Sustainable Privacy

Samuel M. Smith, Ph.D.

v1.2.4 2025/11/15 (Original 2023/09/18)

Abstract—Sustainable privacy takes a more holistic view of privacy protection. Conventional protection mechanisms, such as K-anonymity-based de-identification, are shown to be non-viable due to various attacks. The contextual linkability re-identification attack on selective disclosure is also described. This demonstrates how focusing on unlinkability can be counter-productive, especially when it defeats more comprehensive protections. Indeed, sustainable privacy requires, at the least, a more comprehensive approach that combines economic, legal, regulatory, and technical protections.

Index Terms—privacy, de-identification, re-identification, chain-link confidentiality, contextual linkability.

1 Introduction

Stated simply, sustainable privacy refers to the maintenance and preservation of personal data privacy over time. There are two sides to sustainable privacy. One side is how a person maintains their personal data privacy over time, and the other is how a holder of someone else's personal data respects and supports personal data privacy over time.

The difficulty of sustainable privacy is that any information-gathering, usage, and sharing system is leaky. Information, especially information that is actively being used for almost any purpose, leaks out over time, thereby gradually eroding the privacy of any data being managed as the source of that information. Certainly, the sharing of data is inherently leaky, i.e., it is intentional and is, therefore, problematic when viewed from the perspective of sustainable privacy.

This report outlines the technical and legal issues surrounding sustainable privacy and guides better sustainable personal data privacy.

1.1 Three-Party Exploitation Model

Sustainable privacy is based on a three-party exploitation model. Fundamentally, the goal is to protect the person from exploitation via their personal data. In common usage, exploitation is selfishly taking advantage of someone to profit from them or otherwise benefit oneself. So, any unintended usage by any party is potentially exploitive. Intent is with respect to the person (data subject).

In this model, the 1st party is the person who is the source of the original data. The data they source is, therefore, 1st-party data. The 1st party may or may not be the data subject. This is a more expansive definition of 1st-party data than merely data to which they are the subject. To clarify, this definition is meant to protect all data sourced by the 1st party on any subject, not merely data for which the 1st party is the subject.

A 2nd party is the direct recipient of 1st party data as an intended recipient by the 1st party.

A 3rd party is any other party that obtains or observes 1st party data but is not the intended recipient.

There are two main avenues of exploitation of 1st party data: 1) Any 2nd party that uses the data in any way not intended by the 1st party. 2) Any 3rd party who uses 1st party data.

To clarify, any unintended (unpermissioned) use of 1st party data by any party, 2nd or 3rd party, is naturally exploitive.

Moreover, because a 3rd party is defined as an unintended recipient, then any use of 1st party data by a 3rd party is, by definition, unpermissioned and therefore exploitive.

Furthermore, 1st-party data may be conveyed by one 2nd party to another party (i.e., shared) in a non-exploitative manner when such conveyance and eventual use by that other party are intended (permissioned) by the 1st party. The intended sharing makes the downstream recipient of 2nd party data, effectively a 2nd party by our definition. To elaborate, the means of conveyance does not have to be direct from the 1st party to the 2nd party, but may be indirect via a chain of parties that share the information. Each party in the permissioned chain is, by definition, a 2nd party.

This model elevates the intent (expressed or otherwise) of the first party regarding the use of data they source as the a priori determinant of exploitive or non-exploitive behavior by 2nd and 3rd parties. Although the diagram below illustrates all the vectors by which data may leak and thereby erode the sustainable privacy of 1st-party data, the focus of this report is on how 2nd parties may either help or hinder sustainable privacy. Refer to the SPAC whitepaper for an approach to protection against 3rd-party exploitation through metadata correlation. [50]

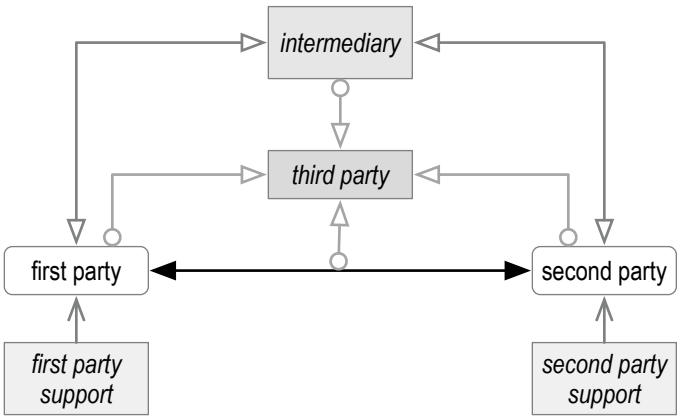

Figure 1.1. Three-Party Exploitation Model

1.2 Data Privacy

Information or data privacy is defined as the relationship between the collection and dissemination of data, technology, the public expectation of privacy, contextual information norms, and the legal and political issues surrounding them. Data privacy is challenging since it attempts to allow the use of data by 2nd and 3rd parties while protecting personal (1st party) privacy preferences and personally identifiable information (PII). The fields of computer security, data security, and information security all design and utilize software, hardware, and human resources to address this issue. [28] This definition is compatible with privacy viewed from the perspective of 1st party data rights and the role of 2nd parties in the three-party exploitation model. The Trust over IP (ToIP) foundation's architecture specification phrases privacy protection as answering the question:

> *Privacy: will the expectations of each party with respect to the usage of shared information be honored by the other parties?[61]*

The primary mechanisms by which 2nd parties erode sustainable data privacy rights are as follows:

- Exploitive use of 1st party data by 2nd parties.
- Sharing of 1st party data by 2nd parties with 3rd parties, either overtly or inadvertently, via leakage.

