Spring 4-2025

Differential Privacy for Microdata Streams: Adversarial Approaches

Sean McElroy

DIFFERENTIAL PRIVACY FOR MICRODATA STREAMS: ADVERSARIAL APPROACHES

A doctoral dissertation submitted to Dakota State University in

partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Defense

April 2025

By

Sean McElroy

Dissertation Committee:

Dr. Varghese Vaidyan

Dr. Tom Halverson

Dr. Gurcan Comert

Beacom College of Computer and Cyber Sciences

DAKOTA STATE UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Sean McElroy

Dissertation Title: Differential Privacy for Microdata Streams: Adversarial Approaches

---

Graduate Office Verification: Brianna Mae Feldhaus Date: 04/08/2025

Dissertation Chair/Co-Chair: DocuSigned by: Varghese Vaidyan 7D0D713978DE43F... Date: 04/08/2025
Print Name: Varghese Vaidyan

Dissertation Chair/Co-Chair: _____ Date: _____
Print Name: _____

Committee Member: DocuSigned by: Tom Halverson BE50EF3DC4B5472... Date: 04/08/2025
Print Name: Tom Halverson

Committee Member: Signed by: Gurcan Comert C7BB8E96597A4F5... Date: 04/08/2025
Print Name: Gurcan Comert

Committee Member: _____ Date: _____
Print Name: _____

Committee Member: _____ Date: _____
Print Name: _____

Submit Form Through DocuSign Only
or to Office of Graduate Studies
Dakota State University

ACKNOWLEDGMENTS

Great personal achievements are rarely accomplished alone; this research is no exception. I deeply appreciate and thank my entire dissertation committee, including Dr. Halverson and Dr. Comert, particularly my committee chair, Dr. Vaidyan. Great patience and expert guidance rewarded me with knowledge, skills, and abilities memorialized in this dissertation, and I am all the better for it. Thank you for illuminating the way.

My journey at Dakota State University was influenced and encouraged by many bright minds whom I had the fortune to meet and learn from, including Drs. Streff, Rimal, Wang, Lancelot, McKee, Steinhagen, as well as Quentin Covert. These mentors and friends shared brilliance and helped me find my passion for empirical data privacy measures. It was also organized by Zotero, an amazing reference manager, and a bevy of open-source software that made my research journey possible; every open-source software developer is a hero in my book.

Finally, before embarking on this journey at DSU, many warned me that the path to a doctorate is long, dark, and perilous. A younger version of myself did not heed these monitions, but a now older and wiser me understands this completely. In the search for more light, I found great strength and profound patience during my four-year self-imposed exile, buried in coursework, research, and authorship, from my loving partner. Jake, I could not have completed this without you.

Thousands of written pages and hours later, I hope this work adds another pebble to the mountain of knowledge I climbed on my way to this point that helps another reach an even greater height. For those embarking on their own doctoral adventure: the road is long, dark, and perilous. Through great humility, you too will find great success.

Lux in tenebris

ABSTRACT

Many attacks on personal privacy exist that create a variety of harm. As the world has become more interconnected, always-on, and real-time, many entities collect, aggregate, process, use, and disseminate the whereabouts, preferences, actions, and associations of humans everywhere that can subject them to surveillance, mistreatment, identity theft, and other invasions of our private lives. Laws, rules, and regulations have not protected fundamental rights of privacy, but where policymakers have failed, technological solutions have emerged. A significant development is e-differential privacy, a technique that can inject noise into data about individuals and their actions to strike a balance between the utility of personal information and the privacy of data subjects in such databases. While differential privacy has a robust and sound approach, many data controllers and processors have failed to adopt it.

Differential privacy is a high-stakes endeavor: if implemented incorrectly, published anonymized datasets can be reassociated to identify individuals. Moreover, differential privacy is more difficult to apply to event-level data, also known as microdata streams, that represent the same data subject many times in a database with slight changes as their location or behavior varies close to an identifiable personal norm. While the mathematical guarantees of the approach have withstood two decades of rigorous review and quantitative testing, practitioners lack tools that can validate correct implementations and appropriate privacy loss budgets against future attacks on published microdata streams. This proposal addresses that research gap through quantitative technical action research that culminates in two experimental artifacts that adversarially interact: one that attempts to identify weaknesses in the application of differential privacy and another that tries to resist privacy-harming reassociation of event-level data. The iterative and adversarial interactions between these two artifacts allow for the progressive improvement of

each that can both identify and treat implementation errors of differential privacy across various domains.

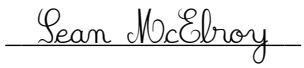
The production of generalized tools that can validate applications of differential privacy would yield a novel and significant contribution to many fields that generate or handle microdata streams, including geolocation data. Validating these tools first in a synthetic empirical cycle and then for a real-world scenario in a client engineering cycle using quantitative, statistical approaches enables future research and application of these artifacts and the principles they implement to protect the personal privacy of individuals in our increasingly connected and scrutinized lives.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,



Sean McElroy

COPYRIGHT

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

1.1 Overview

Thomas Paine, a Founding Father of the United States, opined: "Liberty cannot be purchased by a wish". It is by knowledge and intention that freedoms are guaranteed, as increasing surveillance and aggregation threaten to remove the choice of individuals to decide how their lives and actions are known and published. As devices from pocket watches to mobile phones to connected vehicles collect continuous streams of microdata about our actions, movements, and even our heart rates, significant effort is required to retain privacy today. The privacy threats manifested by modern technology are well documented, but the methods to protect against subsequent harms, especially for the constant recording of minute changes, are the subject of a rich and growing body of privacy knowledge.

Differential privacy is a process that modifies the actual values in a statistical database such that the membership of a single individual's data within it cannot be inferred from subsequent knowledge and analysis of the entire population of modified entries. This process involves perturbing each categorical and numerical value from its original, actual value by adding random noise in a calculated way. The wholesale modification of records can lead to nonsensical record values that may not align with their domain, such as households with zero or a dozen residents where two genuinely reside. However, aggregates

of differentially private databases, such as averages, medians, and means, closely represent the original data. Thus, applying a random noise-generating function and the magnitude of the noise added allows dataset publishers to make an informed tradeoff between utility and privacy in a manner that provides rigorous mathematical guarantees.

Many applications of differential privacy have focused on data sets that contain one entry, or row, per data subject. Indeed, many data sets are structured as such, including census roles, patient listings, and survey respondents. However, there are many areas of concern about whether differential privacy can and is applied where this structure is not maintained, notably in data interchangeably called "microdata streams", "set-valued data", and "itemsets". These structures can often represent the same data subject with different attributes in the database, such as geolocation coordinates over time collected by a navigation application or clickstream telemetry data collected by a browser extension. However, stream data may be highly cross-correlated, harming the guarantees of differential privacy made over single-subject databases and requiring specialized design and implementation considerations. This potential represents an open and active problem for differential privacy to protect the privacy of data subjects in microdata streams.

