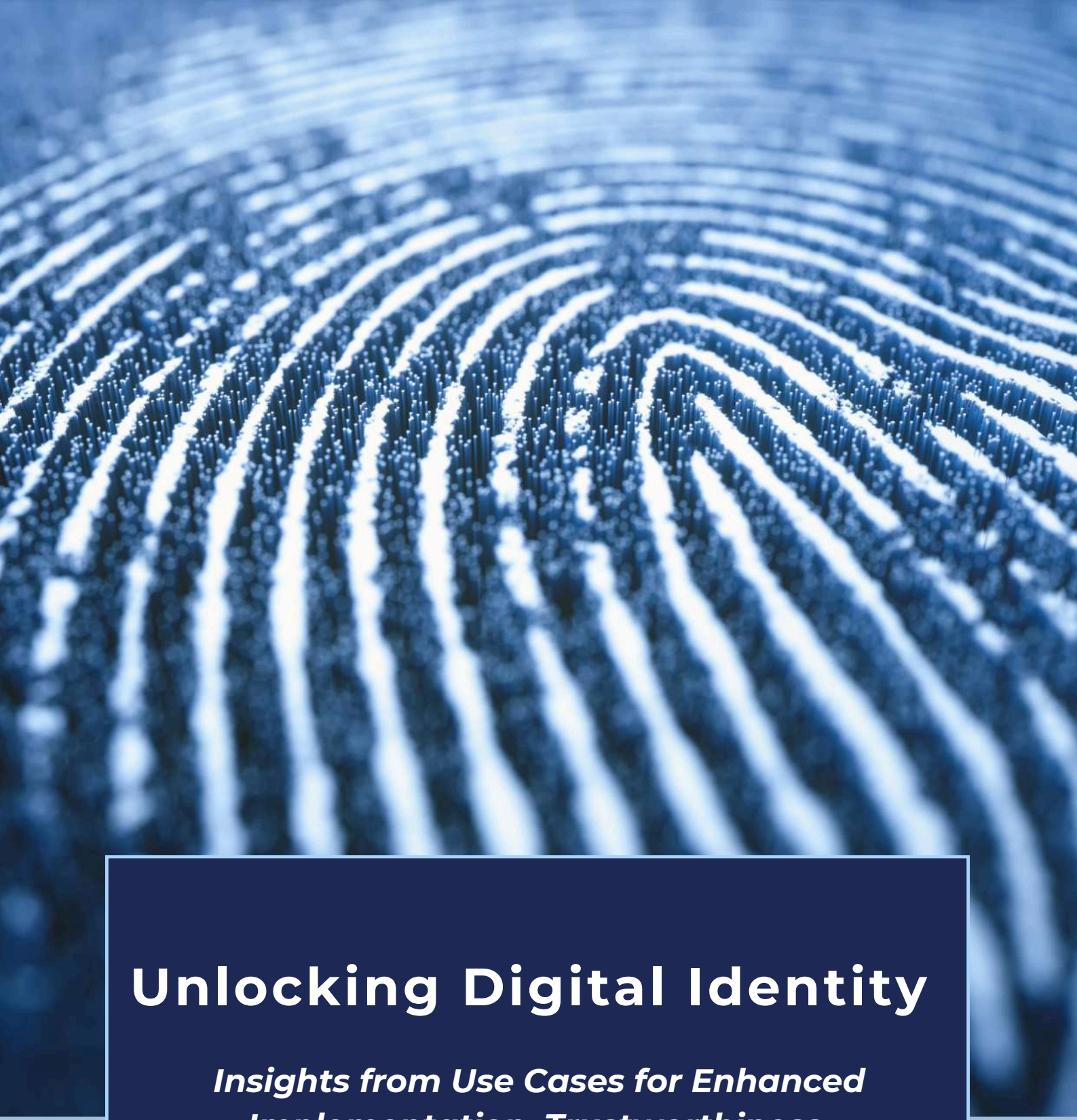


Unlocking Digital Identity

Insights from Use Cases for Enhanced Implementation, Trustworthiness and Individual Empowerment

HTF HUMAN TECHNOLOGY FOUNDATION

JULY 2024

SUMMARY

INTRODUCTION

In an era where digital identity (Digital ID) systems are becoming a cornerstone of accessing the digital economy, public services, and online connectivity, the pressing need to ensure these systems are implemented with a high degree of trustworthiness and empowerment for individuals cannot be overstated. As public and private sectors stand on the cusp of major infrastructural decisions regarding Digital ID technologies, the implications of these choices extend beyond the technical and financial, touching on profound ethical and socio-economic dimensions. These decisions will ultimately shape the openness and inclusiveness of our digital economies.

As we navigate this complex terrain, the insights and recommendations offered by this report aim to guide multiple stakeholders — from policymakers and technology providers, to end-users and society at large — towards realizing the full potential of Digital ID systems. In this report, we delve into the intricate web of challenges and opportunities presented by digital identity systems, by focusing on a series of four critical use cases:

- online protection of minors,
- health,
- electronic voting,
- and authentication of content created by generative AI systems.

This study – based on collaborative efforts of an international working group of policy, legal, technology and identity specialists – not only unveils specific unresolved problems within these domains but also furnishes targeted recommendations aimed at enhancing the reliability and individual-centric nature of Digital ID systems.

This report builds upon the conclusions and recommendations of a previous report of the Human Technology Foundation, published in conjunction with the Digital Identity and Authentication Council of Canada (“DIACC””), “Universal Digital Identity Policy Principles to Maximize Benefits for People: a shared European and Canadian perspective”[1]. Therein, the following set of policy design principles were defined to help guide the optimal development and implementation of digital identification policies:

1- Digital identity policy must be people centered

- Digital identity must be **inclusive**
- Digital identity adoption must be **voluntary**
- Digital identity must be **resilient**
- Digital identity policy must be **intuitive for both institutions and people**
- **Privacy** must be central to digital identity policy

2- Digital identity policy must foster empowerment

- Digital identity must be **user-controlled**
- Digital identity must be based on **informed consent**
- Digital identity must allow **data portability**

[1] Maximizing Benefits of Digital ID_Report

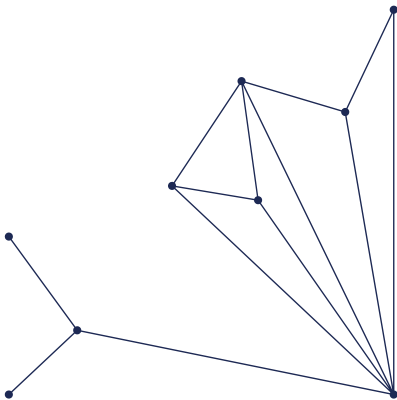
3- Digital identity policy must encourage trust through governance

- Digital identity must be **transparent**
- **Accountability** for digital identity use must be well defined
- Digital identity policies require **security**
- Digital identity must encourage **interoperability**
- Digital identity policy must be **future-proofed** by focusing on desired outcomes
- Digital identity policy must be developed and evolved to **strengthen public and private dialogue**

Set against these principles, the previous HTF/DIACC report found that efforts to deploy digital identity solutions are hindered by a pervasive sentiment of ambivalence and distrust regarding digital identity. If we are to take full advantage of the potential of digital identity to unlock access to services, users must be convinced that digital identity can be used to increase the security of individuals' digital footprint and provide them with an enhanced sense of agency and autonomy in a digital world.

The detailed, use-case based findings presented here underscore a critical juncture in our journey towards a digital future. They reveal a landscape rife with challenges ranging from safeguarding minors in the digital realm to ensuring the integrity of our democratic processes and personal health data. Yet, within these challenges lie unparalleled opportunities to foster a digital environment that is secure, inclusive, and respects the rights and freedoms of all individuals.

By addressing the nuanced implications of digital identity in our increasingly interconnected world, we embark on a path towards a future where digital identity serves as a foundation for empowerment, trust, and the protection of individual rights in the digital age.



METHODOLOGY

The purpose of this report is:

- to highlight issues relating to the use of digital identity systems in four selected areas of study identified above (online protection of minors; health; electronic voting; and authentication of content generated by AI);
- to highlight benefits that can be derived from the use of digital identity systems;
- present the recommendations of the working group on how to address issues where possible and maximize the benefits identified.

To achieve this purpose **the Human Technology Foundation (HTF), with financial support from Project Liberty Institute** gathered a working group of international advisors including several members of the International Technology Law Association (iTechLaw) to research and analyze several use cases divided among four different areas.

Overall, about twenty international use cases of digital identity systems were compiled, researched, and analyzed by the group as a starting point. The aim of this preliminary work was not to deliver an in-depth study or assessment of each of the use cases, but rather to provide to the working group a source of data to feed into the overall reflection. A brief description of each of the use cases studied is appended to this report.

Findings were refined and augmented through specialist interviews, working group discussions and collaborative contributions to this report's authorship.

For each of the four use case areas, the report below outlines the context and current state of digital ID; identifies issues and benefits for each area; and makes recommendations – applying principles identified in the introduction – to maximize benefit and address issues.

WORKING GROUP

Eric SALOBIR
Chairman of the Executive Committee,
Human Technology Foundation

On behalf of the Human Technology Foundation I would like to thank everyone involved in this study and especially our partner Project Liberty Institute which provided us with the financial support to complete this report.

I would particularly like to thank our long-standing partners involved in this digital identity working group: **Thalès, McCarthy Tétrault, EY** and the **La Poste** group.

I would also like to thank **Grimaud Valat**, the project leader and senior advisor to the foundation, Fabien Toux, Charles Morgan, Jen Mossop Scott and the I Tech Law network for their expertise.

Grimaud VALAT
Project leader, senior advisor

Human Technology Foundation

Lawyer, Partner

DMTV Avocats

Fabien TOUX
Project manager, content and events

Human Technology Foundation

François BEDARD
Senior Development Officer,
DIAAC

Jade BUCHANAN
Partner,
McCarthy Tétrault

Régis CHATELLIER
Head of prospective studies,
CNIL

Candice DAUGE
Head of Digital Identity and services,
Docaposte

Michelle DE MOOY
Director of Tech and Public Policy,
Georgetown University

Kristan FOSS
Partner,
Bull & Co Advokatfirma AS

Marie GARNIER
Founder and Partner,
MaG Consulting

Claire GODRON
Digital Identity & Onboarding,
Thalès

Doron GOLDSTEIN
Partner,
Withers Bergman LLP

Charles MORGAN
Partner,
McCarthy Tétrault

Jen MOSSOP SCOTT
Partner,
EY

Nikhil NARENDRAN
Partner,
Trilegal

Gilles ROUVIER
Founding Partner,
Lawways

Wendy SELTZER
Principal Identity Architect,
Tucows

Trish SHAW
CEO and Founder,
Beyond Reach Consulting Ltd

Elvira TULVIK
Partner,
Magnusson

1

AGE VERIFICATION AND PROTECTION OF MINORS

We commence this report with a use case that highlights both the promise of digital identity and the profound ambivalence and distrust that many people feel about digital identity into focus. It is a use case that underscores both how digital identity can be used to protect certain vulnerable individuals (minors) from harmful content, but also highlights the discomfort that many have expressed about how digital ID could be used to surveil some of our most sensitive, intimate, online interactions.

Many jurisdictions around the world have adopted (or are currently considering adopting) legislation that prohibit access by minors to harmful online content, such as pornography [2]. However, even where such laws are in place, they are rarely, if ever, enforced. The "disconnect" between stated society values (as reflected in such child protection legislation) and the reality of laissez-faire enforcement has resulted in a situation in which "adult content" is almost universally available and widely consumed, often for free.

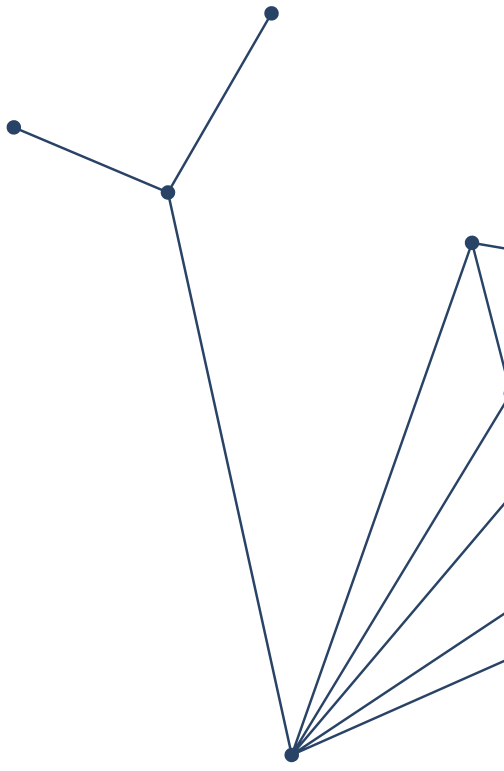
In 2022, 82.6% of the overall population owned a smartphone in France, 81.6% in the USA and 81.9% in Germany [3]. In 2021, 93.9% of Canadian households owned at least one smartphone [4]. In France, 90% of minors aged 12-17 owned a smartphone in 2022 [5].