The conventional best practices for managing personal data are often based on the principles of privacy by design and privacy by default (PbDD) [5].

Recent advances in technology, however, have made many conventional best practices for such PbDD policy insufficient for sustainable privacy. This report will explain why. One of the best practices recognized for PbDD is called data de-identification (or data anonymization).

The most common approach to de-identification is based on an approach called K-anonymity [30]. The basic idea is that a data set may be de-identified by deleting any attributes in a data set that contain personally identifying information (PII), such as name, address, and phone number. More sophisticated approaches also delete sufficiently identifying quasi-identifiers. A quasi-identifier is any subset of attributes that together are personally identifying. Indeed, various K-anonymity approaches to data de-identification have become the primary best practice for protecting the privacy of 1st party data when sharing with 3rd parties. The attraction of K-anonymity as a best practice is that it provides a safe harbor to any 2nd party to share any and all 1st-party data with any 3rd party for any purpose. Essentially, if the data has been de-identified using K-anonymity, it is, by definition, no longer 1st-party data. Unfortunately, K-anonymity as a de-identification technique is easy to defeat and, therefore, should no longer be considered an acceptable best practice [2; 7; 8; 10; 22; 23; 31; 33; 35; 48; 61].

There are two other mechanisms for de-identification that so far are considered practically infeasible to defeat and hence are suitable for sustainable privacy. These are differential privacy and synthetic data privacy [1; 15-2035; 38; 41; 57; 59; 64].

Given that K-anonymity is broken and viable alternatives to K-anonymity exist, the use of K-anonymity can no longer be considered a best practice for the de-identification of data before sharing. The only allowable de-identification approach is either a differential privacy or a synthetic data privacy-based mechanism.

The next sections delve into the primary factors underlying sustainable privacy in more detail and provide guidance on best practices for achieving it.

2 Re-identification

Let's first consider the problem of de-identification and re-identification of data. It was long thought that de-identification or anonymization of data could provide privacy using a technique called K-anonymity [30]. Indeed, the ease and pervasiveness with which de-identified data may be re-identified have resulted in the US FTC (Federal Trade Commission) issuing a warning that those who share de-identified databases and purport that merely through conventional de-identification that the privacy rights of the associated persons are protected, may be in violation of the laws regulating the use and sharing of sensitive data [8; 9; 53].

2.1 Linkage Re-identification Attacks

Recent research has shown that fully de-identified sparse datasets (using K-anonymity) can be merged to re-identify the data. [2; 13; 14; 32; 34; 45] In 2022, this was further extended to what is called a down-coding attack, which enables the re-identification of data even when every field is a quasi-identifier, i.e., there is no personally identifiable information in the dataset. Even fully de-identified low-sensitivity data about interaction patterns can create a social signature that enables the re-identification of the majority of users. [29] These are all examples of what are called linkage attacks [42]. In general, the vulnerability to linkage attacks inherent in conventional de-identification mechanisms means that using such mechanisms for maintaining data set privacy is an exercise in risk management rather than a guarantee of protection [29; 46].

2.2 Profiling Re-identification Attack

Online interactions between parties captured as interactions of anonymized members of a social graph using only time, duration, and type of interaction are enough to re-identify the majority of the members of the social graph using only a 2-hop interaction graph [10]. The latter is an example of a new type of attack called a profiling re-identification attack, where machine learning is used to re-identify based on de-identified behavioral data and not merely by linking de-identified database attributes (quasi-identifiers or non-identifiers) [29; 60]. Indeed, graph-based machine learning seed-set-expansion algorithms can profile an individual across communities over the whole internet [31; 56].

2.3 Contextual Linkability Re-identification Attack

As mentioned above, any de-identified dataset, even when all attributes are quasi-identifiers, may be vulnerable to re-identification through various statistical correlation attacks, whether they are linkage-based or behavioral profiling-based correlations. In this section, we introduce a new correlation attack based on contextual linkability that defeats the purported privacy protection mechanism commonly known as selective disclosure [22].

The selective disclosure, whether via Zero-Knowledge-Proof (ZKP) or not, of any 1st-party data disclosed to a 2nd party may be potentially and trivially exploitable and correlatable via either linkage or profiling re-identification techniques when those techniques are applied to auxiliary data obtained at the time of disclosure (presentation) of selectively disclosed attributes[65] . We refer to an attack that utilizes the statistical correlation of auxiliary attributes obtained from the context of a disclosure as a contextual linkability re-identification attack. Essentially, it's the use of a set of non-selectively disclosed attributes (auxiliary data) obtained from the context of the disclosure that is sufficient to re-identify the discloser despite selective disclosure. Thus, a contextual linkability attack may trivially defeat the cryptographic unlinkability provided by selective disclosure mechanisms, including those that use ZKPs.

In essence, the vulnerability stems from the fact that the verifier may structure the context of the presentation so as to provide sufficient auxiliary data that the combination of contextual auxiliary data and selectively disclosed data identifies the discloser (presenter). In other words, contextual linkability has the potential to create a data set of quasi-identifiers that can be combined with selectively disclosed attributes in a way that re-identifies the associated subject of the selectively disclosed attributes. Thus, ZKPs or other selective disclosure mechanisms by themselves may provide insufficient privacy protection. Any unconstrained, selectively disclosed set of attributes is inherently re-identifiable unless the discloser takes care to both protect from contextual linkability and impose a contractual liability on any use of that data. Essentially, bare selective disclosure implicitly grants the disclosee (verifier) a safe harbor to use, assimilate, and re-identify the disclosed data.