1.2 Statement of Problem

Differential privacy, a process that modifies the actual values in a statistical database such that the membership of a single individual's data within it cannot be inferred from subsequent knowledge, has been hailed as "the gold standard for privacy protection in computer science and cryptography" [1]. However, the consequences of correlations among data set entries must be carefully considered when applying the technique, which uses an additive noise mechanism to item attributes. When correlating them with external demographic or behavioral data sources, an observer can reidentify the same data subject multiplied by alternate values, such as geolocation coordinates, across a time series. While this type

of event-level privacy risk in "microdata streams", "set-valued data", and "itemsets" is well-researched literature, the methods for detecting and addressing this risk are highly domain-specific [2]–[4].

Implementers seeking differential privacy have multiple toolkits available to aid them, such as CASTLEGUARD and OpenDP [5], [6]. However, these toolkits and the expansive body of research can be challenging to parse, if not inaccessible. While a large body of differential privacy research explores these challenges and potential solutions related to microdata streams, it is often highly domain-specific in its focus and offered solutions. Some research efforts are so focused on theoretical data shapes or narrow applications that other researchers have questioned whether the body of knowledge suffers from oversaturation by cherry-picking unrealistic scenarios and producing validated approaches that are not generally applicable [7], [8]. The stakes are high, as an error in applying differential privacy techniques renders published datasets vulnerable to reidentification attacks, a Pandora's box that cannot be closed once made publicly available for scrutiny.

1.3 Purpose

The purpose of this research effort is to explore the frontier of the mathematical guarantees of differential privacy, as formally established by Dwork et al., and the subsequent improvements in the general body of knowledge as they relate to microdata streams [9]–[11]. The technique's efficacy is well-explored across various domains and data shapes. However, without a tool that implementers can use to measure the safe application of differential privacy, they may have set the privacy loss budget ϵ inappropriately to achieve the desired balance between privacy and utility, or the data may have unaddressed or even unidentified correlations that could open a published data set to reidentification attacks. By exploring this frontier, this research shall outline ways to identify and address these errors and deliver reusable research artifacts.

1.4 Research Questions

Question 1: How well does ϵ-differential privacy generally protect microdata streams containing many records correlated with the same data subject or cross-correlated to each other?

The first research question relates to how well ϵ-differential privacy generally protects microdata streams containing many records correlated with the same data subject or cross-correlated to each other. Various attacks on differential privacy have been described and tested in domain-specific research, particularly concerning correlations for event-level data in microdata streams. Much early research into the method's efficacy from 2006 to 2015 focused on applying differential privacy when applied 'continuously' to database query result sets, where repeated queries could tease out underlying values with enough differentially private responses. This type of information disclosure through repeated querying is variously referred to in the literature as 'differential privacy under continual observation' [10]. However, continuous observation in this era of research did not refer to the same data subject observed continuously over a time series, but rather demographic subset demographics repeatedly observed as a set [12].

Question 2: Are there treatments that better preserve the privacy loss budget and the utility of ϵ-differentially private microdata streams at scale and across domains?

Similarly, however, more observations can leak information as additive noise can be averaged out if the application method for a given privacy budget insufficiently protects against correlations over a dimension, such as time. Microdata streams, often represented as continuous time series itemsets, are usually explicitly tested for a given schema rather than generally assessed for correlation attacks. By developing a framework and measurement approach for generally assessing the guarantees of differential privacy across microdata streams, the purpose of creating a reusable artifact for implementers can be realized. The second research question posits whether there are treatments that better preserve the

privacy loss budget and the utility of ϵ-differentially private microdata streams at scale and across domains. As noted in the research problem statement, the field is ripe with efficacy research testing the juncture of a given microdata schema and a shared fine-tuned approach to adjust and measure the resulting changes to the privacy-utility trade-off of a differentially private output. Suppose one can construct a viable generalized approach to measuring the frontier of differential privacy for microdata streams. In that case, generalized treatments, including those generated by machine learning or artificial intelligence approaches, may be developed as broadly applicable for more than just a nuanced microdata schema.

1.5 Significance of Study

Undoubtedly, developing a generalized approach for measuring the fitness of differential privacy for microdata streams in terms of correlation risk would be challenging, given the diverse forms event-level data can take. However, the resulting measurement would broadly apply in research and practical contexts. In research contexts, a generalized approach would improve the research efficiency of new treatments and allow for a comparative analysis of adjacent problem domains through a joint assessment of correlation risk. In practical contexts, a generalized measurement approach would allow varied practitioners across industries to gain privacy assurance in their privacy engineering work, which today requires a deep mathematical and statistical understanding to assess. By safely opening the application of differential privacy to more practitioners, the privacy of individuals within microdata streams would be better preserved.

1.6 Conceptual Framework

The primary constructs of this research are statistical structures, which are "phenomena that can be described by variables, [with values having] a probability distribution over the

set of possible phenomena" [13]. Specifically, this research focuses on microdata streams cross-correlated with data subjects. In the illustrative case of mobile device geolocation data, the association of timestamped ping in a sample is related to the probability that all other future-timestamped pings relate to the previous one. Various characteristics of a ping, such as the latitudinal and longitudinal position, velocity, and time-delta, influence the probability that other pings that are future-dated may represent the same data subject.

The conceptual framework entails a set of structured microdata belonging to fewer data subjects. Each subject set within the data set has several continuously related records representing a data stream of elements about a data subject over time. This data stream may either be one-dimensional (such as a heart rate or absolute speed) or multi-dimensional (such as a geolocation stream with latitude, longitudinal, and altitude values) and additionally includes a stable anonymous identifier to distinguish related microdata elements belonging to the same data subject. A client who possesses this data in a raw and precise form, called the data provider client, wishes to share data with a data consumer client in a manner that preserves the identity of data subjects and maximizes the utility for the data consumer client, thus its economic value. These are problem concepts. The conceptual framework contains specialized concepts related to the harm of privacy data [14], such as surveillance, secondary use, decisional interference, and exposure.

1.7 Summary of Methodology

ϵ-Differential privacy, as differentiated from intuitive definitions of general differential privacy that emphasize the relative difficulty in identifying individuals in a given data set, is mathematically defined as the probability that a given element (where an element is a datum or a subset) is or is not present in a privacy-preserving transform of that data set, within a given privacy loss budget [11]. To answer the first research question, how

the number of multiple, related microdata attributes in a data set improves the ability for an artifact to make inferences that correlate them, one needs both an artifact that can make such inferences and a sensitivity analysis to establish the limits of efficacy for the artifact given changes in related microdata attributes. To answer the second research question, the dual engineering cycle of iterative development of an artifact is appropriate and necessary to solve this problem for a client in a real-world problem space.

Several methodologies were considered for this research question, including a hybrid, or multimethod, approach that includes both design science and quantitative methods. Mixed method approaches, in contrast, combine quantitative and qualitative approaches in various ways and are the most popular subset of a broader approach to multimethodology [15], [16]. More generally, multimethod approaches provided combined benefits of different methodologies and balanced non-overlapping weaknesses, but not necessarily based on a quantitative-qualitative distinction [15]. Although technical action research may be considered more prominent in qualitative research questions, mainly where it includes participatory research such as in adult education [17], [18], this methodology is also well suited to empirical validation of an experimental artifact [13]. Unlike multimethod and mixed-method approaches, TAR provides for an iterative cycle of design and validation rather than more traditional, sequential approaches.