These devices are a gateway to the wealth of information in the digital world, but they are also an open window to the many and significant dangers faced online by minors including:

- Content that is legal but inappropriate or harmful to minors;
- Illegal content;
- Risks of online harassment;
- Exposure to sexual or other predation

It is fair to state that anyone who has a smartphone also has almost unfettered access to pornography. Worse still, access to child pornography can be made even easier by the misuse of generative AI. These days, AI systems can be used to create synthetic content that may represent pornography including child pornography. While being particularly difficult to address from a legal point of view, the risk of exposure to such content to minors is even greater than before.

Under the circumstances, it is important to examine why is there such a "disconnect" between the "official" and "practical" response to regulating access by minors to adult and other forms of harmful content. Is it because these laws are useless? Is it because the means to enforce them are lacking or non-existent?



[2] Recently : E.U. Digital Services Act (UE) 2022/2065 october 19th 2022 ; Canadian Bill S-210: An Act to restrict young persons' online access to sexually explicit material
[3] https://fr.statista.com/statistiques/1360012/taux-de-penetration-du-smartphone-dans-certains-pays/
[4] https://www.statcan.gc.ca/o1/fr/plus/5289-plus-la-proportion-de-menages-ayant-un-telephone-cellulaire-augmente-plus-lutilisation-du
[5] https://fr.statista.com/statistiques/505110/taux-de-penetration-du-smartphone-par-age-france/

We consider that the above-referenced "disconnect" may be partially explained by three sources of societal ambivalence toward adopting a more rigorous approach to enforcement:

- First, some may consider that it is unrealistic (or, possibly, prudish) to attempt to prevent children from accessing adult content. There is a view that minors have always been "curious" about sex and have always found ways to access "adult" content in society, and that the net harm may be minimal.

- Second, many adults may feel discomfort with enforcement of rules as a regards a digital identity "solution" that would essentially require everyone (even adults) to provide credentials that confirm that they have reached the age of majority even if they agree with the aim of safeguarding minors' access to adult content. Such solutions are considered by many to pose a potential threat to privacy and to counter several of the core principles that were identified in our previous HTF/DIACC report.

- Third, age verification tools pose a significant challenge to the "business model" of online adult content service providers. In short, they increase costs, reduce the number of users and add "friction" to the process of accessing content. In short, service providers have little incentive to implement age verification tools.

We address these points in turn.

1. No Harm Done?

As regards the first form of resistance (that blocking access to adult content for minors is not really necessary because harm is minimal), we direct readers attention to the devasting findings of the UK Children's Commissioner revealed in her report "'A lot of it is actually just abuse: Young people and pornography " report, published in January 2023[6]. This report highlights the early exposure and harmful effects of online pornography on young people.

Among the report's finds:

- **Early Access and Downward Trend in Exposure Age:** The average age at which minors first access online pornography is thirteen years, with a significant portion exposed by the age of eleven and some by the age of nine. This trend towards early access correlates with the age at which children gain access to mobile phones. Even children as young as six can be impacted by deceptive schemes that draw attention using cartoon imagery.

- **Consequences of Early Exposure:** Early access to pornography by children increases the risks of addiction and exposure to extreme content over time, with over 20% of underage boys viewing pornography once or several times a day.

[6] cc-a-lot-of-it-is-actually-just-abuse-young-people-and-pornography-updated.pdf (childrenscommissioner.gov.uk)

- **Violent and Misogynistic Nature of Pornography:** Today's pornography is often violent and degrading, with a large proportion of young adults having seen violent pornography, including degrading acts, sexual violence, and non-consensual sexual acts before the age of eighteen. Sexual violence in pornography predominantly targets women, with a majority of young people having seen violence against actresses, compared to a smaller percentage against actors.

- **Impact on Sexual Relationship Perceptions:** Pornography significantly alters young people's expectations regarding real-life sexual relationships, negatively affecting their body image and promoting a transactional and objectifying view of sexuality, contrary to values of trust, consent, and communication.

- **Real-life Consequences:** A substantial percentage of respondents believe that girls expect sexual relationships to involve physical aggression, and a similar percentage of young adults have experienced some form of sexual violence.

These findings underscore the urgency of implementing effective protective measures to preserve the mental and physical health of minors against the risks associated with access to online pornography, and one which becomes increasingly difficult to monitor and prevent with advancements in technology. “Deepfake porn” and AI tools that allow children to “undress” their classmates may soon make even the blocking of access to porn stream sites insufficient.

2. Balancing effective age verification measures with privacy

If we can agree that unfettered access by minors to pornographic and other forms of harmful content is a cause of harm to minors and to society, it is important also to acknowledge that the mechanisms that society adopts to address such harm must also reflect best practice to preserve individual privacy and autonomy, including the core principles set out in the HTF/DIACC report. The concepts of data minimization, efficacy, and least privacy intrusive mechanism come into play. When it comes to online age verification measures, many Internet users feel that the introduction and use of such systems would inevitably lead to an invasion of their privacy. The desire for anonymity is particularly strong when it comes to visiting adult-only sites, and in general appears to outweigh the desire to protect minors.

Currently in many jurisdictions, providers of adult-only content must ensure users are “age compliant” according to applicable laws before granting access to their services. For example, online service providers must implement measures for content moderation and protection of minors in accordance with the laws and regulations in force, such as the Digital Services Act in the European Union, or other pre-existing national legislation.

As things stand, however, this legal obligation is often not respected in practice, and the majority of systems deployed to monitor users’ age compliance are no more than easily-bypassed declarative banners without any actual age verification measures. In reality, these measures are ineffective in achieving actual prevention of access to inappropriate material.

Prohibiting access to websites with adult content to anyone who cannot provide proof that they have reached the age of majority (in the same way that we require young people to provide age verification before they can purchase alcohol, enter a bar or drive a car), would certainly address the society objective of "protecting minors from harmful content", but what about privacy and reliability?

In Canada, the required use age verification technology in relation to adult content has been the source of notable and intense political debate. Opposition parties have proposed the adoption of mandatory age verification requirements, led by Senator Miville-Deschênes[7]. However, the Canadian federal government has strenuously resisted supporting the adoption of such legislation on the grounds that such requirements would pose an unacceptable threat to privacy. These include arguments that requiring adult content service providers to verify age would result in "sketchy" website operators gaining access to personal information about their users which could then be exploited for nefarious purposes; and that some of the "privacy-friendly" digital technology used to verify age is unreliable (e.g. anonymous video analytics cannot reliably distinguish between a 17-year-old and an 18-year-old).

However, based on our review of use cases studied by the working group, we find that, in fact, it is possible to reliably verify the age of those who access adult content in a manner that is fully respectful of privacy and autonomy.

We also note that protection of minors in the digital era requires the implementation of a wide range of measures across the whole digital value chain - from users, to parents/guardians, to suppliers - including manufacturers of equipment and software. Using digital identity mechanisms to restrict access should be considered as one of several tools to help curtail the significant impacts and issues described in point 1 above. Parental/guardian control and influence constitutes the first and most efficient protection for minors and vulnerable populations but are not as frequently used as perhaps they should be. So, in tandem with technical age verification solutions, it appears essential to work on strong educational packages for both underage people and the adults who care for them.

[7] Bill S-210: An Act to restrict young persons' online access to sexually explicit material: S-210 (44-1) - LEGISinfo - Parliament of Canada

3. What about the Business Case?

The specificity of this minors' online protection digital identity use case stands in the fact that deploying systems to verify and certify the age of online services' users is not intended to promote or facilitate access to services. On the contrary, such measures are designed to exclude unauthorized users from certain online services.

The consequences of this may be perceived as negative by both individual users and service providers'. Users who meet the age limit have their experience hampered by the presence of the verification system. Users who do not meet the age limit are excluded from the system. Service providers either way have access to their product and potential revenue streams curtailed - either through a higher-friction user experience for legitimate users, or elimination of a group of potential users entirely. For neither group is the direct benefit of these solutions for minors (i.e. their protection against content likely to cause them significant harm) likely to be front of mind. Nor is the nature of the harm minors may suffer obvious to such users, further justifying the importance of an education policy on this subject, for adults and minors alike.

Internet users typically do not like delay or resistance when accessing online content, adding to the negative public perception of online age verification. It should be remembered that even pop-up banners concerning cookies, which were made compulsory in certain jurisdictions to protect users' personal data, are considered too disruptive to browsing by many users.

And just because a solution has been made compulsory to protect the public does not mean that it will be accepted and/or respected, even by those it is intended to protect. For example, in France in the 1970s, the compulsory wearing of seatbelts in cars was seen by a large proportion of the population as a liberticidal measure. [8]

At the same time, if the system actually works as intended to prohibit access by minors, age-restricted online service providers will experience a loss of audience and revenues, given the business model of most of "free" websites, i.e. traffic monetization. In addition to the loss of audience and revenue, the implementation of these controls will incur costs for platforms and service providers. Under the circumstances, motivations to circumvent the use of such systems will likely be high on the part of both users and service providers.

Such issues will only be exacerbated by the multi-jurisdictional aspect of the Internet insofar as the laws of certain jurisdiction do not prohibit access by minors to "adult content" or impose harmonized standards as regards access control. In such circumstances, "adult content" service providers may simply relocate to more permissive jurisdictions and/or users of such sites may find ways to mask the jurisdiction from which they are accessing the content (using VPN or other similar technical measures).

[8] https://www.radiofrance.fr/franceculture/podcasts/le-pourquoi-du-comment-histoire/l-obligation-du-port-de-la-ceinture-de-securite-est-elle-une-atteinte-a-ma-liberte-3097022

We set out general and more detailed findings and recommendations below.

General recommendations 

To be effective and acceptable in the digital era, age verification solutions for protection of minors online must meet several key criteria.

- **It should be free for individuals/users.**
- **It must be as simple as possible to install and then to use as part of the browsing experience.**
- **The anonymity of the user must be guaranteed, together with the security of the solution and data protection.**
- **The benefits resulting from the deployment of the solution must convince users of their utility and must be credible in their eyes. In other words, the solution must be perceived as sufficiently reliable and robust to provide real protection for minors (i.e. by excluding them), without imposing undue constraints on authorized (adult) users of the services. Conversely, a solution that causes "friction" as regards online access, but that is easy to circumvent, will be perceived as hampering the experience of legal users without protecting minors, resulting in abandonment of the system in favor of easier workarounds.**
- **Regarding the issue of jurisdictional arbitrage and the and potential use of VPNs or other circumvention technologies, the protection of minors must also include the harmonization of legislation. As it is in practice nearly impossible to achieve complete harmonization, we need to consider the rules applicable to connections from certain countries whose legislation offers particularly poor protection for minors. There is also a need to consider the introduction of rules for blocking or filtering certain sites whose content should be subject to age certification, but which are hosted in countries that do not have legislation in place to protect minors. These issues need to be examined with a view to ensuring that individual freedoms are not disproportionately infringed.**
- **One special aspect of this particular use case – in contrast to others studied in this report - is that it represents an exception to the principle that the use of a digital identity system should be entirely voluntary. To be truly effective, the use of online age verification systems for online protection of minors should be mandatory – i.e. anyone wishing to access such content must use a digital identity system.**

In detail: How to reliably verify the age of a user, while respecting privacy?

Our compilation of case studies shows that it is indeed possible to verify a user's age in a reliable manner, while at the same time respecting the data minimization principle, in accordance with the highest privacy, security and data protection standards, through a process that implements a dual-anonymity principle. It is currently possible to issue a certificate of age compliance in a certified manner, without the certifier knowing the use that will be made of the certificate, and without the "gatekeeper" recipient of the certificate (i.e. in this case, the adult content website operator) knowing the identity of the certified person.

Such a solution for robust age verification which maintains anonymity is well represented by the double anonymity system recently introduced by Docaposte.

The Docaposte solution is based on an Internet age-verification platform that acts as a trusted intermediary between the user and the site. The trusted age verification platform is responsible for confirming the age of the individual by verifying authorized forms of government identification. The trusted age verification intermediary securely encrypts the age verification data and then creates a hashed age credential token. The trusted age verification intermediary does not transmit any information that identifies the user to third parties. Instead, only the user's anonymous age credential is shared with the user's special-purpose mobile application, with which the user can then provide the anonymous credential to any consulted site that requires such age verification.

This ensures double anonymity: the site does not know the identity of the user, and the age verification certifier does not know which sites are subsequently consulted by the user who provides the age verification credential.

Adopting such a dual anonymity solution helps to ensure that: a) the age verification process is reliable; b) there is no "stigma" associated with the specific act of proving one's age; and c) no sensitive personal data need be shared with adult website operators (unless the user wishes to do so).

