Preserving Privacy with Technology
A data protection analysis of the Nym mixnet

No Author Given

No Institute Given

Abstract. We argue privacy-enhancing technologies can form the basis for the emphasis of the GDPR on self-determination when it comes to personal data. We investigate one of these privacy-enhancing technologies in light of the GDPR: the Nym mixnet, a technology to anonymize network-level communication. We demonstrate how the Nym mixnet can serve as an example of data protection by design and default for data processors. The network layer is often left out of data protection, but we argue is required for data protection, and has wider ramifications for the realisation of the right to privacy as technologies such as the Nym mixnet can go beyond the limited paradigm of individual consent by providing a more robust technical materialisation of fundamental rights and principles, going beyond even the GDPR as shown by frameworks such as the right to digital integrity that enshrine a fundamental right to be free of surveillance..

Keywords: privacy, data protection, digital integrity, mixnets

1 Introduction

Regulation such as the General Data Protection Regulation (GDPR) seeks to mitigate the negative consequences of data-driven surveillance paradigm, such as involuntary data collection and discrimination. However, how can particular privacy-enhancing technologies be effective in realising the goals of the GDPR in Europe? As a case study, we present a technological approach using the Nym mixnet for shifting the paradigm of the digital economy by radically reducing the collection and processing of personal data through technical means [6].

Although the problem of data protection is multi-layered, this case study is important as the Nym mixnet provides protection at the lowest level of data, the network layer of core internet protocols like TCP/IP and UDP. These protocols are used by *every* application to send data across the internet, but the network protocols themselves leak IP addresses and other metadata. Although IP addresses may not considered personal data by some, IP addresses should be considered personal data insofar as an IP address can identify or contribute to the identification of an individual via algorithmic inference. Likewise, the timing and volume of packets can also be used to indirectly identify individuals. The rise of artificial intelligence (AI) algorithms that can process network data on a large scale and infer personal data from this data makes using these kinds of

network-level protections increasingly urgent. Yet very few technologies can help protect this personal data via data minimization. Thus we investigate the Nym mixnet, an anonymous overlay network built to enforce data minimisation on the network level, and how this technology contributes to other data protection requirements in the GDPR beyond data minimisation.

2 The Market of Privacy-Enhancing Technologies

The GDPR is a regulatory intervention into the digital economy to stem the prevalence of data-markets and business models based on the involuntary gathering, processing and exploitation of personal data. Its principles were meant to guarantee the self-determination over personal data, protecting the rights of people to have a say in what is known about them and by whom, but these have been far from realised in practice. Admittedly, it takes time for markets to respond to regulation, but in the years that have passed since the GDPR came into effect the response has been underwhelming (if not outright undermining) of the intended principles. Market actors have largely responded with minimum compliance while all else remains the same. From the perspective of ordinary people, the effects of the GDPR have unfortunately manifested themselves in terms of malicious non-compliance that *appears* to comply in the form of cumbersome cookie-settings and inscrutable service agreements. The GDPR, by focusing on individual consent and data protection, has resulted in the burden of responsibility being placed on individual consent in a context where this cannot be meaningfully enacted. However, the novel characteristics of digital mass surveillance lies in its relational and collective nature: "Some seek to reassert individual control for data subjects over the terms of their datafication, while others aim to maximize data-subject financial gain. But these proposals share a common conceptual flaw. Put simply, they miss the point of data production in a digital economy: to put people into population-based relations with one another. This relational aspect of data production drives much of the social value and harm of data collection and use in a digital economy" [16] This means that relying solely on the consent of the individual remains largely ineffective for realising the principles of the GDPR, protecting the right to privacy as well as reducing the overall harm of data collection. Personal data is not just personal, it also operates as statistical information revealing patterns about populations that can surface particular profiles as targets [1]. On the technical level, even when personal data is encrypted and protected, patterns of communications and its metadata can be used to effectively deanonymize, profile and target people as well as reveal sensitive information about systems and infrastructure [5]. What is needed is a collective and technological approach, whereby the principle of data minimization is fulfilled in the technical implementation of the communications infrastructure itself through privacy by design.