The research question has two distinct dimensions: Can an experimental artifact detect cross-correlation of related microdata series in a data set with ϵ-differential privacy applied, and under what circumstances can one accurately detect them? The first dimension represents a knowledge question that can be answered by a program, an algorithm, or an applied method. Design science approaches are generally suited for this dimension, as "design science iterates over solving design problems and answering knowledge questions" [13]. However, the second dimension, 'under what circumstances', requires an experimental and empirical approach, which is a form of studying the "utility of an intervention" or "understanding the best predictors of outcomes" [19]. Because the research experiments

need to validate both the robustness of the ϵ-differential treatment against the artifact's efficacy for establishing limits of the treatment guarantees in specific microdata contexts, the iterative artifact refinement cycle characteristic of technical action research is the best methodological fit for this research question. Furthermore, TAR is well suited to validating an artifact in a real-world context, and since ϵ-differential privacy toolkits, such as OpenDP, are available and becoming more widely available, ensuring that the methods they employ are used with appropriate contexts is vital to successful implementations that preserve privacy within an expected privacy loss budget.

1.8 Limitation of Study

Technical action research is significantly longer due to its dual empirical and client engineering cycles. As such, the potential applicability of the proposed research outcomes may be limited to the extent that their development is curtailed by the available resources and time to continue iterating through the research cycle. In addition, an adversarial approach in which a generalized measurement artifact informs the development of a generalized treatment will necessitate design, empirical, and engineering decisions that may underfit for a given mock model or overfit for a particular client engineering problem space. Testing the broad applicability of finalized research artifacts is essential to understanding the overall significance and replicability of the work, which may be limited to the extent that diverse client engineering problem spaces are available and testable with the resulting artifacts.

Chapter 2

Literature Review

2.1 Introduction

Differential privacy has grown, matured, and evolved significantly in the nearly two decades since Nissim and Dinur revealed the 'Fundamental Law of Information Recovery', which asserts that one cannot guarantee privacy for a dataset without adding noise that perturbs the attributes of published elements [20]. The advent of a mathematically sound method, which forms the basis of Cynthia Dwork's work on differential privacy, fundamentally changed technical data privacy [9]–[11], [21]. From these significant and fundamental contributions, the field has grown in many different research domains and, in some cases, matured to oversaturation. The following review of the body of knowledge of differential privacy as it developed from a general approach to guarantee privacy following a privacy loss budget to the nuanced approaches specific to providing the same across various types of microdata streams uses a systematic approach. From a systematic search and selection, relevant contributions are evaluated for their importance in forming the basis for the research questions central to this dissertation.

2.2 Related Works

2.2.1 Applying Differential Privacy to Search Queries in a Policy Based Interactive Framework

This early work, soon after Dwork's seminal papers on data privacy [9], [10], [21], [22], briefly touches on concepts developed by many following works, including categorical vs. numeric attributes relevant to personal data, challenges specific to interactive and repeated queries of differentially private data, and the challenges of choosing an appropriate privacy loss budget ϵ [23]. The purpose of this study is to explore the relationship of e to the noise parameter, albeit through a curious quantitative lens: an evaluation of data processed through the Microsoft Research 'PINQ' tool, an extension of the at-the-time popular LINQ library of .NET extension methods that provided differentially private outputs. This mapping is explored in the context of the order of results returned, which differs from the general guarantee of differential privacy about individual participation within a data set of query logs.

Query logs are a form of private microdata stream, or set-valued data, as for a given client, they contain a chronological set of terms that expose the state of mind of the querier. Individual terms, term groupings, the spelling of terms, and the progressive refinement of a query can uniquely identify individuals. However, this paper uses empirical methods to explore this topic without defining a null hypothesis (or confidence interval) or demonstrating a conclusion regarding a statistical result. Nevertheless, it exemplifies the significant interest in using differential privacy to protect microdata streams in database queries, which has remained a substantial area of academic interest in the literature from the late 2000s through the 2010s.

2.2.2 Differential Privacy for Location Pattern Mining

The exploration of the application of differential privacy in this research experimentally details the relationship of location-based data, also known as 'trajectory data' in the literature, not so much based on its results but rather the discussion about the unique nature of trajectory data in differentially private databases when users can opt out of them [24]. In the context of the trajectory data set reviewed, privacy is defined as the ability to match pauses, or 'stay points', of individuals in bounded areas of interest. Measurements are conducted for the true positive rate and the miss rate of matches across a continuum of privacy loss budgets.

A key finding early in the paper is the acknowledgment that concealing whether an individual is a member or not in the dataset is more challenging than what can be measured empirically from such a pattern-mining exercise. Because inferences can be drawn from locations where users loiter, opting out of collection at a given stay point can become apparent when habitual patterns are inferred from large trajectories for individual users. Second, the combination with outside data can establish a context that allows for the reidentification of individuals or information leakage about when a portion of an individual's data set is excluded. This problem is unique to databases of microdata streams.

2.2.3 Publishing Set-Valued Data via Differential Privacy

The challenge mentioned above of context is addressed head-on by this research that explores how to eliminate context to protect set-valued data [25]. Chen et al. recognize that when itemsets or their categorical values are partitioned, the mechanism for partitioning can leak additional information that harms the guarantee of differential privacy. By strictly building context-free taxonomy trees, partitioning schemes do not encode latent information that can be used to correlate or ultimately reidentify data streams. This scheme has implications for all microdata streams that may be published, and this re-

search validated this with technical action research first over synthesized model databases and two large real-life data sets. It is the first chronologically published paper in this systematic review that identified context as a danger and provided a theoretical framework and practical application to address this for streams.

2.2.4 Probabilistic Relational Reasoning for Differential Privacy

Because differential privacy guarantees privacy rooted in sound mathematical proofs [11], in theory, formal verification mechanisms could be used to validate a given implementation. Barthe et al. produced a groundbreaking paper introducing Coq, theorem-proving solver software, to the domain in this highly technical paper that expresses differential privacy in terms checkable by Coq, called CertiPriv [26], [27]. This method is explored for several theoretical domains in the paper, including 'data streams'. In the context the term is used in this design science research paper, it could equally apply to differing uses of the word: both repositories that are continuously changing due to a continuous 'streaming' influx of new, edited, or deleted records, or the same for cross-correlation set-valued data. Researchers seeking to formally validate differential privacy for microdata streams are informed by a series of logical proofs in this work that can be adapted for Coq or related theorem provers.

2.2.5 PrivBasis: Frequent Itemset Mining with Differential Privacy

As stated earlier, microdata streams are synonymous with set-valued data and itemsets. Frequent itemset mining, or finding items frequently occurring together in a data set, presents a challenge for differential privacy. Such analysis is not dissimilar to the location pattern mining explored by Ho & Ruan but is a more general case that applies to economic and medical research [4]. A refinement of prior work in the domain of knowledge discovery

in databases (a storied and expansive subfield in information science known simply as KDD), the purpose of this empirical design science research was to improve on previous frequent itemset mining (FIM) techniques, which began to break down at large values.