A drawback of the several cases that we studied where double anonymity solutions are in place is that most are single-purpose solutions that are not designed to be interoperable with each other, which constrains the overall reach and effectiveness within a complex ecosystems. It also appears that the underlying business model, which makes it possible to offer solutions that are free at the point of use for users, is mainly based on charging platforms for the service (in particular through a fee per certification), which is a significant economic and technical constraint and may discourage adoption by adult content service providers. This highlights even more the problem inherent to the economic model in which the age certification service provider is financed by the service provider requiring age certification.

Recommendation

Online age certification should be created in compliance with the technical principle of double anonymity.

In detail: How to ensure Interoperability?

Age certification solutions are by their very nature difficult to achieve acceptance by the target audience (from users to online service providers). The risk of rejection is compounded when there is a wide range of look-alike solutions to choose from, or when there is a lack of interoperability and mutual recognition of certificates issued by different identification solution providers.

Without interoperability, various scenarios emerge. Either online service providers implement on their websites/platforms the full range of age verification solutions to satisfy their users (the cost and complexity of this scenario makes this unlikely).

Or users adopt all the existing solutions to access all or at least a majority of websites requiring age verification. This scenario is also not credible and users encountering frictions in their browsing will look for a workaround.

It should be stressed that technical interoperability does not currently appear to be a major problem. On the contrary, the question of interoperability seems to arise more from the point of view of the mutual recognition of the certificates issued by the various players, which is linked in particular to the economic model currently emerging.

Recommendation

Online age certification solutions should issue interoperable certificates. We recommend the application of existing technical and security standards to facilitate the technical interoperability of solutions (in particular ISO standards).

This requires agreement between stakeholders to recognize each other's solutions. We therefore recommend the creation of a consortium of players offering age certification solutions that meet the same ethical, technical and security standards to ensure the operational and political interoperability of the certificates issued. The principles set forth in the HTF/DIACC report "Policy design principles to maximize people-centered benefits of digital identity" can be applied to create such standards.

In detail: What would be a viable business model?

Studies of the solutions and models proposed, for example, by Docaposte and Greenbadg show that age certification solutions are, at this stage, mainly single-use age certification solutions based on a one-way funding system that relies on economic partnerships with the service-providing platforms themselves to integrate the solutions.

This model is imposed by the fact that the development, testing and dissemination of these solutions is the result of private initiatives. This has led to the choice of a simple and traditional economic model, which meets the requirement of being free for users. The downside of this model is that while the developers and publishers of certification solutions are rewarded by a fee for each certificate generated and used on the platform, they have no economic interest in allowing the use of certificates provided by third parties (e.g. competing certification solutions). However, mutual recognition and interoperability of these certificates would actually benefit everyone by making it easier to deploy these solutions, thereby limiting the use of workarounds.

In aggregate, however, interoperability can be perceived as a way to develop a more virtuous business model, favorable to more rapid dissemination of age verification systems and individual companies may ultimately find business benefit through deployment of interoperable solutions.

It is interesting to look at the choices made by players in bankcard payment services. These players have chosen to promote interoperability and mutual recognition of the payment instruments issued by each of them. In both Canada and France, this has led to the creation of a private economic interest grouping bringing together most of the leading financial institutions in each country with the aim of ensuring the interoperability of payment cards.

This interoperability has expanded, and now most of the major banks allow interfacing or have partnerships with international networks such as Visa, MasterCard, UnionPay, JCB, American Express, Discover and Diners Club International.

Thanks to the facilities offered by interoperability and the joint organization of resources and remuneration of service providers, card payments will be in the majority in some countries, including France, by 2023. [9]

[9] https://fr.statista.com/infographie/29927/utilisation-moyens-de-paiement-preferes-par-pays/

In detail: Should digital identity solutions be single-purpose or multi-purpose?

If digital identity systems proliferate - especially without interoperability - to solve single potential use-cases like age-of-majority verification (or other scenarios such as legal status, residence verification, education proof etc.) then there is a risk that wide proliferation of various digital identity systems could pose challenges to user acceptance.

Proliferation of single-purpose identity solutions could lead to confusion: too much choice makes it difficult for users to select the solution or solutions that suit them best, leading to users abandoning use of digital identity solutions due to lack of accessibility and/or intelligibility.

Single-purpose identity solutions can also risk derivation of use from simply having access to a solution. For example, adult users are unlikely to accept being potentially identifiable as consumers of adult-only content online, simply by virtue of being in their possession of a very specific authentication application which may identify the use to which it is put. It seems more difficult to assume using a solution that is only designed to carry out online age verification to access adult content than to use a generalist digital identity solution that allows, among other functions, to do this.

In addition, the proliferation of solutions based on digital identity but for a single or specific use poses serious challenges in terms of data protection and data proliferation/multiplication.

The multiplication of data and its duplication in various applications necessarily increases storage requirements and the environmental impact of digital identity solutions. This does not seem acceptable.

It therefore seems appropriate to develop multi-purpose digital identity systems, based on secure digital wallets. This will minimize duplication of data and optimize the availability and use of data by individuals for their own benefit by enabling the creation of certified and reliable attributes, as seen – for example - with the Queensland Digital License system in Australia, which is an app that can store Queensland citizens' identifications easily on their mobile devices and can perform Proof of Age.

Recommendation

We recommend that the creation of age conformity certificates should rely on multi-purpose digital identity solutions to increase acceptability, improve interoperability and optimize data governance and management.

Interview with Digital Affairs Ambassador Henri Verdier: What are the perspectives for the deployment of digital identity solutions in age certification?

Henri VERDIER

Henri Verdier is the ambassador for Digital Affairs for the French Ministry for Europe and Foreign Affairs since October 2018. He is a member of the prospective committee of the National Data Protection Commission (Commission nationale de l'informatique et des libertés "CNIL"). In 2014, he was appointed General Administrator for Data ("AGD"), then in 2015 Interministerial Director of Digital and State Information and Communications Systems ("DINSIC").

As part of the development of digital identity, Ambassador for Digital Henri Verdier shared his perspectives on the development of digital identity services as part of age certification in an interview held on April 29, 2024. He shares his views on the deployment and social acceptability of digital identity solutions.

Barriers to the deployment of age-certification digital identity solutions

The deployment of digital identity solutions needs to adapt to the political-bureaucratic timeframe which, even if it is not the timeframe for innovation, is important to ensure respect for fundamental freedoms. The first age-control solutions did not fully guarantee anonymity. Firstly, in a state governed by the rule of law, a de facto imperative solution cannot be imposed in this field without having studied, tested and controlled the consequences in terms of privacy protection. It must be ensured that the solution preserves privacy and social trust. No one should be able to turn the solution against users. The issue of social acceptability is therefore at the heart of the deployment of digital identity solutions to control the age of visitors to adult-only sites, for example.

> "The French Prime Minister's office has estimated the number of unique visitors to pornographic sites in France at 41 million per week. The need to prove one's age, even if this verification is not linked to one's identity, can undermine acceptability through the perception of surveillance.Visitors to such sites may have the impression of revealing themselves, or to have left a trace."

The necessity to comply with the principle of minimizing data collection

The ambassador in charge of digital affairs believes that the greater the use of identification by individual attributes for social purposes, the more successful it will be. It will help to reduce the feeling of being under surveillance, and therefore guarantee greater social acceptability, whatever the nature of the actors involved in age certification, whether private or public.

> "There is a duty to recognize what data is going to be useful and to adopt the principle of minimizing data collection."

A European initiative to help strengthen the social acceptability of digital identity

Henri Verdier believes that Europe will contribute to greater social acceptability of digital identity solutions with the introduction of the easy-to-use and interoperable Digital Wallet.

> “The introduction of the Digital Wallet in 2025, which will be interoperable and based on individual identification attributes, will make the user experience easier. This innovation should be perceived as a bureaucratic solution without too much fear of surveillance by users. This should encourage its adoption.”

The business model challenge for digital identity solutions: an economic balance to be defined

With the digital civilization already well established, proving one's digital identity on websites is becoming increasingly important for a growing number of applications. Relevant use of age would enable us to respond to many use cases. In his own personal opinion, ambassador Henri Verdier believes that a balanced business model has still to be found for age verification solutions, and that pay-per-use, given the colossal number of uses that will emerge, is not necessarily the right solution.

RECOMMENDATIONS SUMMARY

- **Age verification solutions must meet several key criteria.**
  - It has to be free for individuals/users.
  - It must be as simple as possible to install and then to use as part of the browsing experience.
  - The anonymity of the user must be guaranteed, together with the security of the solution and data protection

- **Online age certification should be created in compliance with the technical principle of double anonymity.**

- **Creation of a consortium of players offering age certification solutions that meet the same ethical, technical and security standards to ensure the operational and political interoperability of the certificates issued.**
  - Operational interoperability of solutions, which requires an agreement between stakeholders to recognise each other's solutions.
  - Application of existing technical and security standards to facilitate the technical interoperability of solutions (in particular ISO standards)
  - Application of the principles set forth in the HTF/DIACC report “Policy design principles to maximize people- centered benefits of digital identity” to create such standards
  - This group/network should initiate a transversal discussion on the funding and model to be developed to offer age verification solutions that are interoperable and free of charge for their users. We recommend that the results of this work be published to increase the transparency.

2

HEALTH

Our second use case relates to the deployment of digital identity solutions in relation to management of individual health data. Use cases such as the creation of Mon Espace Santé in France demonstrate that it is possible to considerably improve the storage and access to health data by patients and medical staff, to the benefit of the quality of patient monitoring and treatment. The WHO digital health initiative also demonstrates how important it is to develop interoperable systems at an international level in the field of health.

It should be noted that the nature of health data itself has changed significantly with the increasing dissemination of hardware and software solutions able to record and monitor individuals and their environment on a constant basis. For example, many people use software apps and consumer devices such as FitBit (one of our studied use cases) to track information such as the number of steps a person takes in a day, heart rate and rhythm, blood oxygen, calorie intake, and sleeping patterns. Although such data is not collected in a medical setting and is not systematically shared with a medical professional, it can provide invaluable insights into an individual's overall health. So, when we talk about health data, we no longer simply refer to data derived from medical records: so-called 'daily' data or lifestyle data, in combination or in addition to traditional medical health data, can provide information on the state of health and well-being both of an individual and even of a population as a whole.

As part of our study, we set out to explore the use of health data, including both traditional medical data and lifestyle data with an aim to explore how interactions between individuals and their health data could be improved for their own benefit and, by extension, the general interest.

We identified two main areas of research. The first is where the primary preoccupation of the use case is to maximize how individuals' health data is made available to them as part of their care pathway. We look at how data is collected, processed and used to support patients throughout their medical journey to ensure that patients receive the best possible support, while ensuring that they have direct influence over the governance of their health data.

The second is to investigate how individuals use their health data by themselves outside the healthcare context. This area raises important questions about the empowerment of individuals in the management of their health data, the control they can exercise over it, and the opportunities they have to benefit directly from this data, for themselves or for sharing purposes (particularly altruistic ones).

These two main preoccupations have given rise to issues discussed below.

In detail: The benefit and risk balance of individual governance of health data in the care pathway

An individual's health data is, of course, considered to be highly sensitive since it provides information about highly private parameters to those who may have access to it.

From the patient's perspective, one of the key issues that arose from the analyzed case studies is the balance between the application of the Principle of Least Privilege access control ("PoLP" : variation of access rights on the basis of the rule that one can only access the information and resources that are necessary for a legitimate purpose) and the ability for the individual to benefit from the best care pathway possible. Therefore, digital identity systems should be conceived to enforce PoLP access to ensure that medical information is only made accessible to those who need to know it in order to provide good patient care.

Only relevant healthcare staff should have access to health data, with the level of access depending on the precise function in the care pathway and the level of decision-making autonomy (doctor, nurse, paramedic). Patient identification by administrative staff should adopt the same philosophy (no access to unnecessary data regarding the purpose of identifying the patient).

However, it is interesting to underscore that in some cases, medical staff do not need to have access to some medical information to provide good care. For instance, a patient may not wish to inform their dentist of a mental health issue treated by medication.

Conversely, restricting access to medical data can also lead to risks during an emergency.

Nevertheless, it is often difficult for a non-practitioner to distinguish between what is useful to his/her doctor and what is not. Overall, this seems to suggest that qualified medical professionals who can demonstrate a "need to know" should be provided access to as broad a range as possible to relevant health data (including, potentially, lifestyle data, as discussed further below).

Recommendation

We recommend that the development of a digital identity system incorporating health data should be designed to improve patient care by enabling healthcare staff to access easily and directly all the data which may have an impact on patients.

In detail: Digital identity in the Lifestyle Data realm

Health data is not only medical, clinical or genetic data. For example, data relating to daily life or lifestyle, or data collected by "smart"/IoT devices, can also provide useful information to healthcare staff when treating a patient. Even if this data necessarily has a different level of accuracy or reliability compared to medical, clinical or genetic data. Empowering people to take control of their lifestyle data should lead to the creation of a digital identity system enabling people to pass on their daily/lifestyle data if they so choose to healthcare staff, for their own and/or altruistic benefit.