There is currently a missed opportunity, both on the side of regulators as well as market actors, to address the GDPR as an impetus towards an alternative innovation pathway, in which technologies can play the role of a material

realisation and enforcement of fundamental rights. Regulators and technologists are typically pitted against one-another with technological innovation perceived as a linear competitive race and regulation as hindrances and constraints on the racetrack. However, insights from the social sciences and history demonstrate how technological innovation does not take place in a vacuum removed from social dynamics and is far from a linear process [9]. Rather, technology and infrastructure should be understood as the material manifestation of societal priorities and power-relations [17]. Once built, technologies and infrastructure acts as a material enforcement of these power relations. Technology can – but does not always – then also play the role of a material manifestation of social consensus on what comprises essential needs, functions, and rights. The relationship between technology and regulation is not just one of compliance. Instead, a technological approach can play a key role by acting as a *de facto* materialisation of fundamental rights and legal principles.

3 Data Protection Analysis of Nym

Nym is developing a mixnet to enforce the right to privacy, and thus enable data protection. We present a brief overview of the mixnet, and an GDPR analysis of it. We are supported in our analysis by the General Data Protection Regulation (GDPR), that – amongst other obligations – enforces the obligation to implement data protection by design and by default as per article 25 of the GDPR.[1] Although European legislators have inscribed data protection by design into the GDPR, currently there is a lack of technology to accomplish these goals, and the goal of engineers should be to create software that enforces these fundamental rights by design[3]. It should be noted that Article 5 has data minimisation as an exemplary kind of processing, and it is not strictly required, but we would note that the increased power of algorithmic inference requires more careful minimisation that originally foreseen by the GDPR in order to uphold data protection principles. The presentation at the IFIP Summer School would outline our analysis in terms of the GDPR and ePrivacy Directive and ask for feedback.

To quickly review the GDPR, a *controller* is an entity (possibly a natural person) that determines the means and purposes of processing data as given in article 4(7) of GDPR.[2] In contrast, a *data processor* is an entity that processes data on behalf of a controller. For example, a government website may collect data on citizens and so be the controller but send it to a data processor based on software by IBM. Rather than strictly enforcing a right to privacy, the purpose of the GDPR is to create a regime of accountability for controllers, where users can control the processing of their own personal data via obligations put upon

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[2] Further clarifications are given in *Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor"* WP 169.

the data processor [12]. In other words, data protection is not equivalent to the right to privacy more than an extension of the right to the self-determination in terms of personal data.

In order for there to be even the possibility of the self-determination of data, there must be the possibility to *prevent* the processing of data in the first place, in order to enforce data minimisation and the rest of the principles. It is the preservation of this possibility that creates the right to privacy; this right can be technically enforced by privacy-enhancing technologies that enforce data privacy by design. The data processor bears responsibility to use privacy-by-design as per article 24 and 25 of the GDPR state. In fact, recital 78 of the GDPR states explicitly that: "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfill their data protection obligations." Thus the need to fulfil these obligations goes downstream to data processors.

As controllers are explicitly instructed by the GDPR to use processors that meet GDPR requirements (Article 28(1) and Recital 81 of the GDPR), why does there not yet exist a market for privacy-by-design data processors? Prior work identifies privacy possibilities not just in business-to-business data exchange, but in *privacy protection* consumer market that could supplement the current regime of surveillance capitalism (i.e. 'free' services in return for customer data) as well as future paradigms that are equally privacy-invasive (i.e. the 'own your data' movement where customers must explicitly sell their data in exchange for services). Although there have been concerns that the GDPR should not legislate a market for privacy-enhancing technology into existence [8], the fact of the matter is that the 'market for privacy' itself is still very small and immature at the present moment, for various reasons including the desire for surveillance by data controllers [2]. Nonetheless, this does not change the fact controllers have an obligation to demand privacy-enhancing technologies from their data processors. Network-layer privacy, as provided by an anonymous overlay network, is exactly the kind of privacy-enhancing technologies that a market for privacy should support. In fact, it is of particular importance as privacy on the network-level is a precondition for privacy on higher levels, such as those of Web applications, which would otherwise leak IP addresses and other metadata associated with network traffic.