FIM has particular analytical applications for microdata streams. Accordingly, the researchers measured the utility of differentially private processing by analyzing false negative and error rates across five databases. Two contained microdata streams (search queries and web navigation clickstreams). The particular basis-reduction method in this research was a key finding, as rich microdata streams can be treated in a dimensionally reduced fashion to preserve privacy in highly correlated schema designs for microdata streams [4].

2.2.6 Geo-Indistinguishability: Differential Privacy for Location-Based Systems

Implementing differential privacy for continuous numerical values is generally realized by adding the outputs from a random noise function, typically Laplacian or Gaussian noise, to each value. This work considered an improved privacy outcome by considering differential privacy not as the perturbation of each dimension of a trajectory vector but in the context of location-based data, as a distance from an actual location calculated as the distance to perturb a 2-dimensional location on a map [28]. While novel, the authors acknowledge that microdata streams, such as trajectory information, are insufficiently protected by value modification alone in the face of correlation attacks against time-series microdata streams. This problem is fundamental in many industries' applications of differential privacy, where streams are annotated by time. That dimension is the critical context that can allow for inferences and additional correlations that do not protect the post-processing guarantees of differential privacy.

2.2.7 Differential Privacy in Intelligent Transportation Systems

Traffic management centers that track the movement of individually identifiable automobiles collect, process, and store sensitive information that can harm data privacy. Kargl et al. adopt the nomenclature to discuss the problem of microdata streams by distinguishing between event-level privacy and user-level-privacy like Dwork et al. when they were discussing changing database membership with streaming edits [10], [29]. More than merely recognizing the problem, this quantitative research proposes that an entire user's stream (or set values) should be treated as a whole set for the user to form the privacy loss budget ϵ. This research admits that extending the benefits of differential privacy to sets rather than individual rows may reduce utility to a level unacceptable by clients of such a system.

2.2.8 Monitoring Web Browsing Behavior with Differential Privacy

Clickstreams can be especially difficult to protect with differential privacy, as raw clickstream data can include specific network address information and query string parameters that contain Urchin Tracking Module (UTM) parameters, which makes protecting this set-valued data challenging. Fan et al.'s paper demonstrates a disparate approach to addressing microdata streams: generalizing itemsets into aggregates before applying differential privacy [30]. Unfortunately, obscuring quasi-identifiers through grouping constructs reduces utility by an additional factor beyond the reduction realized by the ϵ-differential privacy budget applied. While this proposed model in this work could be an excellent fit for a nuanced application for aggregated clickstream data, the approach could be construed as the sprinkling of differential privacy over anonymization, which does not allow for a parameter-based approach for trading off utility for privacy.

2.2.9 Distributional Differential Privacy for Large-Scale Smart Metering

Smart meters that track high-fidelity power usage over time create microdata streams of information that can be highly sensitive. Such information provides insights into course behaviors when compared against known structural characteristics of a household, such as air conditioning frequency and efficiency. These microdata streams, even at a summation level, can provide information that exposes specific device types within a residence when the source data can be queried multiple times over different periods with narrow criteria [31].

Unlike the previously discussed research, these aggregated sources of data provide anonymization. Smart metering data is already aggregated because the collection point is the primary distribution inlet to a structure's electrical system. The critical insight of this research for differential privacy of microdata streams is the relationship between the distribution of item set values and the sum queries across multiple item sets. Because item set values were normally distributed in this domain, sum queries were also distributed, and differential privacy could be applied to the sum queries. This insight provides a conditional application for a subset of microdata streams for normally distributed sum queries.

2.2.10 Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies

Genomic data are a form of microdata stream when considering the encoding of genetic information, which is highly dimensional and contains redundancy of attributes in the form of repeated codon sequences. While the data about a single individual may not be represented multiple times, large segments of genetic sequences are a form of set-valued data and are therefore included in the scope of this literature review. In this theoretical

work, Tramèr et al. explore the forms of attacks specific to large set-value data sequences that can be generalized as a problem for all forms of microdata streams.

Prior knowledge of a subset of attributes of highly-dimensional set-valued data has a similar effect of high cross-correlation of data set members in that the amount of data perturbation required to satisfy the privacy loss budget ϵ depends on the range of this prior knowledge for positive membership privacy [32], [33]. Depending on this range, Tramèr et al. note that as a primary result of this research, this may require less additive noise than is needed to implement the classical definition of differential privacy. This insight may hold broader implications for establishing privacy loss budgets in many microdata streams where prior knowledge exists or can be assumed through correlative techniques with additional data sets.

2.2.11 Protecting Locations with Differential Privacy under Temporal Correlations

When timestamps are collected alongside microdata streams, the literature, including this research, may specify that the data set requires "event-level differential privacy" [10], [34]. The contribution of this theoretical framework, validated through technical action research, is that the classical notion of differential privacy must be made more specific. Rather than require that a single event's membership be unknowable between two 'neighboring databases', more stringent protection is needed. For location-based, timecoded data, the event for a given subject must be indistinguishable from a δ-location set, defined as the probable locations for a user in their trajectory vector, rather than the entire database [34].

This concept is novel and essential for many microdata stream manifestations, often encoded with absolute or relative timestamps. This approach "guarantees the true location is always protected in δ-location set at every timestamp" [34]; however, it fundamentally requires the data set publisher to apply differential privacy to accurately define

and implement the δ-location set membership for the correct definition of "probable" in the context of the microdata. For instance, pedometer data may be defined as probable as the distance achievable by human movement. However, were this the sole definition of probable, a jogger who embarks on a city bus that travels faster than a person could run would break this assumption. Regardless, this contribution provides a practical approach for a 'continual observation' consideration first acknowledged by Dwork [10], [11]. However, the researchers also note that this method protects the data of a single event but does not protect the entire trajectory, which may be discernable from outside context or correlation even when using a δ-location set. Xiao & Xiong further developed a version of this publication in a journal article, which included a more focused look at Markov models generally treated in this work [35].

2.2.12 Bayesian Differential Privacy on Correlated Data

While microdata in streams may be highly correlated for set member groups within set-valued data, Yang et al. focus on the dangers of external correlation and contribute a more stringent definition of differential privacy to account for such [36]. Using a Bayesian rather than frequentist approach, the researchers express an algorithmic extension that converges to classical differential privacy as adversarial knowledge grows to the full breadth of the data set, excepting a single entry and scales backward as a function of that adversarial knowledge to express differential privacy under the threat of correlation. While widely discussed as a problem, this is the first paper chronologically in the papers eligible for this systematic review that directly provides a solution that can generalize the problem and formally define it with algorithmic methods.