Today, it should be emphasized that during a medical examination of a conscious patient, doctors are already in the habit of asking the patient about their lifestyle. Do they smoke? Drink alcohol? How often? However, often the quality and completeness of the information provided by patients to their doctors in this context is limited and based on declarative elements only.

The advantage of including lifestyle data in the health data of any patient who so wishes would be to give their doctors access to much more complete, accurate and usable data than in a simple declarative interview. The cross-referencing of this data, carried out with the necessary precautions, with medical data via artificial intelligence systems for example, could also speed up the diagnosis of certain pathologies, or anticipate their occurrence.

Today, none of the case studies examined facilitates the sharing of such IoT device generated lifestyle data by the individual to their physician for the individual's benefit. This “gap” represents both a challenge and a major opportunity for healthcare improvement.

With appropriate controls and in an entirely voluntary manner (in line with principles of voluntarism, informed consent and user control) it should be possible to make both medical data and daily/lifestyle data available to healthcare staff, while ensuring that it is labeled and identified as traditional medical data vs. lifestyle data (e.g. health data generated by IoT systems like connected watches/apps - approved or not by the health/scientific community).

Recommendation

We recommend the creation of digital identity systems enabling individuals, if they so wish and under their full control, to make their lifestyle available to their physician for consultation alongside their traditional health data, in particular to optimize their medical care.

In detail: Health data and anonymity/privacy

As mentioned in the introduction and earlier report drawn up by HTF/DIACC, the principle of data minimisation must be used to preserve confidentiality and protect privacy, and must go as far as seeking maximum anonymity in the use of data. Any system must be designed to deliver only the information that is useful for the intended purpose.

We highlight that revealing a person's identity should not always be considered necessary nor useful, even regarding healthcare. For example, a doctor examining a patient does not necessarily need to know the patient's full identity, but he or she does need to have access to the patient's health records and be sure that the patient has been previously identified. Conversely, administrative staff receiving a patient at a healthcare facility must be able to verify the patient's identity in order to integrate them into the care program.

The complexities of health data and anonymity/privacy in the context of digital identity reinforces the need for multi-purpose digital identity systems, which would enable cross-referencing of data to create such certificates as recommended here. It would assist in reliability of certificates by cross-checking data, and assist in minimization of data duplication.

Recommendation

We recommend that any digital identity system should be designed so that the data it contains can be used to create attributes or certificates that confirm a status or piece of information and link that status or piece of information to the individual/holder of the digital identity system, while revealing no information other than that contained in the certificate. For health data, it should be possible to generate ad hoc or customized certificates from the digital identity system.

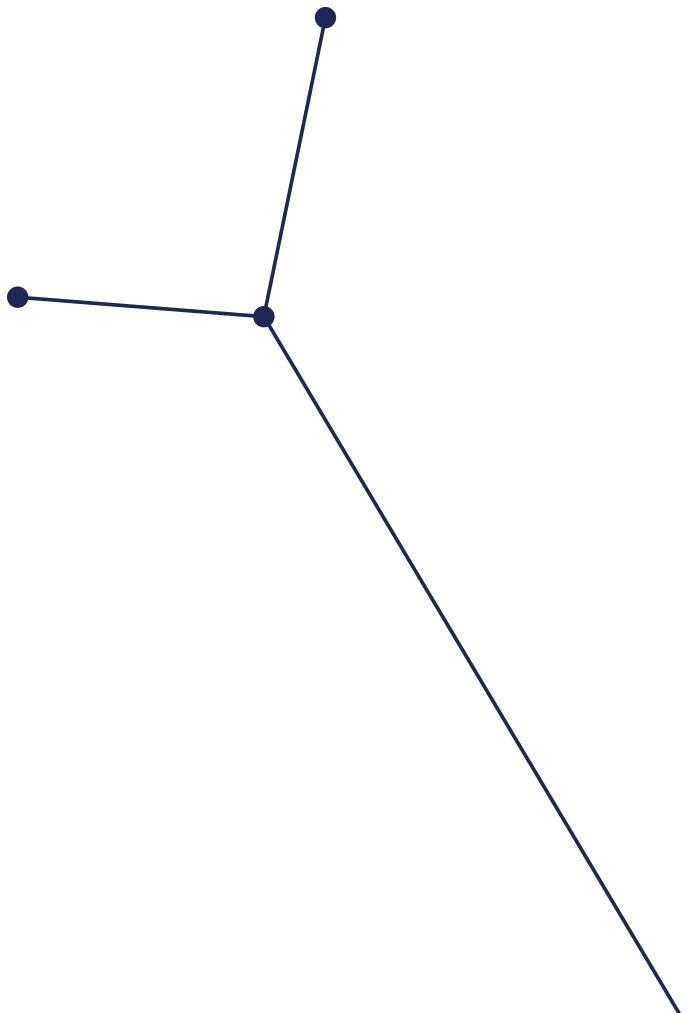
In detail: focus on vital emergency care and unconsciousness

Some specific circumstances require healthcare staff to be able to access critical data without the patient's awareness, or their ability to express consent or refusal. This situation needs to be directly addressed in the design of a digital identity service managing access to individuals' health data. This is already the case in several countries such as France, with an “emergency hammer” principle. This principle allows healthcare professionals to access the medical record of a person who is unable to express their wishes in an emergency. This procedure is designed to allow any healthcare professional to consult the shared medical record of a patient whose condition poses an immediate risk to his or her health. In the parameters, the holder of the shared medical record must indicate whether or not he/she authorises this access in the event of an emergency.

In the context of digital identity, this is where certificates/attributes linked to an individual should also be created that can be accessed by authorized healthcare teams at any time, whether the individual is conscious or not. These may include attributes such as blood group, position on organ donation, and people to contact in the event of a problem.

From a broader perspective, issues around health data provision in the context of emergency care and unconsciousness needs to be addressed at two levels when it comes to digital identity solutions:

- Firstly, enabling authorized access to a certain amount of data may be required when a patient is unconscious (certificates/attributes and access authorities to be put in place).
- Secondly, it should be possible to configure access to health data using an opt-out system. By default, when a patient is unconscious, carers should be able to access that certain defined emergency health data, but there should be an option for the patient (when conscious, prior) to restrict this access by opting out. The patient should be able to configure some or all data as private and inaccessible to carers. If the patient chooses to restrict access to some health data, this must be clearly disclosed to carers.



In detail: Health data certification

The creation of a digital identity system that includes health data should make it possible to improve care for individuals and give them back control over their data. However, this objective must take into account the variable nature of health data (clinical, genetic, lifestyle) and the international nature of population interactions. A digital identity should enable an individual to report health data that is reliable, and perceived as such anywhere in the world.

The harmonization of international standards for categorizing health data by type or destination could enable the certification and qualification of health data by type or destination in the individual's wallet, making this data internationally interoperable because it is issued and certified according to the same standard. This would enable individuals to benefit from better care, on the one hand, but also to share this data more widely, where appropriate, by providing reliable and precise indications of the source and quality of the data.

Such a standard should be adapted to take into consideration devices and systems that generate daily/lifestyle data that may become health data by destination or interpretation. We would point out that such a system could facilitate the creation, on the basis of the same data, of other attributes benefiting from a high level of trust.

For example, a certificate of majority described in Use Case 1 above, designed according to the principle of double anonymity, and based on certified health data could be used in all circumstances requiring proof of age, internationally, without the use of a third-party solution, and while respecting the principle of data minimization.

Recommendations

- **We recommend that digital identity systems that manage health data shall be developed to meet a level of assurance that is at least 'substantial' and, whenever possible, 'high'.**
- **We recommend that digital identity systems should be developed to clearly label health data so that its origin and quality can be identified.**
- **We recommend that such data labeling should be transparent, intelligible, and certifiable.**
- **We recommend the harmonization of international standards for categorizing health data by type or destination.**
- **We recommend that such international standard harmonization should take into consideration devices and systems that generate daily/lifestyle data that may become health data by destination or interpretation.**

In detail: Autonomy and data control

None of the systems and use cases studied provide for active control by individuals over their health data.

Individuals must be able to share their health data voluntarily and in an enlightened manner, for medical research purposes for example, but this data must not be accessible to third parties for purposes other than patient care, the provision of health services, scientific or medical research, and ultimately if not authorized by the individual.

Access to – and control of – health data by individuals may give rise to abuses, in particular requests for access by third parties who have no legitimate reason for access. A landlord should not be able to ask a candidate tenant for information about their health, for example. Within the European Union, the GDPR provides regulatory protection for individuals against this type of request, and we encourage its generalization.

Recommendations

We recommend that digital identity systems should enable individuals to access and control their health data, in particular for the purposes of sharing it in the general interest; such a tool is likely to enable the implementation of the data altruism envisaged by the DGA (EU Data Governance Act).

Health data included in a digital identity system should not be made accessible to third-party applications without a legitimate purpose in having access to it and without a particularly clear system of information and consent to sharing.

Interview with Doctor Fabrice Brunet: Towards a classification of health data?

Fabrice BRUNET

Dr. Fabrice Brunet is President and CEO of the Health Innovation District. Until January 2023, he was CEO of the Hospital Center of the Montreal University ("CHUM"), as well as President of the University of Montreal Health Network. On the academic side, he was Professor at the Department of Pediatrics of the Montreal University, Professor of Medicine at the University of Toronto and the University of Paris, and Affiliate Professor of Management at HEC Montreal.

In an interview held on April 26, 2024, Dr. Fabrice Brunet shared his perspectives on the development of digital identity services used to manage healthcare data. He gives us his vision on the challenges of sharing and making healthcare data accessible to healthcare professionals.

The development of altruistic health data sharing

According to Fabrice Brunet, there are limits to the use of altruistically shared health data, in order to protect patients. We need to be sure these data are shared in the public interest. It is therefore essential to define the consent required for this sharing, to know the type of research and whether this sharing is carried out as part of a specific research program.

> "The limits to be set on the use of data include the level of consent, information on data collection, in other words, the definition of the research goals behind the data collection and the definition of the recipients of such research."

Health data classification is necessary

All uses of health data must be strictly for the benefit of the patient. Patient data must be stored confidentially in a data warehouse. Data access authorizations have to be granted by the patients according to their characteristics.

> "The limits to be set on the use of data include the level of consent, information on data collection, in other words, the definition of the research goals behind the data collection and the definition of the recipients of such research."

Access to health data subject to conditions

The confidentiality of health data must be qualified in the specific case of a sick patient. Physicians may need access to data that patients do not wish to disclose. This specific access must be granted under certain conditions and for a limited time, such as the duration of the treatment.

> “Access to health data classified as confidential by the patient must be subject to conditions. Suitable medical staff must assess the existence of the need, and this must be for a limited period, such as the time of a treatment.”

RECOMMENDATIONS SUMMARY

- **We recommend:**
  - that the development of a digital identity system incorporating health data should be designed to improve patient care by **enabling healthcare staff to access easily and directly all the data which may have an impact on patients.**
  - the creation of digital identity systems enabling individuals, if they so wish and under their full control, to make their lifestyle available to their physician for consultation alongside their traditional health data, in particular to optimize their medical care.
  - that any digital identity system should be designed so that the data it contains can be used to create attributes or certificates that confirm a status or piece of information and link that status or piece of information to the individual/holder of the digital identity system, while revealing no information other than that contained in the certificate. **For health data, it should be possible to generate ad hoc or customized certificates from the digital identity system**.
  - that digital identity systems that manage health data shall be developed to meet a level of assurance that is at least 'substantial' and, whenever possible, 'high'.
  - that **digital identity systems should be developed to clearly label health data** so that its origin and quality can be identified.
  - that such data labeling should be transparent, intelligible, and certifiable.
  - **the harmonization of international standards for categorizing health data by type or destination.**
  - that **digital identity systems should enable individuals to access and control their health data**, in particular for the purposes of sharing it in the general interest; such a tool is likely to enable the implementation of the data altruism envisaged by the DGA (EU Data Governance Act).
  - that **health data included in a digital identity system should not be made accessible to third-party applications without a legitimate purpose** in having access to it and without a particularly clear system of information and consent to sharing.

3

VOTING AND ELECTIONS

By the end of 2024, an unprecedented number of people—approximately half of the world's population—will have participated in various elections. In 70 countries, more than three billion voters will have to choose a new president, new parliament or equivalent. The scale of electoral participation in 2024 highlights the global significance of democratic processes. Ensuring that elections are accessible, secure, and trustworthy is a fundamental challenge that may require innovative solutions.

Recent events, such as the January 6 Capitol attack in the USA, political turmoil in Brazil, and the manipulation of information during the Brexit campaign, illustrate the vulnerabilities in current democratic systems. The misuse of data, as seen with Cambridge Analytica [10], further complicates the landscape, demonstrating how digital platforms can be exploited to undermine democratic processes.