The contextual linkability vulnerability renders the status of selective disclosure and/or ZKPs as privacy mechanisms to the narrow corner conditions where there is zero contextual linkability by the second-party disclosee (verifier) at the time of presentation. Because most presentation contexts are under the control of the 2nd party (verifier), the verifier needs merely to structure that context with enough quasi-identifier attributes (auxiliary data) to re-identify the presenter, which in turn would enable the 2nd party to link the de-identified presenter back to the issuer with the presentation details, thereby defeating cryptographic unlinkability. This cryptographic unlinkability may be the only salient reason to use a ZKP over other selective disclosure approaches in the presentation in the first place. This does not mean that there are no corner conditions where the presentation context is sufficiently under the control of the presenter (1st) party such that the presenter can structure the context so as to prevent the verifier from correlating any

other quasi-identifiers, but none of the standard published use cases for cryptographic unlinkability satisfy that condition.

Correctly understood, selective disclosure is a naive form of K-anonymity performed by the discloser (presenter). The discloser is attempting to de-identify their own data. Unfortunately, such naive de-identified disclosure is not performed with any statistical insight into the verifier's (receiver's) ability to re-identify the selectively disclosed attributes, given the contextual attributes that are also disclosed (inadvertently) at the time of presentation and under the verifier's control. Indeed, the act of presentation creates a context that singles out the presenter. It is roughly equivalent to a de-identified release of data of a single record (cell size of one). This provides isolation that simplifies the task of re-identification using contextual auxiliary data. Singling out is a more precise way of describing indirect identification under the GDPR [6]. The act of disclosure by one party to another party singles out the disclosing party. This makes the data personal, even when selectively disclosed to remove PII. Consequently, the recipient of bare, selectively disclosed data must treat it as personal data, or they may be in violation of the GDPR. In this light, selective disclosure should not provide a safe harbor because the data so disclosed is always singled out. Unfortunately, current regulatory policy does not respect this distinction.

In light of this vulnerability, many of the standard use cases for selective disclosure (with or without ZKPs) in verifiable credentials (VCs) are examples of anti-patterns for privacy protection [62]. This is because these standard use cases assume a presentation context that is under the control of the verifier, which means a malicious verifier can restructure that context to statistically guarantee correlation and defeat the selective disclosure with or without a ZKP.

For example, when a disclosure is made at the place of business of the receiver (verifier), the receiver may use readily available location data from mobile phone providers to re-identify based on a geo-fence query or readily available facial identification based on on-premise security camera footage. Similarly, if the presentation of a facial biometric is required, the receiver may also use facial recognition systems to re-identify the presenter. If payment is required, the receiver may use the presenter's credit card information to re-identify them.

Likewise, when the disclosure is made on the receiver's website, the receiver may use readily available IP source-addressing and routing information to re-identify the presenter. This vulnerability includes TOR (onion routing) protected internet communications, which are vulnerable to timing attacks [40; 47; 63]. In detail, the time-of-departure and time-of-arrival of packet streams may be correlated to link the two parties.

Moreover, for social applications that employ bare repeated selective disclosures (even with ZKPs), the set of social interactions observable by the 2nd parties forms a context that may be a correlatable social graph. Therefore, a profiling reidentification attack that merely requires the time, duration, and type of interaction associated with each selective disclosure may reidentify the individuals making the selective disclosures. [31; 56]

Ironically, any receiver (verifier) sophisticated enough to verify a ZKP selective disclosure presentation is sophisticated enough to use these readily available contextual re-identification techniques to defeat that selective disclosure. The receiver may not have the computing infrastructure in-house, but they merely need to share the contextual data they collect with a data broker who performs the reidentification on their behalf. The advent of generative AI Agents trivializes such reidentification capability.

Indeed, systems that use selective disclosure as an advertised privacy protection mechanism may result in a net decrease in privacy protection for users because of the false belief that selective disclosure alone is sufficient to protect the discloser (presenter) from reidentification and hence tracking. This may increase the number of re-identifiable disclosures that would not have

happened otherwise. Users may be lulled into a false belief that because their selectively disclosed attributes do not include any personally identifying information, there is no need for them to impose any constraints on the use and/or sharing of their naively de-identified (selectively disclosed) attributes. Indeed, the receiver may surreptitiously induce such unconstrained disclosures by reinforcing the false belief that the de-identified attributes are not (easily) re-identifiable. For this reason, using a bare selective disclosure mechanism may be considered irresponsible by any organization that purports to use it for privacy protection.

To elaborate, the core defect of any K-anonymity-like approach, including selective disclosure, is that there is no a priori way to establish if any attribute is an identifier, quasi-identifier, or non-identifier. All attributes are potentially identifying attributes based on the available auxiliary data. This includes auxiliary data obtained from the context of the disclosure. As a result, bare (naive) selective disclosure alone provides no guarantee of privacy protection to the discloser. Thus, de-identifying aggregated 1st-party data, including de-identification via selective disclosure, provides no meaningful privacy protection.