2.2.13 Deep Learning with Differential Privacy

The topic of how deep learning algorithms, including those used to train machine learning models and neural networks, is a lively topic of societal debate and recent academic

research, invigorated by recent developments in AI and concerns related to data privacy and copyright protection. How such algorithms can be accountable to data privacy is the topic of this research, which focuses on defining and measuring an aggregate privacy loss function through deep learning training and performance testing [37]. The utility effects of implementing ϵ-differential privacy in deep learning contexts are mixed in this paper. For the MNIST data set of handwriting recognition, a typical machine learning benchmark also tested in this paper, accuracy was reasonably high (≥ 0.89) at minimal values for ϵ (10-5); however, another benchmark tested, the CIFAR image dataset, faired much poorer in accuracy with a less private (higher values for ϵ) application of differential privacy, at least 7% off from state of the art [37]. The research acknowledges that implementation choices can significantly impact utility when differential privacy is applied in deep learning contexts. Special care must be taken to ensure that when microdata streams are mined with techniques drawing from knowledge-discovering in databases (KDD) in deep learning systems, that utility is carefully measured across all iterations of an implementation.

2.2.14 Composing Differential Privacy and Secure Computation: A Case Study on Scaling Private Record Linkage

As discussed in previous research, the linkability of records through external correlation, a phenomenon this paper by He et al. refers to as Private Record Linking (PRL), is formally researched as a set of tradeoffs among existing methods that are relevant to microdata streams. The tradeoff is observed that prior approaches to protect against PRL are correct, private, or efficient, but not all three simultaneously by their threshold definitions [38]. Concurrently, the paper defines a concept of "end-to-end privacy", which is loosely used in other work in the literature of this era in adjacent privacy research to refer to privacy properties holding at each stage of a transform or for each intermediary for a federated learning or distributed environment. The primary contribution of this quantitative research is a new method for outputting results from a dataset that is unperturbed

by an additive noise function, or 'truthful release,' while preserving differential privacy guarantees over the database. However, the authors note that the practical applications of partial truthful release are of unknown practical value.

2.2.15 Constrained-Based Differential Privacy for Mobility Services

Fioretto et al. noted that differential privacy could cause undue burdens for microdata streams for specific applications sensitive to the perturbations Laplacian additive noise introduces. In particular, multimodal transit systems that use real-time location data to determine the real-time shifts in origin-destination pairs across a city can lead to inefficient traffic flow changes and economic inefficiencies when investments are directed based on an inaccurate understanding of accurate system usage [39]. While recognizing the privacy harm insufficient privacy protections can cause for data subjects represented in microdata streams, the key finding of this quantitative research is that by carefully redistributing noise to preserve certain features essential to consumers of the private data set, differential privacy can still be achieved through non-traditional means and data set consumers enjoy far more efficiency in subsequent decision-making without harming data privacy to the extent traditional differential privacy guarantees it. This work is notable for the research's utility and for recognizing that adversaries may not enjoy full knowledge of a constrained-based, differentially private system and could fare better or worse in various correlation-based or other attacks.

2.2.16 Publishing Spatial Histograms Under Differential Privacy

As previously discussed in work by Xiao & Xiong, temporal correlations pose a significant risk to data privacy; however, even when no temporal attribute is encoded in set-valued

data, location data is equally problematic for data subjects. This work by Ghane et al. denotes this and provides a novel extension of differential privacy for set-valued data that can be transformed from trajectory datasets and subsequently aggregated into spatial histograms. While spatial histograms may appear to protect trajectories sufficiently at courser resolutions, multiple queries can provide for detectable changes that allow the location and trajectory of an individual to be inferred [40]. By estimating the number of trajectories in the data set and using that parameter as part of the update function for a differentially private particular histogram, a novel improvement was realized: the utility for these types of two-dimensional aggregations is more consistent in utility across variable data. Again, as in Fioretto et al.'s research, the literature broadens applicative interest in differential privacy as domain-specific implementations reimagine the algorithms while guaranteeing the same classical tenants.

2.2.17 Practical Collaborative Learning for Crowdsensing in the Internet of Things with Differential Privacy

Differential privacy was initially conceived in a single database, where the population could be known and considered for developments for attribute privacy such as ℓ-diversity and t-closeness. However, these guarantees naturally lend themselves to central data repositories. When highly sensitive data is collected in massive quantities, implementation weaknesses of privacy handling technologies are amplified at scale, increasing the risk of privacy harm. The introduction of LDP, or local differential privacy, is far earlier in the literature on differential privacy [41], [42]. Local differential privacy provides a distributed model for sensitive data collection, aggregation, and treatment for differential privacy.

This work, however, by Guo and Gong, offers an improvement for local differential privacy that addresses a problem for this when applied to datasets, including microdata streams. For those sets, centralized and local differential privacy require additive noise to be applied to each set member when queried. When noise is used independently, the

standard deviation grows, and conversely, the average testing accuracy decreases with membership size scaling [43]. This work uses collaborative learning across many similar devices with an algorithmic technique known as the alternating direction method of multipliers (ADMM) to reduce the standard error that would otherwise grow proportionately with member size. This publication is the first of many papers in this chronological, systematic review that proposes a nuanced improvement for LDP.

2.2.18 Trajectory Privacy Protection on Spatial Streaming Data with Differential Privacy

Further developing the broad research themes previously discussed in Xiao & Xiong and Ghane et al., this publication by Liu et al. notes the unique problems of differential privacy as applied to microdata streams and further acknowledges while subsequent work has addressed temporal correlations, spatial correlations for location-based data remain problematic [44]. An essential contribution of this quantitative research is that differential privacy cannot be applied to event-level data without unique considerations if those events contain spatial trajectories. In that case, this paper proposes that each trajectory (e.g., home→office→grocery→home) must be independently differential private to protect against spatial correlation attacks. This research directly addresses a gap previously noted in the temporal correlations work by Xiao and Xiong. The analysis in this work by Liu demonstrates that applying differential privacy globally or even on a per-location basis for each node on a set of overlapping trajectories is insufficient to achieve the mathematical guarantees differential privacy requires for spatial microdata streams.

2.2.19 Amplification by Shuffling: From Local to Central Differential Privacy via Anonymity

Microdata streams can be represented in many ways: processed centrally or in a distributed manner, with or without temporal or spatial dimensions that enable correlation attacks and membership inference attacks via relationship and static or streaming data sets. The specific scenario explored by Erlingsson et al. is a form of microdata that records users' private preferences as an event stream of changes to those preferences. The method proposed in this quantitative research is to anonymize data, including timestamps, and then shuffle entries using a random permutation [45]. With this approach, the property of differential privacy can be theoretically demonstrated over a contrived dataset. When tested in a local differential privacy system, the implication is that lower values of ϵ may be acceptable for the given dataset characteristics. However, the practical application of this specific work may be narrow, given the nuanced prerequisites for this outcome to hold. The authors acknowledge these limitations in the discussion section. Curiously, they also predict that industrial applications of LDP may have overbudgeted for privacy without qualifying, which might adhere to domain requirements specified and tested in this work.

2.2.20 Differential Privacy-Based Indoor Localization Privacy Protection in Edge Computing

As Zhang et al. note in their wireless access point stream research, sensitive information about users can be leaked in unanticipated places in network devices. In this research, the signal strength between a wireless client and a wireless access point, in terms of its received signal strength indicator (RSSI), can be used to locate the physical presence of clients through triangulation [46]. However, the methodology of this technical action research is curious in several respects, given the development of related literature up to

this point. For one, a training data set of RSSI values is split arbitrarily and labeled by location through a neural network classifier (e.g., office area or lounge area). Next, the intermediate weights of the neural network's hidden layer are processed, treated with ϵ-differential privacy, and recombined. With the network trained, actual RSSI values are placed through the same process for classification.