The introduction of new voter identification rules, particularly in the United States, has sparked a contentious debate. Critics argue that such measures are designed to suppress the votes of Black, Hispanic, and youth populations. These groups are disproportionately affected because they are less likely to possess the required forms of identification in the form of reliable physical ID (let alone digital). For instance, studies have shown that 21% of Black Americans and 23% of Hispanic Americans lack a driver's license, compared to only 8% of white Americans. This discrepancy is rooted in historical and socio-economic factors, such as barriers to obtaining birth certificates or financial resources to get an ID [11].

Proponents of mandatory voter identity laws argue that they are necessary to prevent voter fraud and maintain electoral integrity. However, evidence of widespread voter fraud is minimal, and the number of voters disenfranchised by strict ID laws often exceeds the instances of fraud these laws aim to prevent [12].

This dynamic of both inclusion and security is crucial context for adopting digital identity verification systems for voting. It is crucial to stress that the deployment of digital identity systems can help give marginalized populations access to voting and state services. For example, Aadhaar, the digital ID System deployed in India, has facilitated access to essential services for numerous marginalized individuals, including access to the voting process. It also provides access to subsidies, pensions, and food rations. By providing a unique identity, it has streamlined the process for individuals without prior identification to receive government benefits.

The introduction of Aadhaar into the voter registration process has been designed to reduce duplication and ensure that individuals can exercise their right to vote. Aadhaar-based verification is an effective method for maintaining an up-to-date and accurate voter list, which is essential for conducting fair elections.

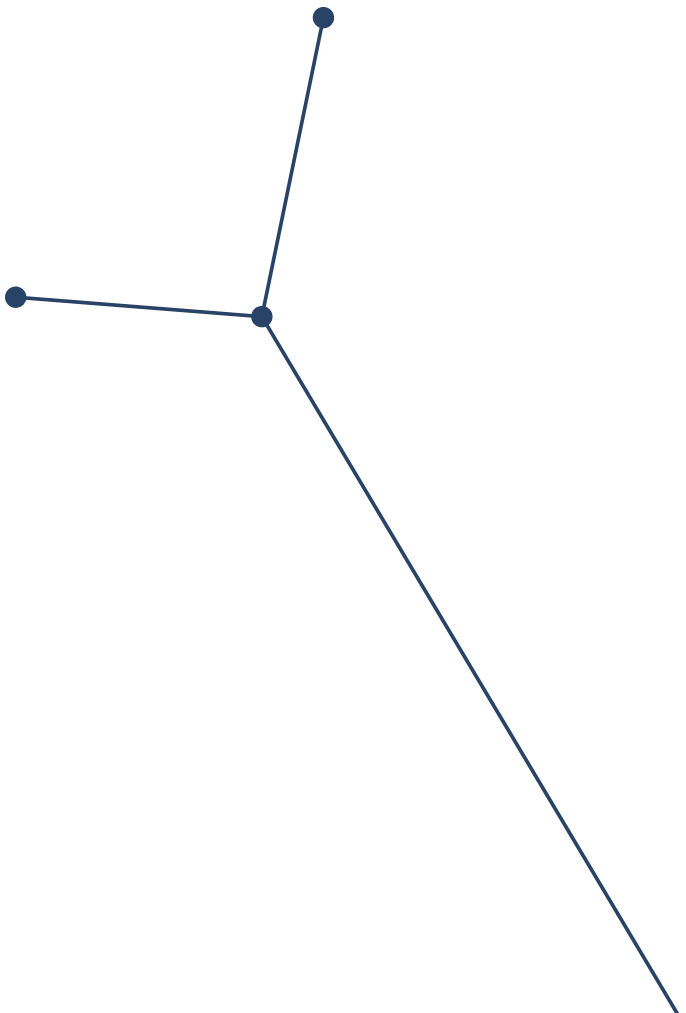
Still, it shall be kept in mind that Aadhaar also raises some concerns regarding privacy and confidentiality of such sensitive citizen’s data as this system has already faced data leaks [13].

[10] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html ; https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
[11] https://www.brennancenter.org/our-work/research-reports/impact-voter-suppression-communities-color
[12] https://journalonworldaffairs.org/2021/05/13/voter-id-laws-the-motivation-and-impacts-on-african-americans/
[13] https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms?from=mdr

As well, the digital ID system and i-Voting platform in Estonia have facilitated the participation of marginalized and geographically dispersed communities in the democratic process. This inclusivity is a critical aspect of Estonia's broader e-Governance strategy, which aims to ensure that all citizens can engage with government services efficiently and transparently.

Our work focused on the use of digital identity system to allow online voting, rather than exploring the use of digital identity to verify voters identity at polling stations.

As things stand, the working group's opinion is that online voting should be considered as an alternative offered to increase accessibility and inclusivity in the democratic field. However, some major risks concerning online voting systems are currently unmanaged.



In detail: How do you create a digital voting booth and preserve citizens' freedom of choice?

Remote electronic voting can be an important factor of inclusiveness in the democratic process. Online voting systems can facilitate participation by allowing voters to cast their ballots from anywhere, reducing the need for physical presence at polling stations. This is particularly beneficial in contexts such as pandemics, for voters residing abroad, or for those affected by mobility issues.

However, it should be emphasized that among the fundamental principles governing the organization of elections is the preservation of citizens' freedom of choice, and correlatively the confidentiality of their vote. This confidentiality is ensured by rules for the material organization of elections, and in particular through the creation of confidential voting spaces, called “polling booths” or “voting booths”. The principle is that the voter must enter the voting booth alone, in order to allow them to vote secretly and without any external influence. Placing a ballot in an envelope further assures the confidentiality of the choice, and the act of voting in person directly allows the voter to be certain that their ballot has not been modified.

The physical voting mechanism helps to ensure that there is no direct external influence at the moment of voting; and in the confidentiality of the vote. As it stands, remote electronic voting does not allow this system to be reproduced..

Although it is possible to validate the identity of the voter, it remains impossible to verify that he or she is not subject to direct external influence during the act of voting. It is also impossible to verify that the vote occurs confidentially.

Electronic remote voting, which can be organized using a digital identity system, does not therefore guarantee the voter's freedom of choice or the confidentiality of their vote.

Technical solutions can be tested to alleviate this problem, but on an experimental basis and by carrying out detailed impact studies on the balance between respect for privacy, data security and the systemic risks that may arise. For example, voters could be required to have a terminal equipped with a camera and to use an AI real-time monitoring system to detect any unusual behaviors or voting patterns that may indicate coercion or undue influence. The camera could also be used to make a scan of the room in which the voter is, to ensure that he or she is alone, then implement time-limited voting sessions that can reduce the risk of third-party coming in to influence by encouraging voters to complete the process quickly and privately.

Recommendations

- **We recommend, as it stands, to deploy remote online voting solutions securely through a reliable digital identity system as an alternative offered to people that encounter issues to physically attend polling stations, as a mechanism to increase inclusiveness.**

- **Given the potential for inclusiveness that online voting represents, we recommend that test deployments of online voting solutions be carried out. These tests should be accompanied by impact studies to encourage the emergence of technical solutions that preserve the principles of confidentiality, freedom of choice, data security and voter privacy.**

- **We recommend creation of clear channels for voters to report any instances of coercion or undue influence.**

In detail: Confidentiality and data minimization

As part of the deployment of a remote electronic voting system, the question of voting confidentiality arises not only at the time of the act of voting, regarding the voter's environment, but also at the level of the vote recording and counting system. Any connection to a remote voting platform with a digital identity indeed involves accounting and electronic recording of the vote cast by the voter, certified by their digital identity system.

This represents a risk in terms of confidentiality, which is not acceptable.

It should also be noted that, as IT/software systems are subject to potential failures, it seems difficult to guarantee the voter a certified accounting of their vote without risking confidentiality. A study of the Estonian system shows that voters are allowed to check their choice after it has been made and to change it up to the end of the ballot time window.

While this allows voters to be sure that their vote has been taken into account and that it corresponds to their choice, the system poses a risk in terms of confidentiality. The fact that individuals can access their voting data means that the same data can, in theory, be accessed fraudulently by a third party. In addition, although this system allows the correct vote to be verified, it could also be perceived as a means of monitoring the population.

Taken together, this shows that it is difficult to find the right compromise between checking the conformity of a vote's registration and confidentiality.

As things stand, the risk associated with a breach of confidentiality and anonymity in the recording of votes seems greater in terms of potential infringements of fundamental freedoms than that associated with an individual failure to record a vote.

In any case, these issues also show that the implementation of a remote e-voting system does not, as it stands, offer the same guarantees as a traditional voting system.

Recommendations

- **We recommend that development of remote electronic voting systems focuses on maintaining the confidentiality of the votes cast.**

- **We recommend that digital identity systems should therefore allow for the issuance of certificates or ballots that are certified by the system as being associated with an identity, but without the voter's choice being associated with their identity. The electoral registration system should have access only to the identity certificate, not to the identity itself and not to the choice made. Thus, the digital identity system should not record any information other than the issuance of a ballot, the content of which is unknown to it.**

- **Furthermore, as an e-voting system should be seen as an inclusive alternative, it should be emphasized that the international interoperability of digital identity systems should make it easier for non-citizens to participate in local elections, where this is open to them. This is the case, for example, for local elections in France, which are open to European citizens.**

Interview with Thomas Klein: Towards a classification of health data?

Thomas KLEIN

Thomas Klein is a municipal councillor of Suresnes. He is responsible for information systems, artificial intelligence and modernization.

In an interview held on May 28, 2024, Thomas Klein shared his perspectives on the development of e voting. He gives us his vision and describes its own experience in Suresnes.

The development of online voting

The question of online voting is an important one, one that comes up at every election in France, and once again in the light of the European elections, where a record abstention rate is expected. Voter participation is a pillar of our democracy, and it is essential to find ways of facilitating the exercise of this right while guaranteeing the security and confidentiality of votes.

> “Online voting is often seen as a solution to reduce abstention by offering a modern and convenient alternative. At the same time, it raises crucial issues of security and confidentiality. It is imperative to ensure that online voting conditions meet the same standards of confidentiality as those offered by a traditional voting booth.”

The case of Suresnes, a town of 50,000 inhabitants

Take the case of Suresnes, where electronic voting machines are being used. Suresnes is one of 82 towns in France to have deployed electronic voting machines. As President of a polling station, I am convinced of the benefits of these machines, particularly in terms of rigorous vote counting and greater transparency in the electoral process. My role is to reassure voters by enabling them to understand how these machines work, to check their integrity, and I do not hesitate to go round the machine with some of them when they want to understand more and make sure that, in fact, the machine is powered by electricity only and disconnected from any network.

> “Technically, it is perfectly possible to have a secure online vote. We carry out secure operations on many subjects, and so we have the skills in France to secure this.”

Online voting raises trust issues

After authorizing the use of electronic voting machines in 2003, to modernize the election and make the process more efficient, the French Ministry of Interior decided to no longer extend the use of electronic voting machines, and to restrict their use to those communes that had already adopted them: doubts on the part of part of the population were becoming too significant.

> “This brings us to a key question: is the argument of convenience sufficient to justify the adoption of online voting? Although I'm an enthusiastic supporter of digitalization, I have a few concerns. The right to vote is the very foundation of our democracy, and is worth the effort, even if it means spending an hour voting in person.”

As is often the case, the real issue is trust. The implementation of online voting can only be considered in a highly climate of trust. Without this trust, the consequences could be serious, with the legitimacy of election results called into question. In 2024, the conditions for a safe and reliable transition to online voting do not seem to be in place in France for many years to come.

RECOMMENDATIONS SUMMARY

- **We recommend:**
  - **to deploy remote online voting solutions securely through a reliable digital identity** system as an alternative offered to people that encounter issues to physically attend polling stations, as a mechanism to increase inclusiveness.
  - that **test deployments of online voting solutions be carried out**. These tests should be accompanied by impact studies to encourage the emergence of technical solutions that preserve the principles of confidentiality, freedom of choice, data security and voter privacy.
  - **creation of clear channels for voters to report any instances of coercion or undue influence**.
  - that development of remote electronic voting systems focuses on maintaining the confidentiality of the votes cast.
  - that **digital identity systems should therefore allow for the issuance of certificates or ballots that are certified by the system as being associated with an identity**, but without the voter's choice being associated with their identity. The electoral registration system should have access only to the identity certificate, not to the identity itself and not to the choice made. Thus, the digital identity system should not record any information other than the issuance of a ballot, the content of which is unknown to it.
  - that the **international interoperability of digital identity systems should make it easier for non-citizens to participate in local elections**, where this is open to them. This is the case, for example, for local elections in France, which are open to European citizens.

4

THE DIGITAL IDENTIFICATION OF SYNTHETIC DATA

The emergence of generative Artificial Intelligence and its democratization raise a large number of issues in several fields including the treatment and ownership of intellectual property rights relating to the data used to generate models, and the intellectual property rights relating to synthetic contents.

Another issue is that generative AI systems have opened up a new door contributing to the rise of fraudulent content such as “deep fakes”, and in particular (as mentioned above in the first part of this report), deepfake porn, which is particularly dangerous in terms of respect for privacy, infringement of fundamental rights and the image of individuals, and damaging in the context of child abuse.