Of course, technologies need to be judged against the rules for data protection and privacy in the required jurisdictions. Although the Nym mixnet has its mix nodes spread across many different jurisdictions, the Nym mixnet has European users, so the General Data Protection Regulation must be supported. Furthermore, the company that created the Nym mixnet is based in Switzerland, and so must also have adequate data protection in harmony with the GDPR and e-Privacy Directive of the European Union. Although network-layer privacy as

such is not explicitly dealt with in the GDPR, nonetheless, network-layer privacy is an important part of GDPR, as we argue below.

As given in Article 5(1) GDPR, the principles of data protection are: the principle of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. It should be noted that article 25 of the GDPR specifically underlines the data minimization principle, which is defined in Article 5(1)(c) as "limited to what is necessary in relation to the purposes for which they are processed." Note that this includes the initial collection of data, as well as any subsequent data processing. Of course, the purposes, nature, scope and context of the data processing should be taken into account, as well as a risk assessment that takes into account the rights of the natural persons (not just 'data subjects') impacted by the processing.

One oft-forgotten part of the GDPR is that the controller has the responsibility to determine *state of the art* solutions and their costs to determine their usage, which would seem to enforce the idea of data processors using privacy-enhancing technologies like a mixnet being preferred data processors. The GDPR itself provides examples of the usage of privacy-enhancing technologies: pseudonymisation as soon as possible and enabling the controller to create and improve security features, as per Article 32 and Recital 78 of the GDPR. As per Article 24(1) GPDR, "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." This duty is further outlined in Article 28.

Despite Article 24(1) GDPR, the use of privacy-enhancing technologies that provide privacy by default remains limited. Although there are many other privacy-enhancing technologies such as the use of differential privacy in databases, we will focus on the Nym mixnet and show how it enables the principles of the GDPR and thus is an appropriate, and even necessary, technical measure to enforce the GDPR. In the current design of Nym [6], the individuals or organizations that run the service providers (which could be any internet application accessed over the mixnet) are the controllers and the Nym mixnet, as well as credential system used to access the mixnet, are considered data processors under the GDPR. In terms of Article 32(a) and (b) GDPR, Nym in particular satisfies the "encryption of personal data" of any data sent through its network, and has technical mechanisms to "ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

It should be noted that the GDPR does not clearly distinguish between the network that sends personal data and the applications that use the personal data in terms of data processing. We hold that data processing naturally should include both the transfer of data over the network and the usage of the data by a processor, network data such as IP addresses and the patterns of communication can allow the inference of personal data, but it is historically not taken into account by GDPR compliance. However, it should be noted that the Nym mixnet only processes network data in transit between a data subject and an application,

and so the Nym mixnet does not enforce the rights of the data subject on the level of the application. With this large caveat, we will in the following sections outline how, per principle, network data is important and how the Nym mixnet provides a foundation for GDPR compliance on higher-level applications.

Lawfulness The Nym mixnet enables any application to be accessed via the Nym mixnet. Thus, the Nym mixnet can not enforce lawfulness of the original data processing enabled by any applications built upon the Nym mixnet. A larger question, given concerns over the "Dark Web" and other possible uses of Nym that could be deemed illegal in particular jurisdictions, is whether or not using the Nym mixnet is itself not lawful.

The right to privacy is not an absolute right in the European Union as it needs to be assessed in light of the reasonable and proportional legitimate restrictions placed in national constitutions according to articles such as art. 8(2) ECHR and art. 52(1) CFREU. In short, in the European Union the right to privacy can be legally violated by the investigation and prosecution of criminal activity. Yet simply considering this exception in the abstract may lead one to believe there are more obligations than there actually are.

The restriction has to be accessible, foreseeable and accompanied by necessary procedural safeguards affording adequate legal protection against arbitrary application of the relevant legal provisions.[3]

In this context the Cyber Crime Convention (CCC) is most relevant.[4] The most relevant article of the CCC reads:

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

As the metadata is removed by design across a number of decentralized parties, it is unreasonable to ask for a backdoor that would compromise the privacy of data processing done via the Nym mixnet. Indeed, the wording *as is reasonable* indicates that any order for information, including a decryption order, does not entail a prohibition on the use of technologies that lead to the incapability of decryption of the data by the electronic communication service.[5] The Convention lays down the obligation to erect in national law the competence to order

[3] See for example: ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 67; ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 52.

[4] Convention on Cybercrime. ETS No.185; Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013, on attacks against information systems and replacing Council Framework Decision 2005/222/JHA overlaps with the Cyber Crime Convention in terms of obligations of Member States to adopt substantive criminal law, but lacks a procedural law section.