One must recognize that naive K-anonymity-based mechanisms, such as selective disclosure, including ZKPs, that provide so-called cryptographic unlinkability, may be trivially linkable by statistical re-identification methods. Any selective disclosure is potentially ineffective unless performed within the confines of a regulatory or legal framework, such as contractually protected disclosure that imposes an incentive on the disclosee (verifier) to not use the data so disclosed to exploit the discloser (provides a strong counter-incentive against exploitive use of that data).

2.4 Security Vulnerability of Unlinkable Disclosure

A selective disclosure via a ZKP may be framed in the context of the well-known issuer-holder-verifier model. [11] The issuer signs a verifiable credential or other data container with a special type of digital signature. The signature enables the holder to generate a proof that the issuer issued that data container to the holder without the holder disclosing a unique identifier that can be traced by the issuer should the verifier share the holder’s presentation proof with the issuer. Essentially, the issuer signs a document on behalf of the holder in such a way that a verifier can verify the document was signed by the issuer, and the holder can prove that the document was assigned to them without revealing the holder's identity. This is sometimes called verifier-to-issuer or vendor-to-issuer unlinkability of the holder with respect to the act of disclosure [58].

This is actually a very weak form of unlinkability. The previous section demonstrates how trivial it may be for the verifier to re-identify the holder despite a selective disclosure with a ZKP. A common use case for such selective disclosure is age verification that proves an age threshold has been met, but without disclosing the actual birthdate. For example, a holder wishes to prove they are of drinking age without disclosing any more about themselves, especially not their identity or any other PII such as birthdate. However, as shown above, contextually leaked auxiliary data, such as mobile device GPS, Face ID, and payment information, all enable linkability by the verifier (the bar) of the holder back to the issuer.

The security vulnerability is as follows: the ZKP requires a special type of signature from the issuer (such as BBS+) [58]. Should the issuer’s private key used to create the ZKP issuance ever become compromised by a malicious party, then that party may issue verifiable ZKPs to unwitting or colluding holders [58]. This creates an undetectable impersonation attack on the issuer. The impersonator can issue any number of verifiable proof-of-age credentials to whomever. By design, the issuer has no way to determine if a given credential was issued by it to a legitimate holder or issued by the impersonator to an illegitimate holder.

To elaborate, what is uniquely problematic in the case of ZKP signatures is that the unlinkability property (by definition) means that the issuer can’t tell which signatures (ZKP) it issued and

which were issued by the malicious impersonator. Ironically, a verifier that suspects that a given ZKP was forged has no way of informing the Issuer of a suspected forgery by linking the presentation of the suspected forged proof back to the issuer without breaking its so-called unlinkability property.

The most common applications of verifiable credentials or entitlements preclude the use of ZKPs because of their unlinkability to the issuer and the forced mismatch with the secure cryptoperiod of the issuing key(s) [4]. From a key management perspective, ZKPs are just a special type of digital signature used as a source authenticator. To elaborate, the issuer uses an asymmetric private key to create the ZKP issuance, which serves as a type of digital signature that provides source authentication.

The most common applications of verifiable credentials (VCs) are persistent in nature. In these applications, such as proof-of-age, for example, the ZKP proof as VC must be verifiable for some extended period of time, such as years, or indefinitely, such as the lifetime of the Issuee (holder) of the ZKP VC. Because ZKPs are based on asymmetric key pairs, the time period of secure verifiability is limited to something less than the cryptoperiod of the issuing asymmetric key pairs. NISTs recommended best practice cryptoperiod for key pairs used for source authentication (i.e., the ZKP issuer's keys) is one to two years. [4] So, at most, a bare ZKP VC can only be used for applications where the VC has a lifespan of no more than two years. Otherwise, one is violating best practices for key management. However, for applications where identity theft via impersonation fraud of the Issuer would be problematic if it were to remain undetected over the full one- to two-year lifespan of the ZKP VC, then at most the lifespan of the VC needs to be significantly shorter than the cryptoperiod. It must be less than the allowable time limit for undetectable harm. For many VC applications, this looks more like days than months and certainly not years.

In contrast, the KERI/ACDC protocols provide mechanisms for issuing persistent or even perpetual VCs via ACDCs that exceed any shorter key cryptoperiods by binding issuances to the key state at the time of issuance [49]. Since this binding mechanism necessarily defeats the so-called vendor-to-issuer unlinkability property of ZKPs, there is no benefit to using a ZKP for persistent or perpetual VC applications.

Moreover, because there is no mechanism in a bare ZKP to identify which issuances were ever compromised due to its unlinkability property, the only viable option is for the issuer to revoke and reissue all issuances from the set of compromised keys or whenever the cryptoperiod expires, whichever is shorter. This is impractical in almost all purported use cases where ZKPs are used as a mechanism to protect holder privacy with respect to issuer tracking of holder behavior when presenting a credential.

This impracticality is exponentially exacerbated by the impending possibility of a quantum computer compromising all ZKP issuer private keys [58]. Any lifelong credentials, such as age verification, would need to be assumed compromised and reissued. Thus, using ZKPs in those use cases is highly counterproductive. It's better to use more secure methods of selective disclosure than ZKPs and instead use legal and or regulatory mechanisms to protect against vendor-to-issuer linkability.

3 Protection from Re-identification Attacks on 1st Party Data

There are two modes of data sharing with respect to 1st party data. The first is the sharing of non-aggregated 1st party data, and the second is the sharing of already aggregated 1st party data.