New laws being considered for adoption, such as the European Union's Artificial Intelligence Act (AI Act) – which represents a landmark effort to regulate AI technologies comprehensively – put a strong emphasis on transparency and accountability.

Such regulations will introduce requirements for watermarking synthetic data produced by generative AI and enhancing transparency regarding the sources of data used to train large language models (LLMs). These measures are designed to address concerns about the authenticity and provenance of AI-generated content and to protect personal data privacy.

Watermarking involves embedding a unique, detectable signal into AI-generated data, making it identifiable as synthetic. This helps in distinguishing between human-created and AI-generated content, which is crucial in combating misinformation and ensuring accountability.

For instance, Google has launched an identifying and watermarking tool for AI-generated images (Google SynthID), which is more resistant to tampering compared to previous methods. However, challenges remain in creating robust, long-lasting watermarks.

In terms of transparency, new guidelines require clear labeling of synthetic data and disclosure of information about its generation. This includes specifying the datasets used for training AI models, which is essential for ensuring compliance with privacy regulations like the GDPR. These guidelines aim to enhance accountability and fairness in AI usage.

To facilitate compliance with these requirements, technological solutions such as digital identity systems can play a significant role. These systems can help verify the authenticity of the data sources and the identity of the content creators, either for the benefit of users to trace their creation and claim their rights over it, or for the benefit of the general interest by making it possible to trace the author of fraudulent content.

The working group’s research show there are two main uses for digital identity applied to synthetic content in order to resolve specific concerns.

- Firstly, the marking of content created by an individual using digital identification helps to protect the creators’ rights but also to make them more accountable. Leica employed these techniques when creating an on-board system in some of its cameras to generate a digital signature and pair it with photographs to guarantee their authenticity.

- Secondly, digital identification could be used to secure access to content distribution media (synthetic or otherwise) through accounts certification.

In detail: Synthetic content tagging by digital identity

Digital identity could be used to electronically 'sign' works and enable them to be tracked, which would be particularly useful for creators. Watermark technologies should, in such case, be used to enable individuals to sign their creations with a certified, machine-readable electronic signature. This authentication is likely to facilitate the author's ability to assert their rights over a creation, or even to 'trace' successive transmissions of their work, or to control any unauthorized duplications.

In addition, the association of a non-fungible token (NFT) with these signatures should make it possible to track the circulation of authenticated creations from end to end, and in particular to benefit from a “droit de suite” (a right to follow) through a smart contract, i.e. a right to share in the proceeds of any sale of their creations, after the first transfer by the creator or their successors in title. It is possible to attach any creation to an NFT whose intelligent contract automatically generates remuneration for the benefit of the initial creator according to predetermined terms and conditions for every new creation transfer.

The establishment of such “droit de suite” would be significantly broader than existing legislation (such as French legislation) and could automatically cover any creation, including those not eligible for copyright.

Recommendation

We recommend to enable the creation, via the digital identity systems, of a machine-readable electronic signature in the form of a watermark that can be applied to individuals' digital creations.

Moreover, affixing such an electronic signature to synthetic content would also enhance the accountability of content creators, by linking a creation to its author without difficulty, and would therefore help to punish any illicit use of AI Generators to create fraudulent content.

However, there is a possibility that such an obligation could be disproportionate to the desired aim. The obligation to 'sign' a creation could affect individuals' right to freedom of expression when they create content.

In addition, digital creations are easy to reproduce. As a result, it could be very complex for a creator to claim the right to withdraw his/her creation and any identified author of a digital creation would be almost definitively and irremediably associated with it. It could generate some serious issues if its work is misappropriated, for example, or used maliciously.

But the marking would help owners to know whether their works have been used as model training data. The verification of digital content ownership is meant to serve as an opt-out, indicating that a third party is penally liable if it uses content to train a model without the owner's prior approval.

Recommendations

We recommend to enable pairing with an NFT system that would allow creators to manage their rights and the conditions of transmission of their digital creations.

We recommend that, in any case, such functionality (NFT, Watermarking) should be kept as an option to be chosen/used by the individual.

In detail: Certification of social network accounts by digital identity

Social networks are one of the most efficient media for the dissemination of content, including therefore illegal content, whether synthetic or not.

It should be noted that the dissemination of illegal or fraudulent content on these networks can be facilitated by the sense of anonymity that exists on social networks and the Internet. However, it should be stressed that creating real anonymity on social networks is complex for non-professional users and many people use their real identity on social networks. Anonymity therefore remains essentially illusory on social networks.

The creation of an obligation to certify social network accounts can be seen as a measure to make users more accountable, to simplify the procedures for identifying account holders, and above all to enable the application of sanctions appropriate to the commission of online crimes.

Mandatory certification of social networking accounts provides an immediate and direct answer to the question of how to identify an account holder. It also enables judicial authorities to impose real sanctions, such as exclusion from one or more social networks, in the event of offenses committed on them. Such sanctions are particularly appropriate in the case of offenses committed by minors on social networks, such as online harassment. In the absence of certification, it is easy to circumvent the closure of an account by creating alternative accounts.

However, such an obligation and its justifications must be weighed against the negative impact it could have on freedom of expression and the right to privacy.

The right to pseudonymity on networks should be preserved in order to allow free and full freedom of expression. It should also be noted that the requirement to have a digital identity system in order to create a social network account could undermine the freedom of some people to access these services if they do not have such a digital identity. However, the use of a digital identity system should remain an option for individuals to choose.

As it stands, it appears that the only real benefit of introducing a requirement to certify social networking accounts would be the ability to enforce a judicial social network ban automatically and effectively.

It should be underlined that it would be a major step forward in protecting vulnerable people by significantly reducing the ability of cyber criminals to easily create one or more accounts. However, this is based on the assumption that the regulation of illegal content should be done at the level of individuals rather than at the level of the platforms themselves. And an individualized approach seems to us to be less effective than a globalized approach at the level of the platform itself.

Without questioning the status and limited liability of content hosts, it should be emphasized that platform publishers have tools and resources that should enable them to detect and regulate illegal content effectively and simply. This point of view is supported by recent European regulations which impose obligations on platforms to moderate content posted through them. These moderation obligations are essential and can largely be carried out with the help of artificial intelligence systems.

As an illustration we would like to enhance that recently, the Belgian Conseil Supérieur de l'Audiovisuel (CSA) successfully monitored the accessibility of pornographic content on Twitter, particularly concerning the exposure to minors. This effort highlighted the platform's failure to meet its obligations in protecting young users from inappropriate content. The CSA utilized an AI-based solution for detection and moderation, demonstrating its effectiveness in identifying and managing such content.

Recommendation 

We recommend the deployment of AI solutions, with human monitoring, to detect, report and even automatically remove illegal content in the most extreme cases.

AI tools, capable of analyzing vast amounts of data and detecting explicit material, proved crucial in this initiative. These tools are indeed capable to scan and filter content in real-time, ensuring that inappropriate material is flagged, which could allow a prompt removal if the flagging is confirmed. The success of this monitoring operation by the Belgian CSA showcases the potential of AI in enhancing content moderation on social media platforms, ensuring safer online environments for users, especially minors.

Recommendation 

We recommend that measures (to enforce judicial social network bans automatically and effectively) be deployed by content hosts and platform publishers, such as AI-assisted detection and removal tools. The deployment of these tools must not result in a transfer of responsibility from content creators and publishers (who must remain responsible for the content they create and/or publish) to hosting providers, and in particular social networks. Otherwise, the deployment of these measures could come up against resistance from content hosts.

It also demonstrated the need for robust AI-driven solutions in content moderation and compliance with regulatory standards. Identifying and removing, or at least flagging up for rapid removal, illegal content would seem to be a more effective and urgent way of protecting the public, and minors in particular, than identifying users of social networks.

The conclusion on this point is that, as it stands, certification of social network accounts via a digital identity is a less appropriate response to the problem of protecting minors and vulnerable people on platforms than the introduction of monitoring by these platforms to moderate the content posted by users.

Recommendation 

We recommend that any identity certification system on social network should be implemented in compliance with the following measures:

- **The certification system must guarantee the anonymity of the user with respect to the platform, in line with the principle of double anonymity (cf age verification). The identity of the user must be hidden from the platform, and the certifier must not know which account is associated with which identity. Cross-checking can only take place in application of a judicial or administrative decision and in certain specifically identified cases.**

- **There must be an alternative to the use of a digital identity system for this certification.**

Interview with Cédric O: What is the responsibility of creating synthetic content generated by artificial intelligence?

Cédric O was an advisor to French President Emmanuel Macron from 2017 to 2019 and Secretary of State for Digital Affairs between 2019 and 2022. He is now co-founding advisor to Mistral AI and a member of Artefact's board of directors.

Cédric O

In an interview held on May 7, 2024, Cédric O shared his perspectives on the digital identification of synthetic data.

The encryption of images generated by artificial intelligence as a means to slow down the spread of false information.

According to Cédric O, with artificial intelligence, the difference between what is true and what is not is going to be extremely difficult. In the case of text, it takes several pages of text to effectively detect an identifiable pattern. On a single paragraph, for example, this is very tricky. For an image, even if it is encoded, we can take a photo of the original image and the encoding becomes inoperative. The former French Secretary of State for Digital Affairs does not believe in technical solutions for encoding images, as there will always be ways of hijacking them. However, encoding may indeed be an element in slowing down the problem, but it won't be the solution.

It is likely that the media's credibility will depend on the vector through which it is disseminated. If it's a reference newspaper with a demanding fact-checking policy, then the information will be labeled as true, but if the information is obtained through a third party, it will be false by default. The burden of proof is reversed.

> “Image encoding may indeed be an element in slowing down the problem, but it won't be the solution to the problem.”

Certification of social networking accounts as a solution to the fight against false information

Cédric O considers that identification on social networks with a system of account certification is probably unavoidable in view of current abuses, even if it poses numerous technical and political problems. It would probably make it easier to tackle cyber-harassment and online hate, and reduce young people's access to problematic content. The level of identification might depend on the case in question.

> We have a real problem with the children. We need to know the age of the person coming onto the account. We need to be sure that Juliette Martin is under 7, not that it is 7-year-old Juliette Martin who is behind it.

He points out, however, that this will take time, such a solution must be planned on a European scale (to be effective), and its application must be the responsibility of an independent authority. Indeed, the issue of control by the State and competent authorities over freedom of expression on the Internet should arise in the case of certification of accounts.

> It's politically delicate to say that we want to tackle online anonymity. But we have to be clear: the current system is not working, and abuses are increasing. Furthermore, it is impossible to make it work on a large scale, both for technical reasons (the mass of content to be sanctioned is such that it would be necessary to be able to automate sanctions) and for reasons of judicial cooperation (which does not work).

Certification of social networking accounts as a solution to the fight against false information

Cédric O considers that identification on social networks with a system of account certification is probably unavoidable in view of current abuses, even if it poses numerous technical and political problems. It would probably make it easier to tackle cyber-harassment and online hate, and reduce young people's access to problematic content. The level of identification might depend on the case in question.

Encoding creations using artificial intelligence as a means of protecting copyright

The former French Secretary of State for Digital Affairs believes that watermarking of artist-generated content would be relevant to control the origin of specific artistic creations for copyright issues.

RECOMMENDATIONS SUMMARY

- **We recommend:**
  - **to enable the creation**, via the digital identity systems, **of a machine-readable electronic signature** in the form of a watermark that can be applied to individuals' digital creations.
  - **to enable pairing with an NFT system that would allow creators to manage their rights** and the conditions of transmission of their digital creations. We recommend that, in any case, such functionality (NFT, Watermarking) should be kept as an option to be chosen/used by the individual.
  - **the deployment of AI solutions,** with human monitoring, to detect, **report and even automatically remove illegal content in the most extreme cases**.
  - that measures (to enforce judicial social network bans automatically and effectively) be deployed by content hosts and platform publishers, such as AI-assisted detection and removal tools. The deployment of these tools must not result in a transfer of responsibility from content creators and publishers (who must remain responsible for the content they create and/or publish) to hosting providers, and in particular social networks. Otherwise, the deployment of these measures could come up against resistance from content hosts.
  - that any identity certification system on social network should be implemented in compliance with the following measures:
    - The certification system must guarantee the anonymity of the user with respect to the platform, in line with the principle of double anonymity (cf age verification). The identity of the user must be hidden from the platform, and the certifier must not know which account is associated with which identity. Cross-checking can only take place in application of a judicial or administrative decision and in certain specifically identified cases.
    - There must be an alternative to the use of a digital identity system for this certification.

CONCLUSION

The exploration of digital identity (Digital ID) systems detailed in this report, underscores the critical need for trustworthiness and individual empowerment in their implementation. Through the examination of four pivotal use cases—online protection of minors, health, electronic voting, and authentication of generative AI content—several key insights and recommendations have emerged.