[5] This is different for public telecommunication providers, such as national telephony providers, who do have to provide a backdoor into any lower-level encryption.

the preservation and submission of available data and metadata.[6] This competence covers the obligation to submit data that is either stored or available, but it does not include a production orders of such data.[7]

The CCC also lies down the obligation to implement law that grants competent authorities the competence to conduct search and seizure of stored computer data which can include personal data, ex. art. 19 CCC. The above indicates that at the jurisdiction level of the CoE and the EU there is an obligation to respond to valid requests of criminal law enforcement agencies or intelligence services when the power of the competent authorities to request data for criminal law enforcement or national security purposes meets the criteria of art. 23 GDPR, art. 11 (and onwards) ePrivacy Regulation and art. 8(2) ECHR and art. 52(1) CFREU. Yet at the moment there is no obligation in law that obliges publicly available electronic communication services to implement of a backdoor in the cryptography that allows for the protection of data by the Nym mixnet, or any alterations to the algorithms used by Nym that eliminate metadata from data in transit across the mixnet. Instead of asking for a backdoor into the mixnet, the authorities should focus on the endpoints, the service providers and the users themselves, that are the subjects of investigation.

Fairness The Nym mixnet also embodies fairness in data processing as mix nodes have no way to discriminate between packets: all packages are encrypted and mixed in the same manner and so treated equal in the mixnet. In this manner, discrimination based on language or other features of the content is impossible. However, the first entry gateway that a user accesses does know the IP address of the user and could blacklist inbound and outbound traffic, and likewise the last exit gateway knows the application. However, this information is de-linked by the usage of the mix nodes. Yet the entry and exit gateways could still blacklist or censor particular users and applications respectively. In this case, the user may use another gateway or setup their own gateway. Nym is currently working on algorithms to automatically detect and remove gateways that censor users from the mixnet.

Transparency The Nym mixnet does not traditionally deal with subject access rights as given in Article 15-22 GDPR, as the personal data processing is done at the application level, but it does enable the user to understand and audit the infrastructure of the Nym mixnet itself. Nym's workings are outlined in a whitepaper that is understandable to ordinary users, as per Article 12 of the GDPR.[8] As the Nym source code is licensed as free and open source software, Nym is compliant with the principles of transparent and fair data processing insofar as everyone can check the code for its data processing capabilities, or

[6] Article 16-18 CCC.

[7] Article 18 CCC includes a production order for electronic telecommunication services, like access providers. As an overlay network on top of existing telecommunications services, the Nym mixnet does not fall under this definition.

[8] The whitepaper is available [6].

ask a third party to audit the code.[9] The human-readable documentation of the Nym project[10] increases the transparency of the data processing and ease of auditing by third parties.

Purpose Limitation As given by art. 5(1)(b) GDPR, the principle of purpose limitation safeguards that personal data is collected for explicit, specified, and legitimate purposes. Furthermore, the data should not be further processed in a manner that is incompatible with the original purpose that the data was gathered for. The mixnet is a way to enforce purpose limitation as it removes metadata and so enforces purpose limitation by technical means. Once anonymized by the mixnet, the data cannot be used for purposes (such as profiling) while the data is in transit, and mix nodes learn nothing about a packet except its next hop in the mixnet. The first hop into the mixnet does learn the sender IP address, but nothing more – including the destination. Likewise, the destination learns nothing more than sender. Even senders and receivers of messages on the mixnet can use Sphinx's Single-Use Reply Blocks (SURBs) to communicate without leaving any long-term identity.

There is a danger that mix nodes capture packets and correlates them for eventual de-anonymization. However, the mixnet includes a 'family' system that spreads out mix nodes ran by the same operator between multiple layers. However, a dishonest mix node could pretend it is ran by someone else. In this case, there are two mediations. The first is a staking system, where only operators of mix nodes that have a certain level of trust (as shown by delegated staking [6]) are more likely to be selected, thereby preventing financially well-endowed adversaries from committing a sybil attack. Also, the placement of nodes in each layer changes every certain number of hours (a deployment parameter) and keys are rotated for forward secrecy, defeating technically attempts to gather data via strategically placing mix nodes in the network. This principle of forward secrecy supports the purpose limitation principle.