Remarkably, because differential privacy is not applied to the resultant data set but to an intermediate processing component that does not represent either a user or event in that intermediate form, the application of Laplacian noise is uncertain as to the privacy afforded users from this scheme. The authors note that ϵ values of <1 create "Especially, when ϵ <1, noise is too large for the network to minimize loss. However, when epsilon is close to 2, high accuracy and not too weak privacy can still be obtained at different error distances." [46] However, the practical deployment of wireless access points and how this privacy budget impacts users in the real world are not considered. Across an office environment with three access points, it is sufficient in many contexts to know a user is within range of any of them.

Conversely, depending on the density of access point deployment across a large university campus, the privacy afforded by this scheme may be tremendous or inconsequential. In addition, the density of access points will vary across residence halls, classrooms, libraries, and open spaces between them. Consequently, this research is an interesting application that is so nuanced in the application of neural networks that it could benefit from adversarial testing to understand the proposed benefit in practice.

2.2.21 Local Differential Privacy with K-anonymous for Frequency Estimation

Recognizing the challenges of microdata streams, particularly for set-valued data where many different elements are present for each data subject, Zhao et al. shy away from refining differential privacy directly to address the privacy leakage potential: they rein-

troduce k-anonymity [47]. It is not established in prior literature whether layering the separate approaches of k-anonymity and differential privacy afford both benefits. Similarly, there appears to be no previous research that, when combined in any particular sequence, differential privacy addresses the weaknesses of k-anonymity in homogeneity or background knowledge attacks while maintaining a measurable and acceptable privacy loss budget and utility.

Other works reviewed in this systematic literature use mean absolute error (MAE) as the utility measurement function when assessing their proposed refinements. Divergently, this work abandons MAE as a measurement of utility and uses relative error, a utility measure largely abandoned in prior literature around 2012 [4]. This curious choice prevents an assessment of the proposed algorithm to other state-of-the-art approaches for microdata streams.

2.2.22 R2DP: A Universal and Automated Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions

Literature sometimes states that the additive noise function for differential privacy will be from a Laplacian distribution, and another popular choice is the Gaussian (normal) distribution. Both distributions are heavily weighted at zero on the x-axis of a Cartesian plane and serve as a source of how much perturbation should be applied to every value to effect differential privacy, with the centroid being no perturbation and it becomes less likely that a high degree of error is injected. The central theme of this research is to determine which distribution is the most appropriate and their parameters thereof in a context-free manner, given the characteristics of the underlying data [48].

Acknowledged in several places throughout, microdata streams (whether locations or

time-series data) require special handling because their privacy budgets differ from user privacy needs. This publication defines the error bounds for 'location privacy' applications, including generally itemset privacy, but stops short of offering an inclusive solution or the R2DP framework under streaming contexts. Mohammady et al. note that the solution is extendable to microdata streams, and additional research and approaches appear necessary as privacy and utility for these contexts (referred to as the "$\ell 2$ metric" in this paper) are not improved for all tested privacy budgets ϵ.

2.2.23 Association Rule Mining with Differential Privacy

Association rulemaking is a form of rule-based machine learning for identifying dependencies and relationships between variables [2]. Similar in some respects to frequent itemset mining, as previously reviewed in the PrivBasis work, this field frequently operates over microdata streams or event-based data, such as transactional records, to optimize sales, marketing, and operational efficiencies. This work by Zhen et al. identifies several mechanisms to extend differential privacy to itemsets to address the unique privacy leak cases while maintaining an improved balance of privacy budgets and utility at scale.

Two novel mechanisms are proposed in this quantitative work: the reduction of dimensionality of microdata streams and resolution to lower the number of candidate itemsets over which differential privacy must operate and an adaptive allocation of privacy budgets ex-post [49]. However, as the literature related to microdata streams broadens in the late 2010s to the present, more works, including this one by Zhen et al., are measuring privacy loss incidentally to the chosen dataset and parameters for analysis and not logically to show these mechanisms are consistent across data sets of unanticipated size or characteristics. This situation has led some researchers to lament that the additions to the body of knowledge may be so nuanced and narrowly applicable as less impactful [7], [8]. In any case, minimizing data for publication is beneficial to adhere to privacy best practices [50], whether or not the reduction of dimensionality improves the results of a

specific transform, like differential privacy.

2.2.24 CASTLEGUARD: Anonymised Data Streams with Guaranteed Differential Privacy

CASTEGUARD [5] is a proposed extension to CASTLE [51], a solution for providing k-anonymity to continually streaming data, whether or not that data requires user or event-level privacy. This work by Robinson et al. implements differential privacy first and then clusters intermediate results in a k-anonymous and ℓ-diverse compliant manner. This 'bolt-on' approach of differential privacy with existing anonymization mechanisms is valid, although the aggregate error can be significantly higher than k-anonymization alone, depending on the parameters chosen and the implementation of differential privacy (centralized vs. local). Unusual for differential privacy literature for microdata streams that provide a proof or experimental result for utility and error, this work does not quantify the aggregate error, so its practical application is not fully demonstrated.

2.2.25 Continuous Release of Data Streams under Both Centralized and Local Differential Privacy

Focusing on providing event-level differential privacy for an eternal stream of inestimable size, Wang et al. propose an astonishing improvement in utility for differentially private range queries of 10 orders of magnitude [52]. However, upon closer inspection, because mean squared error (MSE) is the utility metric chosen for comparison, the magnitude of improvement is an artifact of the utility function, which magnifies differences (e.g., 10^{21} vs. 10^{13}). The proposed algorithm has some unique properties: it truncates result sets in an adaptive manner that aims to improve utility, and it smooths outputs to reduce the magnitude of noise.

Both approaches across four data sets of microdata streams that themselves stream on-

line into the system yielded utility improvements. The net result of these enhancements, which 'spend' the privacy budget ϵ strategically, is to maximize utility. However, this approach can only offer an ex-post differential privacy outcome, despite four successful tests across relevant data sets, if the approach cannot be formally verified for unanticipated data. Minimizing noise error, which this research achieves, also negatively impacts differential privacy guarantee if it allows correlation attacks.

2.2.26 Risk-Aware Individual Trajectory Data Publishing With Differential Privacy

The introduction of IDF-OPT by J. Zhao et al. in this work is an essential development for privacy preservation for microdata streams. This work posits the challenges differential privacy faces when the underlying data set not only contains user trajectories that can be correlated with external data sets but also when the same subject is represented with multiple, including overlapping and repeated, trajectories that can allow for the establishment of behavioral patterns that would enable reidentification [53]. The proposed approach and associated algorithms documented in this work are significant for research questions pertinent to microdata stream privacy, given that the model incorporates a correlation measurement and feedback mechanism to adjust additive noise parameters.