3.1 Non-aggregated 1st Party Data

Any non-aggregated 1st party data shared with a 2nd party may be easily re-identifiable because there is no herd privacy. The data is directly attributable to the one and only 1st party. The act of sharing forms a sharing disclosure context that may be structured by the 2nd party to provide easily correlatable contextual auxiliary data that enables re-identification via a contextual linkage attack. Consequently, due to the ease of re-identification via a contextual linkage attack, the only practically viable protection against the 2nd-party correlation of non-aggregated 1st-party data is pre-disclosure contractual protection by imposing liability on the 2nd-party disclosee and strict post-disclosure chain-link confidentiality on any downstream disclosees or other users of that data, including any later assimilation or aggregation [25]. Chain-link confidentiality can impose a requirement that 2nd parties may not aggregate 1st party data, de-identified or not (selectively disclosed or not), without the consent of the 1st party.

To reiterate, the only sustainable privacy protection mechanism of 1st party data disclosed to a 2nd party, even when selectively disclosed (via ZKP or not), is contractually protected disclosure via chain-link confidentiality.

3.2 Aggregated 1st Party Data

As mentioned above, aggregated 1st party data (multiple 1st parties) may be de-identified using one or both of two statistically provable de-identification techniques, namely differential privacy and/or synthetic data privacy.

3.2.1 Differential Privacy

When used properly, differential privacy takes a data set and corrupts the field values with statistical noise so that it is difficult or impossible to re-identify any individuals [15-18][19; 35; 64]. A major drawback of differential privacy is that the corrupting noise may change the statistics of the aggregated data such that certain types of critical inference are also corrupted, as in the case of data used for medical risk and efficacy [36].

3.2.2 Synthetic Data Privacy

Synthetic data privacy is based on a self-supervised machine learning technique that uses real data as the training set to synthesize a new data set with similar statistics to the training set, but which provides resistance to re-identification of the real data records, given the synthetic data [1; 12; 20; 38; 48; 57; 59]. Therefore, a caveat in generating synthetic data is that the degree of learning accuracy must be limited to not compromise re-identification resistance [41; 44].

3.2.3 Comparison

Synthetic data privacy is more computationally intensive than differential privacy but has the potential for much higher fidelity of its aggregated statistics to the real data used in its training set while maintaining a comparable level of re-identification resistance. Thus, synthetic data may be more valuable than differentially privatized data. In both cases, care must be taken to ensure sufficient statistical uncorrelatability (unlinkability) between the synthetic or differentially privatized data and the real data.

3.3 Protection via Management of the Time Value of Information

Generally, privacy tends to dissipate over time. This is because digital information is inherently leaky, and those leaks become more correlatable as the body of leaks grows over time. The diminishing exploitable time value of correlated information can balance this leakiness.

The primary exploitable time value of correlated information for data aggregators is that it can be used to predict behavior. Advertisers want to predict who will most likely be receptive to their

marketing campaigns. The predictive accuracy of aggregated behavioral information for potential participants in any given market-related behavior is largely a function of the temporal proximity of that market-related behavior when used to make the prediction. We can assign a time constant to a given market, reflecting the exploitable predictive potential of market-related behavior, where information older than the time constant no longer has net predictive value in excess of the cost of aggregating it. Information that exceeds this time constant is considered stale because there is no longer any incentive to aggregate and correlate it. Therefore, despite the fact that privacy dissipates over time, the value of correlation also diminishes over time, allowing cost-effective privacy protection mechanisms to focus resources on near-term correlatability. This provides a sweet spot for sustainable privacy protection, governed by the time constant of the exploitable correlation value. Likewise, the cost of privacy protection can be weighed against the cost of harm resulting from exploitation. If the cost of protection exceeds the cost of harm due to exploitation, then it's not worth protecting (i.e., it's counterproductive to the protector). If the cost of correlation required to exploit exceeds the time value of exploitation, then it's not worth exploiting (i.e., it's counterproductive to the exploiter).

One approach to managing this trade-off would be a protocol for exchanging or sharing information that granularly partitions data-sharing contexts so that correlatability is also granularly partitioned. The Trust over IP (ToIP) is developing such a protocol called the Trust Spanning Protocol (TSP) [33; 50].

The TSP protocol enables one to control the exploitable time value of the correlatable information that can be leaked from a given context. Once a context has become leaky, however, a new isolated context can be created that restarts the clock on time-value correlatability. This provides a trade-space between the friction and cost of forming and maintaining contexts, the length of time before a given context becomes leaky, and the time constant of the exploitable value of leaked information. The cost of protection includes expensive one-time OOBA (Out-of-Band-Authentication) setups. If the leakiness of a given context is cost-effectively protectable beyond the time constant on the time value of exploitation, then new information is sustainably protectable indefinitely.

4 Legal and Regulatory Issues

In general, the idea that conventional de-identification, which involves removing PII, grants collectors of personal data a safe harbor with respect to protecting personal privacy and data rights is an outdated notion. Simply put, conventional anonymization is ineffective. All data collected about a person must be considered sensitive and must only be used by intended users for intended purposes. The practice of effectively *privacy-washing* data via conventional de-identification to share it without restrictions is a problematic approach. Instead, data sharing must be process-based and contextual, with *strings* attached [46]. Even when newer, more advanced techniques such as differential privacy or synthetic data privacy are employed to more effectively de-identify datasets, the sharing of personal data without the consent of the individual is inherently exploitative.