The deployment of age verification systems highlights a complex interplay between safeguarding vulnerable populations (such as minors) against harmful and/or illegal content and protecting individual privacy. Effective solutions must balance these needs through robust, privacy-preserving technologies like double anonymity systems. It is crucial that such measures be free, simple, and reliable to gain public trust and achieve widespread adoption.

Digital identity systems present significant opportunities to enhance patient care and individual autonomy over health data. Implementing the Principle of Least Privilege (PoLP) ensures that only necessary data is accessible to healthcare providers. The integration of lifestyle data with traditional health records, under full control of the individual, can further optimize medical care while maintaining privacy and security standards. Additionally, digital identity systems should empower individuals to share their health data voluntarily for altruistic purposes, such as medical research and public health initiatives. This ability to contribute to the greater good while maintaining control over personal information can enhance trust in digital identity solutions and foster a culture of data altruism, where individuals willingly contribute to advancements in healthcare and scientific knowledge.

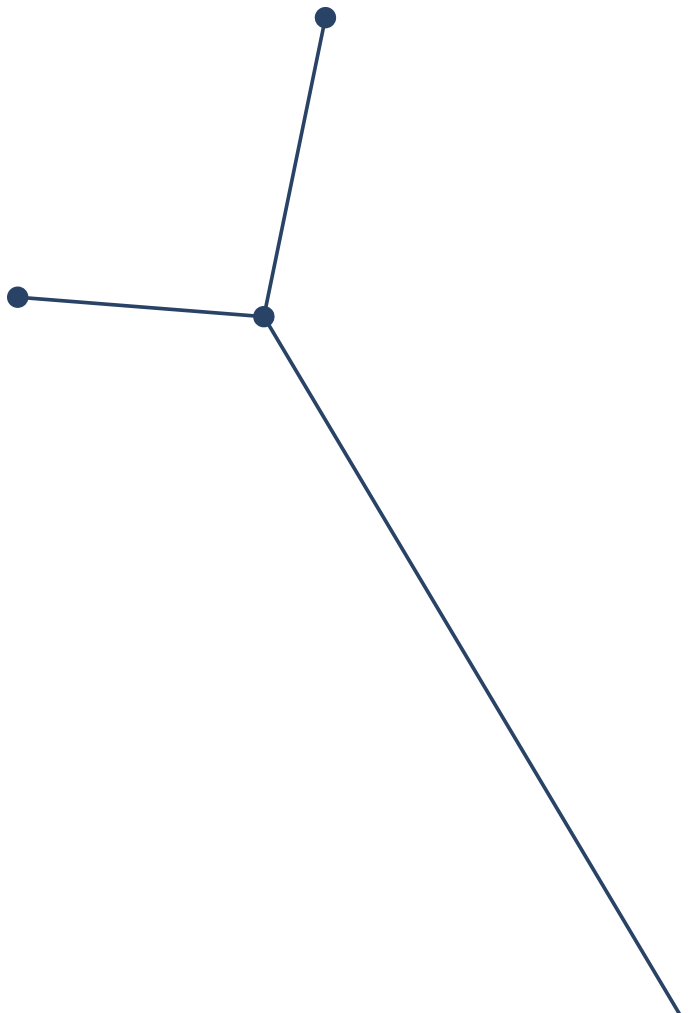
While remote electronic voting can increase accessibility and inclusiveness, it also poses significant challenges in ensuring voter confidentiality and preventing undue influence. Pilot deployments and impact studies are recommended to develop technical solutions that uphold the principles of democratic integrity, such as confidentiality, freedom of choice, data security, and voter privacy. Promoting international interoperability of digital identity systems will also support more inclusive democratic processes, especially for non-citizens eligible to vote in local elections.

The rise of generative AI technologies presents both opportunities and significant challenges, particularly concerning the traceability of digital content. Digital identity systems offer a promising solution to enhance such traceability. By incorporating unique, machine-readable watermarks and digital signatures, these systems can effectively distinguish synthetic creations from human-created content, thus supporting efforts to prevent misinformation and enhance content integrity. However, the implementation of digital identity systems is not without its challenges. Privacy concerns are paramount, as the requirement to digitally sign or mark content could potentially infringe on individual rights to privacy and freedom of expression. Balancing the need for accountability with the protection of user anonymity is crucial. This delicate balance is essential to prevent misuse and protect the rights of creators and users alike while respecting everyone’s privacy and liberty of speech.

Additionally, to avoid user confusion and hinder widespread adoption there is a critical need to develop multi-purpose digital identity systems that streamline data governance, reduce complexity, and enhance user acceptance. These systems should be designed to minimize data duplication and environmental impact, promoting sustainability and efficiency in digital identity management.

To conclude this report, we would like to insist on several overarching themes which were identified within this report and our previous report “Universal Digital Identity Policy Principles to Maximize Benefits for People”. Digital identity systems should be people-centered, inclusive, voluntary, resilient, intuitive, privacy-focused, empowering, user-controlled, based on informed consent, trustworthy, transparent, accountable, secure, interoperable, and future-proof. Adhering to these principles will be essential in overcoming the pervasive ambivalence and distrust surrounding digital identity.

Ultimately, the success of digital identity systems hinges on their ability to enhance the digital experience while safeguarding fundamental rights and freedoms. By addressing the nuanced implications of digital identity in our interconnected world, we can pave the way for a future where these systems serve as foundations for empowerment, trust, and protection in the digital age. This report aims to provide recommendations for achieving these goals as regard to four use cases, offering targeted recommendations to maximize benefits and address identified challenges.



APPENDIX: CASES STUDIED

AGE VERIFICATION AND PROTECTION OF MINORS

Queensland Mobile Driving (Australia)

The Digital Licence is an app that can store Queensland citizens' identifications easily on their mobile devices. With the Digital Licence they can share their information safely and securely, such as when picking up postage, entering a club or pub, and everytime identity check is needed. The application can perform Proof of Age verification and any citizens in possession of photo identification card / Adult proof of age card are eligible to the Digital Licence app. Following a series of successful pilots and trials with a user satisfaction of 94 per cent , the solution has been rolled-out at state-level since November 2023.

GBG Age Verification (UK/USA)

GBG's age verification is a solution designed to prevent underage individuals from accessing age-restricted content, services, products, and venues, ensuring protection for both minors and businesses. It offers a variety of verification methods to provide customers with multiple options, complies with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, and is designed to be fast and hassle-free to improve customer experience. The age verification process is backed by comprehensive global data sources for quick and secure verification, employs advanced document authentication technologies like FaceMatch and liveness checks, and helps in safeguarding against identity fraud. It includes a Venue ID Scanner feature to quickly detect fake, forged, or counterfeit IDs.

Greenbadg (France)

The Greenbadg project proposes a universal and secure multi-use badge for instant authentication. The badge has a range of applications, including mobility, ticketing, access control, KYC enrolment, age verification, login and payment. The user downloads the application, creates an account with a valid ID, and then obtains a GreenBadg after a rigorous identity check. The badge can be used physically or digitally, generating a QR Code for real-time visual authentication or digital authentication via selfie comparison. Identity on Greenbadg is verified at the time of registration with a valid ID, followed by a rigorous verification based on artificial intelligence (AI) carried out by Vialink.

Proof-of-majority solution, Docaposte (France)

Docaposte, the digital subsidiary of the La Poste group, is experimenting a proof-of-majority solution to limit access to adult sites to under-age users. Developed as part of the Government's Child Protection Laboratory, this solution aims to protect minors while respecting user anonymity. It offers a choice of several identification methods and ensures double anonymity: a process where both parties involved in an interaction remain anonymous to each other, which means neither the identity of the users nor the visited sites are traceable. It should be noted that this solution is currently at the proof-of-concept stage (need to see if the solution is viable) and is not yet available. Hosted in Docaposte's data centers in France, the solution includes a digital platform and a mobile application.

Available identification methods include La Poste's Digital Identity, an identity document (via remote verification service), or a Mastercard credit card number. Additionally, the solution respects CNIL (National Commission on Informatics and Liberty) principles for privacy and youth protection. Docaposte, known for its expertise in online identity verification and as the leading health data host in France, plans to integrate this solution in 2024 for other online services requiring secure age verification. The current experiment extends beyond adult sites, covering areas such as violent or adult video games and online sales of alcohol and tobacco, thereby meeting the needs for minor protection and legal compliance.

Zero Knowledged Proof Explonatory (France)

The Laboratory of Digital Innovation of the French National Information Science and Liberties Commission (Commission Nationale de l'information et des libertés, CNIL), proposed a way of verifying the age of online users while preserving their privacy. The initiative aims to enable the verification of an individual's majority without disclosing their age or identity, thus facilitating access to certain sites while protecting personal information. The French National Information Science and Liberties Commission has developed a demonstrator presenting an « ideal » solution for age verification, based on cryptographic concepts such as « zero-knowledge proof ». It is a protocol that allows one party, known as the prover, to prove to another party, the verifier, that a certain statement is true, without revealing any information other than the truth of the statement itself.

This mechanism enables proving a real situation without revealing information related to that situation, thus ensuring the protection of the individual's identity and data minimization. The combination of digital signatures and zero-knowledge proofs can be used to generate a public key, add members to the group and certify the age of users without revealing the identity of the age certification authority.

HEALTH

AADHAAR (India)

India created the world's largest voluntary biometric identity system using faceprints, face and eye scan. Aadhaar, meaning "foundation," was put in place in 2009 as a centralized application to allow every resident of the country to easily establish their identity. It is a system based on a 12-digit unique identification number issued to every resident of the country. It is used to ensure uniqueness during registration and for cloud-based authentication. Individuals authenticate using their Aadhaar number in combination with demographic data, a fingerprint, an iris scan, or a one-timepassword (OTP). By late 2021, the Unique Identification Authority of India reported that 1.3 billion people, or roughly 99% of Indian adults, had enrolled in Aadhaar.

A number of welfare schemes for delivering healthcare to marginalised sections of societies are mandatorily linked to Aadhaar at present, in order to ensure targeted delivery of healthcare benefits to eligible recipients. While other IDs may also be used by individuals for the purpose, one can choose to link Aadhaar to the national health ID 'ABHA' (Ayushman Bharat Health Account), that has been implemented by the government as part of its digital health mission.

Aadhaar has played an instrumental role in improving access to healthcare for the populace by ensuring effective delivery of government healthcare schemes, and facilitating registration under the ABHA scheme.

Further, Aadhaar has aided streamlined management of health records and enabled interoperability between databases in acting as a common linkage. As a unique digital identifier, Aadhaar has not only facilitated accurate delivery of healthcare benefits to specific segments of society but also empowered individuals in enabling them to access their health information to make informed decisions.

India's 2019 "State of Aadhaar Report", which surveyed 167,000 users, found that 92% of respondents were satisfied with how the system worked. The results are an indication of the power that digital identity can have when harnessed for social good.

WHO digital health initiative (WHO/European Commission)

A crucial aspect of the European Union's response to the COVID-19 pandemic has been the implementation of the digital COVID certificate. To enable free movement within its borders, the EU promptly established interoperable COVID-19 certificates, known as the 'EU Digital COVID Certificate' or 'EU DCC.' Utilizing open-source technologies and standards, this system also allowed non-EU countries issuing certificates according to EU DCC specifications to connect, making it the most widely adopted solution globally.

From the beginning of the pandemic, the World Health Organization (WHO) worked with all WHO Regions to establish overall guidelines for such certificates.

To enhance global health preparedness in response to increasing health threats, the WHO is creating a global digital health certification network, building on the robust foundation of the EU DCC framework, principles, and open technologies. Through this collaboration, the WHO will facilitate the global implementation of digital certificates under its own structure, aiming to enable worldwide convergence. This includes setting standards and validating digital signatures to prevent fraud. Importantly, the WHO will not have access to any underlying personal data, which will remain under the exclusive control of governments.
The first component of the global WHO system is operational since June 2023 . The main goal of this initative is to establish a global system that will help facilitate global mobility and protect citizens across the world from on-going and future health threats, including pandemics.

BC Services Card (British Columbia, Canada)

BC Services Card can be used to access a variety of government services, including to view one's B.C. health records in one place, including lab test results, medications, health visits, immunizations and more. The main idea is to have many services gathered in one card. You can use this BC Services Card to verify your age when opening a bank account for instance. One key feuture is the respect for privacy since the BC Services Card Program can not see the information a government service saves about you.

A service, such as a health care organization, may save some of your information but it is never shared between services. For example, police officers can not see your health records or medical history and doctors can not see your driving record . The data minization principle is well respected. Finally, the card helps to prevent theft and fraud by design.

"Mon Espace Santé" (My Health Space, France)

My Health Space is an individual digital space made available by the French government and the French National Health Insurance to enable all citizens to store their medical information and share it with the healthcare professionals who treat them. My Health Space includes:

- A medical profile to enter information about your health and medical situation: age, weight, vaccinations, medical history, advance directives and blood group.
- A shared medical file to store and share your health data with your healthcare professionals: prescriptions, test results, hospitalization reports and medical images.
- A secure health messaging system for secure communication with your healthcare professionals.