Data minimization Preventing data collection by design ensures direct and equal enforcement of data minimization, effectively making it impossible to process data in a manner inconsistent with the GDPR, because it ensures data can only be collected through explicit, practical consent by the data subject. In other words, the best data is no data. Unfortunately, the internet does not use encryption by default without the use of a protocol such as TLS, and even with such a protocol like TLS, internet appications leaks metadata such as the timing and the volume of the packets. This is because it was designed in a trusted academic environment in the 1970s that never imagined itself at the time to be the locus of profit and power it is today. While it could have been argued that timestamps and other forms of identifying metadata like IP addresses were needed to deliver the packets at the time of the creation of the internet, cur-

[9] The code is accessed via https://github.com/nymtech.
[10] The documentation is accessed via https://docs.nymtech.net.

rently privacy-enhanced overlay networks like Tor and Nym show that they are not necessary [14].

The mixnet encrypts the content of the data via the Sphinx packet format and takes any arbitrary-size data stream of packets and transforms it into a number of equal sized Sphinx packets, with padding used as necessary to ensure equal length of all the packets. Information needed for packet delivery is only revealed to the 'next' hop in the mixnet, with only the final gateway (exit node) knowing the destination IP address, and only the first gateway (entry node) knowing the sender's IP address.

More importantly, the Nym mixnet also removes any timing-based metadata. It does this via 'mixing' packets in a series of mix nodes, so that packets exit the mix-node in a randomized order, with the exact order determined by a Poisson process [11]. Therefore, the Nym mixnet limits the necessary data revealed to any actor to a minimum and so protects the privacy of data subjects, fulfilling the principle of data minimization ex art. 5(1)(c) GDPR. Of course, the decrypted payload of the message can still reveal identifying information but the choice of this information is done by the data subject (user), not the data controller or processor.

Note that as Nym works on the level of network data in transmit, it does not enforce data minimisation at the level of the application, although optional attribute-based credentials are given to do so [7]. Therefore, if a user is is communicating with a bank server through Nym, the bank can still collect information about the user, although Nym would prevent the collection of identifying data such as IP addresses and device data revealed by network metadata. Therefore, the need for GDPR compliance moves completely to that bank application as Nym would prevent data collection on the network level beneath the application.

Accuracy Note that accuracy in terms of personal data is done on the application layer, and not the network layer, and so beyond the scope of the Nym mixnet. However, there is information about the network itself that must be accurate, and in this non-traditional manner, Nym maintains accuracy about its own infrastructure. This information is important for end-users to use the mixnet infrastructure. In detail, a blockchain stores various reputation information about the mix nodes, including their key and reputation in the NYM token. As the data subject or controller creates the packets for the mix on their client machine or server, they can check the accuracy of each of the mix nodes. Various tools such as a node explorer lets data subjects manually inspect the network as well.[11] The moment a mix node or other component of the system acts maliciously, the data subject can be informed. The use of tools for monitoring functions balances the distribution of power between the data subject and data controller, thereby also helping with accuracy and fairness in terms of the user-facing parts of the infrastructure itself.

[11] https://explorer.nymtech.net/network-components/mixnodes/active]

Integrity and confidentiality Nym offers the highest level of security to personal data transferred over its network, and so also fulfills the obligation for the confidentialty of communications given by th e-Privacy Directive. The integrity and confidentiality of data sent over the Nym mixnet is protected in a robust manner using cryptography, in a similar manner to other network protocols like TLS. On the level of packets, the integrity and confidentiality of the data is guaranteed using an updated version of the Sphinx packet format [4], in particular the customized Outfox version of Sphinx used by Nym. All data is encrypted, with integrity preserved in the header via the use of a message authentication code. Nym allows direct communication in a privacy-enhanced manner between peers using the mixnet so a server (unlike a traditional peer-to-peer network, whose network broadcasts are not privacy-preserving) is not always required, but a server accessed over Nym would have to enforce GDPR regulations just like any other application involving the internet.