One way to attach strings to the data that conveys the person’s intent for its usage is through chain-link confidentiality [25]. Chain-link confidentiality provides legal protection for privacy by leveraging the well-established framework of confidentiality law. This ensures that the collection, holding, and sharing of personal data are protected with explicit confidentiality. This may be considered a policy of confidentiality by design. With chain-link confidentiality, all personal data can have strings attached for all downstream users and uses of that data. Complementary to explicit confidentiality protection is implicit confidentiality protection[23]. Implied confidentiality is a default policy that augments both confidentiality by design and privacy by design by

leveraging confidentiality law. Together, explicit confidentiality and implicit confidentiality, by default, provide comprehensive privacy protection within the framework of confidentiality law. The emerging open ACDC standard includes support for chain-link confidentiality [49].

We believe that the focus should be on legal and regulatory mechanisms that support the anti-assimilation of data, not merely its de-identification. Anti-assimilation specifically bars sharing and reidentification. It forces the data to be used decorrelatively, even retroactively.

As an overarching principle, any privacy-respecting 2nd party should act under a duty of loyalty to the preferences and expectations of the data privacy rights of 1st parties. This principle is succinctly referred to as data loyalty [24; 43]. The 2nd party data holder must act as a loyal agent of the 1st party. In other words, the 2nd party should be loyal to the best interests of any 1st party with respect to their data. This extends to consent. The act of consent can be easily socially engineered against the best interests of the consenter [51][21][3][54][55].

From a legal and policy perspective, a loyal data agent acts as a fiduciary on behalf of the data subject. By definition, a fiduciary must act in the best interests of its client, which is directly opposed to what an exploiter of personal data would do. It is clear that many, if not most, 2nd parties act more like data exploiters than data fiduciaries.

Exploitation is not limited to selling data; it includes any form of data opportunism that benefits the 2nd party at the expense of the 1st party. Exploitation also includes using data for nudging and manipulation. A fiduciary is responsible for negligence when it allows exploitation by others or fails to utilize data to benefit its clients in accordance with the expressed best interests of those clients. From that perspective, a loyal data agent can be incentivized by being held accountable for mis-, mal-, and non-feasance with respect to this duty.

As the abilities of super aggregators (super correlators) of data advance, mere technological measures will not protect users. This quote from Solove's 2025 book, *On Privacy and Technology*, captures this concept [52].

"Privacy is about boundaries, not secrecy. The law often treats privacy in a simplistic, binary way: personal data is either secret or exposed. And once data is exposed, the law refuses to provide privacy protections—the cat is out of the bag. I call this notion of privacy the "secrecy paradigm." However, privacy is actually much more complicated. Privacy involves a set of boundaries that modulate the flow of data."

One way to better modulate the flow of data is to adopt regulatory measures that embrace the four Ds, namely, *duties*, *design rules*, *defaults*, and *data collection dead ends for data processing and deployements of the aggregation of data*. [27; 37; 39]. Modern privacy protection needs to go from mere respect for personal autonomy and dignity via anonymity technology to providing legal means for people to disrupt the power disparity between them and the super aggregators of data about them. [26]

Acknowledgments

The author wishes to thank all those who provided helpful feedback.

Author

Samuel M. Smith, Ph.D., has a deep interest in decentralized identity and reputation systems as well as the authenticity, confidentiality, and privacy implications of the associated technology. Samuel received a Ph.D. in Electrical and Computer Engineering from Brigham Young University in 1991. He then spent 10 years at Florida Atlantic University, eventually reaching full professor status. He has conducted pioneering research in automated reasoning, machine learning, au-

tonomous vehicle systems, and decentralized identity and reputation. He has over 100 refereed publications in these areas and has served as the principal investigator on numerous federally funded research projects. Dr. Smith has been an active participant in the development of open standards for network and identity protocols. He is also a serial entrepreneur. He serves on the Utah State Privacy Commission and chairs the ToIP Foundation's working group for the KERI Suite of protocols. He is also co-founder and co-chair of the KERI Foundation.

REFERENCES

[1] "13 Tools for Synthetic Data Generation to Train Machine Learning Models," Geekflare,
https://geekflare.com/synthetic-data-generation-tools/

[2] "33 Bits," 33 Bits of Entropy,
https://33bits.wordpress.com/about/

[3] Abrusio, J., "THE (IN) EFFICACY OF CONSENT FOR THE PROCESSING OF PERSONAL DATA," HUMANITIES AND RIGHTS GLOBAL …, 2024
https://www.humanitiesandrights.com/journal/index.php/har/article/download/133/102

[4] Barker, E., "Recommendation for Key Management: Part 1 - General," NIST Special Publication 800-57 Part 1 Revision 5, 2020/05
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[5] Cavoukian, A., "Privacy by Design The 7 Foundational Principles,"
https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[6] Cohen, A. and Nissim, K., "Towards formalizing the GDPR's notion of singling out," Proceedings of the National Academy of Sciences, vol. 117, no. 15, pp. 8344-8352, 2020
https://www.pnas.org/doi/full/10.1073/pnas.1914598117

[7] Cohen, A., "Attacks on Deidentification's Defenses," vol. 31st USENIX Security Symposium, no. USENIX Security 22, pp. 1469-1486, 2022
https://www.usenix.org/conference/usenixsecurity22/presentation/cohen

[8] Cohen, K., "Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data," FTC Business Blog, 2022/07/11
https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal

[9] Collins, P., "Debunking the Myth of "Anonymous" Data," Electronic Frontier Foundation, 2023/11/10
https://www.eff.org/deeplinks/2023/11/debunking-myth-anonymous-data

[10] Creţu, A.-M., Monti, F., Marrone, S. et al., "Interaction data are identifiable even across long periods of time," Nature Communications, vol. 13, no. 1, pp. 313, 2022
https://www.nature.com/articles/s41467-021-27714-6

[11] Bernstein, D., "Verifiable Credentials Overview," W3C, 2025/08/05
https://www.w3.org/TR/vc-overview/

[12] Dankar, F. K. and Ibrahim, M., "Fake it till you make it: Guidelines for effective synthetic data generation," Applied Sciences, vol. 11, no. 5, pp. 2158, 2021
https://www.mdpi.com/2076-3417/11/5/2158/pdf

[13] De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. and Blondel, V. D., "Unique in the crowd: The privacy bounds of human mobility," Scientific reports, vol. 3, no. 1, pp. 1-5, 2013
https://www.nature.com/articles/srep01376

[14] De Montjoye, Y.-A., Radaelli, L., Singh, V. K. and Pentland, A. ". S., "Unique in the shopping mall: On the reidentifiability of credit card metadata," Science, vol. 347, no. 6221, pp. 536-539, 2015

https://dspace.mit.edu/bitstream/handle/1721.1/130329/Unique in the shopping mall- On the reidentifiability of credit card metadata.pdf?sequence=1

[15] "Differential Privacy," Wikipedia,

https://en.wikipedia.org/wiki/Differential_privacy

[16] "Differential Privacy," Harvard University Privacy Tools Project,

https://privacytools.seas.harvard.edu/differential-privacy

[17] "Differential Privacy," Apple.com,

https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

[18] Dwork, C., "Differential privacy: A survey of results," vol. International conference on theory and applications of models of computation, pp. 1-19, 2008

https://web.cs.ucdavis.edu/~franklin/ecs289/2010/dwork_2008.pdf

[19] Dwork, C. and Roth, A., "The algorithmic foundations of differential privacy," Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211-407, 2014

https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf

[20] Eastwood, B., "What is synthetic data — and how can it help you competitively?," MIT Management Sloan School, 2023/01/23

https://mitsloan.mit.edu/ideas-made-to-matter/what-synthetic-data-and-how-can-it-help-you-competitively

[21] Elvy, S. A., "Privacy Law's Consent Conundrum," BUL Rev., 2024

https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4830101

[22] Flamini, A., Ranise, S., Sciarretta, G. et al., "A First Appraisal of Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials,"

https://www.researchgate.net/publication/370897881_A_First_Appraisal_of_Cryptographic_Mechanisms_for_the_Selective_Disclosure_of_Verifiable_Credentials/link/6467fdba66b4cb4f73c1b46e/download

[23] Hartzog, W., "Reviving Implied Confidentiality," Ind. LJ, 2014

https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11108&context=ilj

[24] Hartzog, W. and Richards, N., "The Surprising Virtues of Data Loyalty," Emory LJ, 2021

https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4057&context=faculty_scholarship

[25] Hartzog, W., "Chain-link confidentiality," Ga. L. Rev., vol. 46, pp. 657, 2011

https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1323&context=glr

[26] Hartzog, W., "What is privacy? That's the wrong question," U. Chi. L. Rev., vol. 88, pp. 1677, 2021

https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4056&context=faculty_scholarship

[27] Hartzog, W., "Two AI Truths and a Lie," Yale JL & Tech., vol. 26, pp. 595, 2023

https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4840383

[28] "Information privacy," Wikipedia,

https://en.wikipedia.org/wiki/Information_privacy

[29] Jia, W., Zhou, B., Lu, X. and Xu, X., "Multidimensional social signature de-anonymizes low-sensitivity data," Scientific Reports, vol. 15, no. 1, pp. 31916, 2025

https://www.nature.com/articles/s41598-025-16663-5

[30] "K-anonymity," Wikipedia,

https://en.wikipedia.org/wiki/K-anonymity

[31] Liakos, P., Ntoulas, A. and Delis, A., "COEUS: community detection via seed-set expansion on graph streams," vol. 2017 IEEE International Conference on Big Data, no. Big Data, pp. 676-685, 2017

https://ieeexplore.ieee.org/abstract/document/8257983

[32] "Lie of Anonymous Data," TechCrunch, 2019/07/04

https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

[33] "Mid-year Progress Report on the ToIP Trust Spanning Protocol," ToIP, 2023/08/31
https://trustoverip.org/blog/2023/08/31/mid-year-progress-report-on-the-toip-trust-spanning-protocol/

[34] Narayanan, A., Huey, J. and Felten, E. W., "A precautionary approach to big data privacy," Data protection on the move: Current developments in ICT and privacy/data protection, pp. 357-385, 2016
http://ndl.ethernet.edu.et/bitstream/123456789/66793/1/352.pdf#page=375

[35] Nguyen, A., "Understanding Differential Privacy," Towards Data Science, 2019/06/30
https://towardsdatascience.com/understanding-differential-privacy-85ce191e198a

[36] Oberski, D. L. and Kreuter, F., "Differential privacy and social science: An urgent puzzle," Harvard Data Science Review, vol. 2, no. 1, pp. 1-21, 2020