Pass Santé Mousso (Ivory Coast)

"Pass Santé Mousso" is a digital health record system that allows patients to store all their medical and personal information in one place, accessible at any time via a web and mobile application.

The system also uses a physical medium, such as a bracelet, medallion or card, to facilitate access to medical information in the event of an emergency. It gives healthcare professionals rapid access to vital medical information in the event of an emergency, such as medical history, allergies, medicines being taken and emergency contact details.
The system also allows patients to track their health over time, recording data such as blood pressure, blood sugar levels and body temperature.
It uses advanced security technologies to protect patients' medical information and prevent unauthorized disclosure of personal information. Patients can also control the information shared with healthcare professionals and can withdraw access at any time.

"**E-carte vitale" (Carte Vitale App, France)**

The aim of the carte Vitale app is to simplify relations between healthcare professionals and policyholders. While providing the same functions as the Vitale card, the carte Vitale app offers new advantages:

- Patients are more likely to have their Vitale card with them on their smartphone, so there is always a guarantee that they will be able to make a teletransmission transaction.
- Healthcare forms are secure and reliable thanks to automatic access to the ADRi rights service, reducing the risk of errors and rejected invoices
- The risk of hand-carried contamination is reduced.

The carte Vitale app is a digital tool, providing access to all the services and functions offered by the "Assurance Maladie" (French Health Insurance), such as Sesam Vitale invoicing, access to the AMO's integrated teleservices and, for pharmacists, the pharmaceutical record (DP). In addition to the patient and beneficiary identification data already present on the Vitale card, the Carte Vitale app can be used to integrate new data: the national health identity (INS), eventually, data from complementary health insurance organizations or lifestyle data collected by a smart watch (eg. Fitbit).

Fitbit (USA)

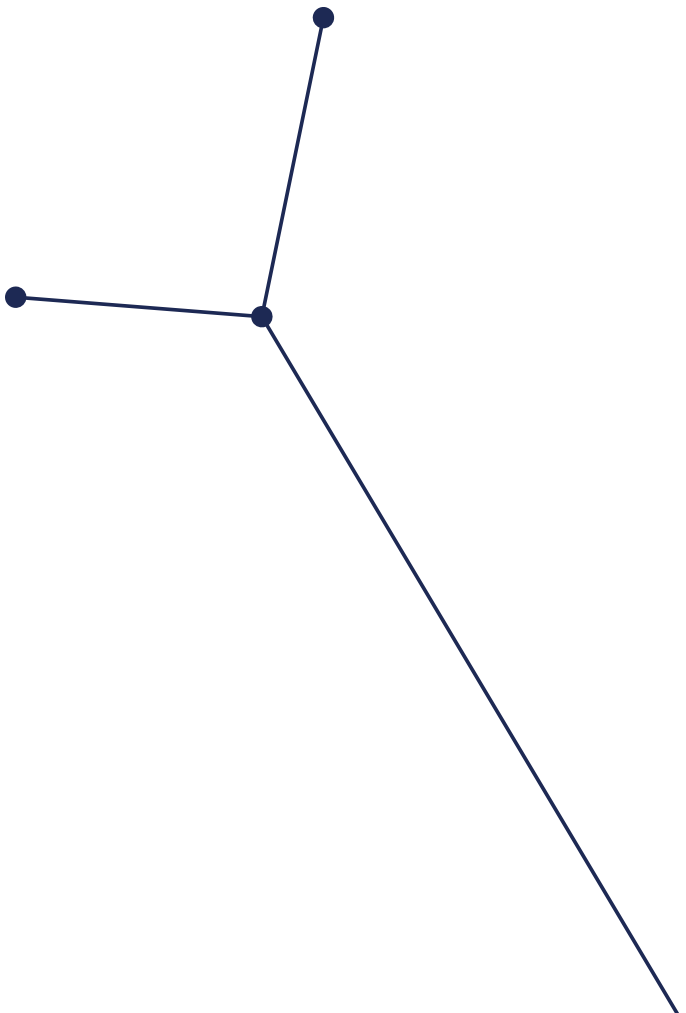
Fitbit is one of several lifestyle/health technologies that include or are integrated with wearable devices as fitness and activity trackers. The data automatically collected by Fitbit (to the extent enabled) include heart rate and rhythm (ECG), blood oxygen, hourly activity, steps/distance/pace and GPS location, floors (stairs) climbed, sleep activity, and calories burned. Generally, limited data is held on the device, with the bulk of the data being synched with and stored on Fitbit's servers. The data can be shared with other health and fitness applications, such Google Health Connect (and Google Fit, which Google has announced will be discontinued in 2025), Apple Health and BetterMe.

In addition to health and fitness data, it is also notable that certain devices from Fitbit, which was acquired by Google (announced in 2019 and completed in 2021), allow contactless payment through "Fitbit Pay", which is to be replaced in July 2024 with Google Wallet, both of which are tied to certain of the user's financial accounts and transaction information.

Fitbit devices can also allow the installation of additional third-party entertainment, lifestyle, and other applications.

Other than data shared with other applications (as described below), access to an individual's Fitbit data is through either a unique Fitbit account and password (though Google has announced that this will be discontinued in 2025), or the individual's Google account. Any new users (and for existing users of the Fitbit login after support is discontinued) will be required to use a Google account.

Access by to an individual's Fitbit data by other applications requires use of the OAuth 2.0 Authorization Framework, but Fitbit does not specify developer requirements for greater security/authentication control (though does recommend – but does not require – use of Authorization Code with PKCE for developers). Access to the data once in those applications would be through, and authenticated in accordance with the requirements of, those applications.



VOTING AND ELECTIONS

K Voting (South Korea)

South Korea will establish an online voting system based on blockchain technology as part of a government project to innovate public services using this advanced digital technology. Blockchain has been identified as a key digital technology because of its decentralized storage system that ensures the accuracy and security of data, generating trust without the need for a reliable third party. This initiative is part of South Korea's on-going efforts to integrate reliable blockchain-based services into the public sector. The new voting system will help election authorities to securely and electronically store the voting process and results on a blockchain, preventing any falsification or alteration of documents. This system is a continuation of a revised law allowing electronic referendums. Although South Korea launched an online voting programme in 2013, it has only been used for elections of leaders in political parties, public institutions and schools. The government will invest $1.1 million this year to improve the blockchain voting system, and will increase this budget in 2023.

Digital Identity, La Poste (France)

La Poste Digital Identity gives access to more than 1,300 services available via France-Connect, those of La Poste and others. La Poste Digital Identity is the first and only electronic identification system in France to be certified by ANSSI (National Agency for Information Systems Security) as meeting the substantial guarantee level of the European eIDAS regulation (digital equivalent of presenting an identity document in person and allows you to confirm remotely one's identity). La Poste's digital identity can be used to make online voting proxies.

AADHAAR (India)

India created the world's largest voluntary biometric identity system using faceprints, face and eye scan. Aadhaar, meaning "foundation," was put in place in 2009 as a centralized application to allow every resident of the country to easily establish their identity. It is a system based on a 12-digit unique identification number issued to every resident of the country. It is used to ensure uniqueness during registration and for cloud-based authentication. Individuals authenticate using their Aadhaar number in combination with demographic data, a fingerprint, an iris scan, or a one-timepassword (OTP). By late 2021, the Unique Identification Authority of India reported that 1.3 billion people, or roughly 99% of Indian adults, had enrolled in Aadhaar.

Voters can voluntarily link their voter identity cards to Aadhaar, and the Election Commission of India has proposed linking the Aadhaar database with the voter ID database to effectively address election fraud and registration errors. Aadhaar is well-equipped to render voting more accessible to marginalised sections of societies, in enabling streamlined registration of voters via linking of Aadhaar cards and potentially facilitating increased voter participation through Aadhaar-based voting mechanisms such as biometric authentication. Such authentication also will help effectively address the occurrence of electoral fraud in relying on Aadhaar as a unique digital identifier to verify voter identity.

However, Aadhaar-based voting also gives rise to credible concerns of state surveillance and violation of voter privacy, given the extent of governmental access to citizens' personal data, including biometric information. The risk of cyber-attacks and unauthorised access to Aadhaar databases given the extent and sensitivity of demographic data that is stored. There have been various instances of alleged data leaks and Aadhaar databases being compromised and the need for undertaking more robust assessments, cybersecurity measures and implementation of security protocols by private parties handling Aadhaar data has been voiced by stakeholders on multiple occasions. It is critical to acknowledge and aim to address these risks in considering any voting system linked to Aadhaar, in order to ensure greater accountability and transparency.

E-voting (Switzerland)

E-voting is part of the Swiss government's strategic plan for e-Government, involving close collaboration between the Confederation and the cantons. Since 2004, 15 cantons have offered online voting to a limited proportion of their electorate in over 300 Proofs Of Concept (POC). The identity verification process is based primarily on the use of voter identification cards and personal verification codes.

In addition to data protection, financing is the most significant obstacle for e-voting. Each canton faces a basic fee for the system's use and operation, along with variable costs.These variable costs depend on the total number of voters in a canton and the percentage eligible for e-voting. However, Swiss Post does not disclose specific figures.

The nationwide implementation of e-voting would follow the standard legislative procedure, necessitating parliamentary approval and, potentially, a public referendum. The timeline for this process is currently uncertain.

I-voting system (Estonia)

In Estonia, I-voting, or electronic voting, allows citizens to cast their votes via the Internet using a computer with an Internet connection and an ID-card or mobile ID with valid certificates. Estonia was the first country in the world to implement I-voting in national elections, and it has been offering secure I-voting since 2005. Nearly half of Estonian voters used "I-voting" to vote during the last European Parliament elections in 2019. In the wake of the COVID-19 pandemic, the Estonian system has proven to be not only convenient but also a valuable tool to support public health measures. The Estonian I-voting system allows people to exercise their democratic rights without putting public health at risk.

Estonia's I-voting system has been subject to security analysis, and it has been found that more than 30% of the country's ballotsare cast online.

Smartmatic-Cybernetica Center of Excellence for Internet Voting (SCCEIV, Norway)

Norway experimented with online voting for local elections in 2011 and parliamentary elections in 2013, apparently with mostly positive feedback from voters.

However, subsequently, Norwegian voters did not have the option to vote online. There seem to have been isolated cases of online voting usage afterwards, such as in the county of Innlandet in Norway which held a referendum using an online voting system in 2022.

The online voting system was tested with ID Porten (the "ID Gate"), a platform used by citizens to access government services online in Norway, which relies on several independent ID services:

- Bank ID – the dominant services, provided by the bank sector in cooperation (one ID for all banks and other services). Comes in two versions; one app based for use on smart phones and one with a dedicated code device.
- MinID (my ID) – provides codes per paper mail. Publicly supplied.
- Ecard (now discontinued, replaced by Bypass ID and Commfides based on USB pin)

The Innlandet county referendum in 2022 was online only and made several findings:

- voting participation was high (46,7% against a normal of 20-30% for similar referendums)
- older voters struggled with the technical practicalities due to lack of digital ID – reduced participation
- coordination with the national citizen register was challenging (required to verify eligibility for voters)
- quite a few technical complications arose, and the voting system had down-time

The Covid 19 pandemic was part of the online only motivation.

Onelogin - Quest (USA)

Multi-factor authentication (MFA) by implementing sophisticated AI. This helps in over- coming the weaknesses associated with traditional password-based authentication. The AI-powered solution explores risk-based authentication, evaluating factors beyond just passwords, like the user's past login behavior and contextual information (e.g., login location or device used). By comparing past and current authentication attempts, the AI provides a more robust authentication method that adapts to evolving cyber threats.

THE DIGITAL IDENTIFICATION OF SYNTHETIC DATA

Leica M11-P credential system (Germany)

The Leica credential system, introduced with the Leica M11-P camera, embeds Content Credentials into images at the point of capture. This system follows the global Coalition for Content Provenance and Authenticity (C2PA) standard, ensuring each image carries secure metadata such as the camera make, model, who captured the image, and when. Each image receives a digital signature for easy verification of authenticity either on contentcredentials.org/verify or the Leica FOTOS app. This initiative, part of the Content Authenticity Initiative (CAI), aims to combat misinformation, ensuring a chain of authenticity from camera to cloud, and helping creators maintain control over their work.

Google Synth (USA)

Google SynthID is a novel tool developed as a collaboration between Google DeepMind and Google Cloud, aimed at identifying and watermarking images generated by artificial intelligence (AI). The tool embeds a digital watermark directly into the pixels of an image, making the watermark imperceptible to the human eye, yet detectable for iden- tification purposes. This watermarking capability provides a means to trace and verify the origins of AI-generated images. Google has released a beta version of SynthID to a limited number of Vertex AI customers using Imagen, a text-to-image model. The beta release signals the initial step towards providing a robust solution for identifying AI-generated content.

Human Technology Foundation
222, rue du Faubourg St-Honoré
75008 Paris
contact@humantechnologyfoundation.org

HTF HUMAN TECHNOLOGY FOUNDATION

JULY 2024