Nym also provides tools for applications. On the level of the application itself, data can be protected using an attribute-based credential [6]. The attribute-based credentials allow the data subject control over any data revealed, and this data can be made confidential using zero-knowledge and the credentials use a digital signature [7] to guarantee the integrity of the data. The usage of these credentials is necessary only to pay for bandwidth in the Nym mixnet and only optionally usable in a wider application-specific interface, nevertheless these attribute-based credentials should be used more widely as a meaningful, technological implementation of consent through selective disclosure. However, Nym differs from normal applications like web-sites and most smartphone apps insofar as servers are forced to commit to data minimisation on the network level.

Storage Limitation The Nym network encrypts all data before it leaves the client device of the user (and likely data subject) and makes each packet indistinguishable by making all messages the same size, via splitting larger data streams into smaller messages and adding padding to messages. Therefore, even if the data is stored by a mix node, it is difficult for the mix node to distinguish the packets and access any personal data. Only the first-hop, the "gateway" of the Nym mixnet, determines network-level information about the user such as the IP address, but these gateways cannot read the payload of messages sent over the Nym mixnet and so cannot easily infer personal data from the communication of the user. Also, the user may add "cover" traffic as a sort of noise to any data they send to the gateway, preventing the gateway from learning even when the user is online or not. In addition, terms of service and future security enclave work can help ameliorate concerns over storage of packets by malicious mix nodes.

Accountability As outlined earlier, Nym is built to enable data protection by design and default. Other aspects of accountability are typically dealt with by applications, although the organization that creates the Nym mixnet software,

Nym Technologies, does have a Data Protection Officer and written terms of service with the mix nodes to ensure accountability, as well as the various security measures and policies required by the GDPR.

One interesting aspect of Nym is also that it enables technical accountability for its own infrastructure by its user themselves, where the Nym mixnet allows its correct operations to be ascertained using cryptography via any user is sending packets via the network. At each "hop" in the mixnet, each packet has a unique onion-wrapped 'tag' that is stored by the mix node. The original purpose of this design was to prevent the same packet from being sent more than once (a 'replay' attack) to the same mix node, as if the same tag is detected the packet is dropped rather than processed by the mix node. This technique is also used to determine the correct rewards in terms of NYM tokens by mix nodes, as mix nodes that drop packets and so fail to help provide privacy are given less rewards than those mix nodes that correctly process messages to provide anonymity. The user of course knows their own tags for their messages, and can check the mix nodes to see if their packets are being correctly processed or dropped. Further work on assuring accountabiity using secure enclaves is on-going.

Beyond Article 5, Article 32 of the GDPR on the "security of processing" requires "appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate" features such as "the pseudonymisation and encryption of personal data." Although this focus on the encryption of the content and pseudonymization of obvious identifiers still holds, we would point on that network-level data protection should also be included as an appropriate measure, one that should even be included by default.[12]

Beyond the GDPR, in terms of the ePrivacy Directive, the Nym mixnet can be thought of as a "service provider" that can help "systems for the provision of electronic communications networks and services" which in turn "should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users."[13] This requirement is fulfilled by the unlinkability of network packets given by the Nym mixnet [10]. Although the ePrivacy Regulation has been withdrawn, the Nym mixnet also helps uphold the ePrivacy Directive.

4 Beyond the GDPR: Right to Digital Integrity

With the withdrawal of the ePrivacy Directive in February 2025, a new ethical framework is needed. Compared to the GDPR, is it possible a more stringent framework for digital rights is possible than even the GDPR, one that would enforce the usage of privacy-enhancing technologies like the Nym mixnet? To recapitulate the larger historical trends, The present digital economy is based on

[12] https://gdpr-info.eu/art-32-gdpr/
[13] https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng

the availability of personal data considered as a commodity that can be traded. This 'surveillance capitalism' has been built into core technosocial infrastructures with the active participation of democratic states. As the social and geopolitical security consequences of this development have become increasingly evident, data protection laws have emerged, culminating with the adoption of the General Data Protection Regulation (GDPR) in Europe. The GDPR is now the most aggressive regulation vis-à-vis the private companies that participate in this surveillance economy, although it is worth noting that the GDPR largely spares state actors themselves in its material scope. Furthermore, the GDPR primarily acts as a tool for regulating this market, limited to mitigating its effects: it already assumes data as a commodity and thereby falls short of shifting the surveillance paradigm that characterises today's digital economy [15].