[37] Parker, G. G., Van Alstyne, M. W. and Choudary, S. P., "Platform Revolution: How Networked Markets Are Transforming the Economyand How to Make Them Work for You," WW Norton & Company, 2016.
https://www.amazon.com/dp/B00ZAT8VS4/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1

[38] Patki, N., Wedge, R. and Veeramachaneni, K., "The synthetic data vault," vol. 2016 IEEE International Conference on Data Science and Advanced Analytics, no. DSAA, pp. 399-410, 2016
https://ieeexplore.ieee.org/abstract/document/7796926

[39] Bublies, P., "Data is giving rise to a new economy: How is it shaping up?," The Economist, 2017/05/06
https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

[40] Arntz, P., "Tor anonymity compromised by law enforcement. Is it still safe to use?," MalwarebytesLABS, 2024/09/19
https://www.malwarebytes.com/blog/news/2024/09/tor-anonymity-compromised-by-law-enforcement-is-it-still-safe-to-use

[41] Platzer, M. and Reutterer, T., "Holdout-based empirical assessment of mixed-type synthetic data," Frontiers in big Data, vol. 4, pp. 679939, 2021
https://www.frontiersin.org/articles/10.3389/fdata.2021.679939/full

[42] Powar, J. and Beresford, A. R., "SoK: Managing risks of linkage attacks on data privacy," Proceedings on Privacy Enhancing Technologies, vol. 2, pp. 97-116, 2023
https://petsymposium.org/popets/2023/popets-2023-0043.pdf

[43] Richards, N. and Hartzog, W., "A Duty of Loyalty for Privacy Law," Wash. UL Rev., 2021
https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4055&context=faculty_scholarship

[44] Riemann, R., "Synthetic Data," European Data Protection Supervisor,
https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en

[45] Rocher, L., Hendrickx, J. M. and De Montjoye, Y.-A., "Estimating the success of re-identifications in incomplete datasets using generative models," Nature communications, vol. 10, no. 1, pp. 1-9, 2019
https://www.nature.com/articles/s41467-019-10933-3

[46] Rubinstein, I. S. and Hartzog, W., "Anonymization and risk," Wash. L. Rev., 2016
https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4948&context=wlr

[47] Fadilpašić, S., "German authorities apparently cracked Tor anonymity, but onion heads say its still safe," techradarpro, 2024/09/19
https://www.techradar.com/pro/security/german-authorities-apparently-cracked-tor-anonymity-but-onion-heads-say-its-still-safe

[48] "Self-Supervised Learning," Wikipedia,
https://en.wikipedia.org/wiki/Self-supervised_learning

[49] Smith, S. M., "Authentic Chained Data Containers (ACDC)," ToIP Foundation,
https://github.com/trustoverip/tswg-acdc-specification

[50] Smith, S. M., "Secure Privacy, Authenticity, and Confidentiality (SPAC)," 2023
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.md

[51] Solove, D. J., “Murky consent: an approach to the fictions of consent in privacy law,” BUL Rev., vol. 104, pp. 593, 2024

https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4333743

[52] Solove, D. J., “On Privacy and Technology,” Oxford University Press, 2025.

https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5159448

[53] Solove, D. J. and Hartzog, W., “The FTC and the new common law of privacy,” Colum. L. Rev., 2014

https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4036&context=faculty_scholarship

[54] Solove, D. J., “The myth of the privacy paradox,” Geo. Wash. L. Rev., 2021

https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3536265

[55] Solove, D. J., “Artificial intelligence and privacy,” Fla. L. Rev., 2025

https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=4187&context=flr

[56] Su, Y., Wang, B. and Zhang, X., “A seed-expanding method based on random walks for community detection in networks with ambiguous community structures,” Scientific reports, vol. 7, no. 1, pp. 41830, 2017

https://www.nature.com/articles/srep41830

[57] “Synthetic Data Vault Tools,” Datacebo,

https://sdv.dev

[58] Looker, T., “The BBS Signature Scheme,” DIF,

https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html

[59] “The real promise of synthetic data,” MIT News, 2020/10/16

https://news.mit.edu/2020/real-promise-synthetic-data-1016

[60] Tournier, A. J. and De Montjoye, Y.-A., “Expanding the attack surface: Robust profiling attacks threaten the privacy of sparse behavioral data,” Science Advances, vol. 8, no. 33, pp. eabl6464, 2022

https://www.science.org/doi/full/10.1126/sciadv.abl6464

[61] “Trust over IP (ToIP) Technology Architecture Specification,” ToIP,

https://github.com/trustoverip/TechArch/blob/main/spec.md#61-design-goals

[62] “Verifiable Credentials,” Wikipedia,

https://en.wikipedia.org/wiki/Verifiable_credentials

[63] von Robert Bongen, D. M., “Investigations in the so-called darknet: Law enforcement agencies undermine Tor anonymisation,” NDR, 2024/09/18

https://www.ndr.de/fernsehen/sendungen/panorama/aktuell/Investigations-in-the-so-called-darknet-Law-enforcement-agencies-undermine-Tor-anonymisation,toreng100.html

[64] Wood, A., Altman, M., Bembenek, A. et al., “Differential privacy: A primer for a non-technical audience,” Vand. J. Ent. & Tech. L., vol. 21, pp. 209, 2018

https://dash.harvard.edu/bitstream/handle/1/38323292/4_Wood_Final.pdf?sequence=1

[65] “Zero-knowledge proof,” Wikipedia,

https://en.wikipedia.org/wiki/Zero-knowledge_proof