Up to this point in the literature considered in this systematic review, improvements in differential privacy have optimized the base case of classical differential privacy with applicative tweaks but did not include an adversarial testing mechanism. While the method is specific to spatiotemporal trajectories, the general approach is intriguing for its generalization for other highly correlated microdata data formats across differing dimensions outside spatiotemporal concerns. This quantitative, technical action research publication considers a tuple of time, latitude, and longitude, although the method, on its face, appears generally applicable across other dimensions of quasi-identifiers. The approach is algorithmic and treated as a Pareto optimization problem, which can be expressed in a

format simple algorithms or even Boolean satisfiability testing tools for specialized use cases could address.

2.2.27 RoD: Evaluating the Risk of Data Disclosure Using Noise Estimation for Differential Privacy

While a quantitative analysis of differential privacy as it relates to Laplacian distribution analysis (noise estimation, in the paper's terminology), this work by Tsou et al. serves more of an applicative validation of previous work over additional data sets than novel insights relevant to microdata stream privacy. For instance, theorems are provided to discuss and demonstrate the relationship between k-anonymity and ϵ-differential privacy [54]; however, this had already been established theoretically earlier in the literature [9], [55]. A primary value of this research is proving properties and guarantees of differential privacy over large data sets that include microdata streams in this systematic literature review scope.

2.2.28 CGM: An Enhanced Mechanism for Streaming Data Collection with Local Differential Privacy

Bao et al. consider in this work the tradeoff between privacy and utility for microdata streams with a temporal element when the differential is applied without consideration for 'autocorrelation', or the automatic correlations that can be inferred between event-based set-valued data in the data set [56]. Of note, naïvely applying an additive noise function as classical differential privacy would require can introduce an inordinate amount of noise that harms utility. This publication is another in a long line of papers in this era of the literature that attempts to refine the applicative processes to tune differential privacy for better privacy and utility tradeoffs for a specialized domain, the proposed method, correlated Gaussian mechanism (CGM) in local differential privacy.

The novel mechanism in CGM is the recognition that in microdata streams, trajectories are likely to repeat many times with sufficient precision, frequency of measurement, and a long enough period. For example, an office worker who commutes to work multiple days per week will establish a pattern that can harm event-level privacy. This work points out that previous work focusing on user-level privacy in microdata streams, such as PeGaSus [57], does not necessarily protect event-level privacy for them [56]. This work suggests that while combining some perturbation techniques can be helpful when orthogonal, specific microdata stream data privacy protections are still highly domain dependent without utility suffering unduly through a single, general approach.

2.2.29 Real-World Trajectory Sharing with Local Differential Privacy

Another novel refinement of differential privacy for spatiotemporal data, the n-gram approach proposed by Cunningham et al. here, is unique in its dynamic resolution adjustment for spatial data to preserve utility for two-dimensional spatial coordinates [58]. Primarily a partitioning optimization, the researchers note the unique properties of n-gram portioning, which preferentially preserves the spatiotemporal relationships between popular nodes on a trajectory graph rather than the relative frequency of visits to each, may be more attractive to health policy makers performing epidemiological analysis. However, while this mechanism provides improved utility, the researchers note a precipitous drop-off in privacy as evidenced by a decreasing nominal error with increasing values of ϵ. While much research asserts that values of ϵ ¡ 1 may be unsafe [59], this publication notes that such values are recommended as a tradeoff for the n-gram approach to provide sufficient utility. For this reason, the use cases for this application may be nuanced.

2.2.30 Anonymization of Network Traces Data through Condensation-Based Differential Privacy

Several works in the literature reviewed incorporate k-anonymity for clustering and differential privacy to apply additive noise to continuous attributes, including this publication [60]. Network traces, which can be considered a form of spatiotemporal microdata stream since they contain trajectories of sources and destinations and timestamps, are specially treated using a triplicate of permutation of discrete addresses, a clustering of port data, and Laplacian noise for timestamps. Utility in this research has a domain-specific measurement function: 'attack traffic' detection.

While differential privacy techniques are employed, only two specific types of attack traffic could be predicted from this method's unique combination of perturbations: volumetric attacks and uncharacteristic aggregate flows directed to known ports. Indeed, a nuanced approach is relevant specifically to network traces. The general applicability of this method is not generally applicable because the utility measurement function is domain-specific. The work is essential, however, because NetFlow metadata has been demonstrated to impair user privacy, even revealing users utilizing VPNs from the view of a network operator intermediary [61]. With alternative utility measurement functions, the specific triplicate treatment for this form of data may be reusable in other adjacent domains for network trace data outside of adversary detection.

2.2.31 Landmark Privacy: Configurable Differential Privacy Protection for Time Series

Katsomallos et al. explore a unique construction for clustering that they term 'landmark privacy', which they demonstrate experimentally for both traditional spatiotemporal data, in the form of location trajectories, and also for smart grid power consumption, which has similar dimensionality [62]. While this work does not explicitly cite Cunningham et

al.'s work on n-grams, it does refer to n-grams as an earlier theoretical construction and demonstrates some methodological similarity in approaches. Landmarks, in this case, are nodes in a directed graph of significant importance: shown as the only areas of interest that need appropriate privacy applied or that should be treated as especially sensitive and dropped out of the trajectory altogether.

Implementing an adaptive version of the method proved to be the least privacy and utility-harming outcome. The authors distinguish between user-level and event-level privacy, which is standard in this era of microdata stream differential privacy literature, but offer a technique better than user-level privacy but generally worse-performing than event-level privacy. Because this technique focuses on protecting the temporal component, the privacy budget is expended more strongly over the spatial dimensions. A fascinating insight in the discussion of this work is that when there is greater spatial distance between adjacent nodes in a trajectory, privacy is more negatively affected by the technique (and perhaps generally), as a longer directed 'travel' between two spatially distinct nodes may be more dangerous for identifying a particular user behavior. For example, a user who travels directly from Dallas, Texas, to Orlando, Florida, without intermediate stops may be much more distinctive than those making such a trip and regularly stopping for gas or breaks between nodes on a trajectory. This insight has potential applications for adversarial differential privacy use cases.

2.2.32 LDP-IDS: Local Differential Privacy for Infinite Data Streams

As previously established in the literature of this era, this paper also distinguishes between user-level and event privacy. It provides a framework for protecting ω-event privacy for microdata streams when they are also real-time streams of infinite length within the context of local differential privacy [63]. This refinement of a seminal work not selected by the search strategy of this systematic literature review is essential for this field by

Kellaris et al. That paper, in particular, defined the notion of ω-event privacy, which is a specific temporal protection for microdata streams "which protects any event sequence occurring within any window of w timestamps" [64]. This insight is notable for a few reasons: the body of knowledge about microdata streams should include relevant research into ω-event privacy, as much timestamped event-level data is also set-valued data where data subjects' timestamped events occur more than once per data subject. Separately, that paper is vital in recognizing the dangers of correlated and sequential timestamp data related to microdata streams.

This work continues Kellaris' work by addressing LDP and adaptive mechanisms. This quantitative and experimental work tests a variety of ϵ budget division schemes across four frameworks of adaptivity for synthetically created data [63]. Predictably, the value of window ω significantly affects the efficacy of the privacy budget and utility for an infinite series of time-window-protected data, as proven by this research. This intuition is essential for practical applications to consider when implementing differential privacy for microdata streams that contain temporal attributes to ensure the appropriate tradeoff is not only made for the ϵ privacy budget and the domain-specific utility function but a carefully chosen ω appropriate for both.