In the face of what can be described as a failed approach to data protection, there is now a call for the advent of a fundamental digital right, the 'right to digital integrity.' [15]. The principle of 'informational self-determination'[14] is emerging in European case law and judges are seeking to extend protection even beyond the issue of privacy violations. These efforts build on Article 8 of the Charter of Fundamental Rights of the European Union, but are trapped by the 'hierarchy of norms,' only providing a partial solution. This article reaffirms the right to data protection, enshrines the importance of consent when processing data, but does not call into question the underlying paradigm that assumes personal data as a commodity.

In 2018, various French data protection authorities, under the suggestion of the French CNIL declared that "personal data are constituent elements of the human person[15], who therefore has inalienable rights over them." This statement is an explicit rebuttal of the notion of personal data as commodity. Personal data is instead asserted as a constituent element of a person in the same way as their physical body. The proposal is fundamental and yet goes unnoticed to the extent that the CNIL itself is struggling to draw the full consequences of its proposal.

More recently, the notion of 'Digital Integrity' has emerged within political organizations in Switzerland, exploring the extension of the concept of integrity of a person to include their digital existence [13]. The notion is beginning to filter into local Swiss cantonal constitutions: Following a symposium organized by the Faculty of Law of Neuchâtel in 2018, the Valais Constituent Assembly decided to integrate the right to digital integrity when drafting the new Constitution of the Canton of Valais. After two years of work, the Fundamental Rights Commission of the Valais Constituent Assembly in 2020 laid the foundations for an extensive legal process, thereby moving away from the classic approach to data protection, which seeks to avoid the "abusive processing" of data, by proposing a prohibition of "data processing without consent" as a general rule. While this principle appears in the GDPR, it is for the first time explicitly enshrined at constitutional level. This is a fundamental change, as it shifts the burden of proof from the

[14] Ruling of the German Federal Constitutional Court on "informationelle Selbstbestimmung" 1983

[15] Résolution sur la propriété des données adoptée par l'AFAPDP le 18 octobre 2018

individual data subject to the data processor. In the same draft, the right to digital integrity is granted. The drafters specify this notion in particular through the "ability to interact freely through digital technologies."

In 2021, a draft constitutional law was submitted to the Geneva Grand Council proposing the introduction of the right to digital integrity as a new article in the constitution. The Geneva proposal includes well-defined related rights in a non-exhaustive list and will be presented to the people of Geneva for a vote on June 18th, 2023, worded in the following manner: "Digital integrity includes, in particular, the right to be protected against the abusive processing of data related to one's digital life, the right to security in digital space, the right to an offline life as well as the right to be forgotten." This text is rich in novelties, with the concept of "digital life" appearing for the first time in a constitution. Breaking away from a paradigm of data markets and data protection, the protection of individuals and their digital life is now the core of the relation between the individual and the state. The right to an offline life proposes an abstraction of the earlier Valais proposal which remains very technical, and the right to be forgotten finds its place in the hierarchy of norms. Crucially, the right to security in the digital space allows for a profound paradigm shift when it comes to digital security: the digital sphere can no longer be treated by security authorities as a tool that can be compromised for the sake of a particular conflict or court case, but has to be addressed as a sphere that they are tasked with securing in order for people to go about their digital lives in serenity. The right to digital integrity was enshrined in the cantonal constiution of Geneva in June 2023.[16] The right to digital integrity was also added to the constitution of the canton of Jura in 2023.[17]

In Neuchâtel in 2022, an additional right was proposed: The right not to be monitored, analyzed and measured. This right gives a clear picture of the type of society that the constituents are demanding: A democratic digital society that does not surveil it citizens, but instead respects the autonomy and dignity of individuals, their digital integrity and their right to digital life on their own terms. It was passed into the constitution of the canton of Neuchâtel in 2024.[18]

The design of the Nym mixnet is purposefully aligned with the 'right to digital integrity' as well as the related 'right to not to be surveilled, monitored and analyzed.' [6] On a transparent network like the Internet, in order to establish a truly private conversation, communications must be unobservable. Digital rights should follow the same construct. In a society where dignity and life is respected, each person's integrity, including its digital integrity must be protected. The right not to be surveilled, monitored or analyzed should encourage any public institution to provide its services to the people without knowing them, in other

[16] https://www.tdg.ch/le-plr-veut-renforcer-la-protection-de-l-integrite-numerique-409055812296

[17] urlhttps://www.lqj.ch/articles/le-parlement-souhaite-garantir-lintegrite-numerique-du-citoyen-dans-le-jura-43184

[18] https://www.rtn.ch/rtn/Actualite/Region/20241124-Neuchatel-ancre-l-integrite-numerique-dans-sa-Constitution.html

words, a right to anonymity. It would allow individuals to use anonymity preserving tools without the risk to be prosecuted. The realisation of 'the right to digital integrity' would arguably lead to the emergence of a digital economy and innovation pathway that is very different from the current data-driven one and even lead to a revised security policy whereby the human being is protected not only physically, but also in their digital form.

5 Conclusion

Today, data and metadata is widely exposed in digital infrastructure as the default, with the market for personal data assumed as a given. For the principles outlined in the GDPR to be realised in practice, the opposite has to be the case, with the default of infrastructure and services being privacy-preserving. As a first step in this direction, we have evaluated the Nym mixnet in relation to the principles of the GDPR, and the Nym mixnet is shown to be not only compliant but also significantly advancing the principle of data minimization in practice as explored in Article 5 and 32, as well as the other obligatins as given by Article 5 of the GDPR. There are many shortcomings to a data protection approach that focuses on individual consent on the application-layer in an environment where such consent cannot be meaningfully exercised due to the scale and relational nature of digital surveillance on the level of data in transit over the network, particularly as now enabled by the widespread use of machine-learning for inferring personal data and identifying persons. Privacy-enhancing technologies such as anonymous overlay networks like Nym are the basis for these data protection rights to be exercised in practice on the network-layer, although the GDPR still should be enforced on the application layer regardless of the technical protections provided to the network layer. This is because in part the network-level, where TCP/IP or UDP packets flow from sender to receiver, is the fundamental building block upon which other internet-enabled applications are built. To ignore privacy on this network-layer is similar to building a castle on a foundation of sand. Securing privacy by default through infrastructure can enable a new digital economy that does not rely on the commodification of personal data but instead preserves fundamental rights through code.

References

1. Louise Amoore. *Cloud ethics: Algorithms and the attributes of ourselves and others*. Duke University Press, 2020.
2. Lee A Bygrave. Data protection by design and by default: Deciphering the eu's legislative requirements. *Oslo Law Review*, 4(02):105–120, 2017.
3. Ann Cavoukian et al. Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices. *Information and Privacy Commissioner of Ontario, Canada*, 5, 2009.
4. George Danezis and Ian Goldberg. Sphinx: A compact and provably secure mix format. In *2009 30th IEEE Symposium on Security and Privacy*, pages 269–282. IEEE, 2009.

5. Claudia Diaz. Mix networks. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1–5. Springer, 2022.
6. Claudia Diaz, Harry Halpin, and Aggelos Kiayias. The Nym Network, 2021.
7. Harry Halpin. Nym credentials: Privacy-preserving decentralized identity with blockchains. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 56–67. IEEE, 2020.
8. Bert-Jaap Koops and Ronald Leenes. Privacy regulation cannot be hardcoded. a critical comment on the privacy by design provision in data-protection law. *International Review of Law, Computers & Technology*, 28(2):159–171, 2014.
9. Dobres Marcia-Anne. Technology and social agency: Outlining a practice framework for archaeology. 2000.
10. Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings*, pages 1–9. Springer, 2001.
11. Ania M Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The loopix anonymity system. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 1199–1216, 2017.
12. Charles D Raab. Information privacy: Ethics and accountability. 2016.
13. A. Roussel and G. Barbery. *Notre si précieuse intégrité numérique*. Slatkine, 2021.
14. Paul Syverson, Roger Dingledine, and Nick Mathewson. Tor: The second generation onion router. In *Usenix Security*, pages 303–320, 2004.
15. Lusine Vardanyan, Václav Stehlík, and Hovsep Kocharyan. Digital integrity: A foundation for digital rights and the new manifestation of human dignity. *TalTech Journal of European Studies*, 12(1):159–185, 2022.
16. Salome Viljoen. A relational theory of data governance. *Yale Law Journal*, 131:573, 2021.
17. Langdon Winner. Artifacts/ideas and political culture. *Whole Earth Review*, 73:18–24, 1991.