2.2.33 Genomic Data Sharing under Dependent Local Differential Privacy

Genomic data is not typically considered in the standard literature of microdata streams; however, it is a form of stream-based vector that is highly correlated. This work by Yilmaz et al. explores the correlations present in genomic data and the domain space that allows for inference attacks on the application of differential privacy. Because genomic data is highly probable for sets of 64 codon sequences characteristics of amino acids and stop-signals, additive noise may not only be detectable when applied but could be filtered out using error correction techniques when insufficient privacy budgets are applied [65].

The key contribution of this quantitative, experimental research is that noise may not be sufficient to use across a vector of long, highly correlated, low-range values. Instead, domain knowledge about permissible subsequences in the vector may be needed to construct unique probability distributions to apply noise in a manner that domain awareness does not subjugate.

While literature often considers microdata streams in a few archetypal forms: click-streams, location pings or user trajectories, or biometric signals, vectors are an example of a microdata stream that is horizontally correlated for the entry in addition to potential repeated presence in a database. In addition to the specialized treatment to preserve privacy per the budget, this research also contributes an improvement on "randomized response", often explicitly employed in local differential privacy to ensure plausible deniability in data that may be far more homogenous than a full population dataset.

2.2.34 Privacy Preservation for Trajectory Publication Based on Differential Privacy

A specialized differential privacy application, this paper identifies a gap in microdata stream research that trajectory data faces an increased risk of privacy harm with spatiotemporal data, including sensitive labels, such as annotations that leak information about location, meaning, or intent [66]. While a small number of papers were disqualified for eligibility for this systematic review because, upon further review after passing the eligibility selection process, they were included in the search strategy only because they mentioned streaming in a real-time data change process in graph theory research rather than pertain to microdata streams as defined by the scope, this paper bridges both domains.

Yao et al.'s approach is to use the transformation of microdata onto a graph and apply differential privacy to node and vertex weights, formed as an artifact of the construction of the graph, and then publish those records. The utility is measured as the Hausdorff

Distance, which measures the distance between two subsets in metric space [67]. Because Hausdorff Distance can be extended to account for three or more dimensions, the technique is generalizable for other forms of labeled data. The proof is provided and experimentally validated using location-based datasets.

2.2.35 On the Risks of Collecting Multidimensional Data Under Local Differential Privacy

Arcolezi et al. thoroughly analyze typical LDP implementations in adversarial simulations in this paper. The researchers note that the body of knowledge for differential privacy, and in particular LDP, is filled with incremental refinements that show marginal improvements in the privacy-utility tradeoff; however, they also demonstrate the dangers of highly correlated microdata streams that allow for reidentification when ω-event privacy can be compromised [68]. Many other papers have demonstrated the strength of the approach through theorem proving; however, this paper produces both an adversarial approach and countermeasures. Practical strategies for reidentification attacks provide methods for testing incremental improvements that cannot always account for external correlation or pattern recognition at scale in microdata streams.

2.3 Risk of Study Biases

As the body of knowledge for differential privacy in microdata streams develops from 2009 to 2023, the use of private and synthetic datasets incidentally decreases, and so does the frequency of positivity utility findings. This observation does not necessarily imply that private or synthetic datasets are subject to selection or reporting biases. However, such biases may exist among the whole body of knowledge as the literature of the mid-2010s was focused primarily on improving utility in the context of the centralized differential privacy model. As the field has developed, local differential privacy (LDP) research is

more frequent for the same search strategy over time, and both because the LDP utility baselines approach $\sqrt{N}$ utility as compared to centralized designs, utility alone is an important consideration but affected by architectural and multivariant parameter choices that transcend earlier 'privacy vs. utility' efforts that attempted to push the frontier to improve both outcomes of a two-dimensional problem.

However, it is notable that much of the work selected by this systematic review fails to directly build upon previous research by citation when the same data sets are used. Instead, the literature displays a plethora of different datasets. Incongruent experiments over varying datasets frustrate attempts to compare the development of differential privacy for microdata streams since the utility function for differential privacy is domain-specific and thus will vary by the dataset chosen. Furthermore, even for works that develop the field and analyze the same datasets, in addition to the observed trend of not citing or building upon claims in the reviewed works, each redefines utility functions for their research aims. Indeed, some research designs include different experimental setups that require novel utility functions to accommodate their research questions. However, the lack of generalized forms that allow related research to be comparable can encourage researchers to 'talk past one another' in their contributions. The tendency to select particular experimental datasets or utility function definitions may indicate the presence of sampling or ascertainment bias.

2.4 Discussion

Location data is generally a good illustration for microdata streams, as it often includes temporal data (in absolute terms or delta offsets) containing three or more dimensions highly correlated in latitude, longitude, altitude, and sometimes velocity. These are characteristics that lend themselves to three specific types of attacks not generally present in user data:

1. **Domain knowledge attacks:** Geolocation data, for instance, is bounded to the earth's surface features for spatial coordinates. For this reason, except in exceptional cases that involve short-term vehicular travel, such as airplanes, subways, or submersibles, or manufactured structures, such as skyscrapers, the possible space for presence approaches an irregular ellipsoid and not the product of all the ranges of each spatial dimension. Beyond the reduction in space, there are predictable patterns and practical limits of acceleration and altitude that allow some noise injected by user-level or global differential privacy approaches to be identified as such and removed with a high degree of confidence.

2. **Environmental condition inferences:** A knowledge attack specific to location data, awareness of environmental conditions can be applied as a weight to adversarial approaches to guide inferences that deidentify or correlate events across users. If a significant highway collapses and is a standard route for a user, changes in behavior caused by this environmental condition can be attributed to a subset of users most likely to be affected by the change. Observing changes in weather patterns, natural disasters, or congestive traffic incidents could allow pseudonymous identifiers in event data to be better estimated in a manner that harms privacy if not reidentify users fully.

3. **Correlated sets:** Users who cohabitate are likely correlated in other ways throughout a microdata stream: they may travel together on an annual vacation or a weekly grocery store trip. Depending on the fidelity of the temporal data in a location-based data set, both in accuracy between reported and actual location and the time between location updates, individual personal relationships can be inferred by the apparent joining of microdata streams for durations. Not only can correlation be established between individuals, but the nature of their activities can also be inferred when placing assumptions around acceleration data and overlaying the location of

known landmarks within the stream data. The ability of an adversary to establish correlations between users in set-valued data may be improved by more data points collected, requiring ϵ to scale proportionately to the length of the population of events or the query result.

These problems exist both at the points of collection and the points of analysis [69], and combined with the complexity that inference and correlation are domain-specific problems, general approaches for microdata streams may not be readily available that provide sufficient utility for each. For instance, random response methods can cause an exponential decrease in privacy with repeated collection of indoor location positioning data [69], [70]. However, these problems do not necessarily manifest with local differential privacy being applied, although an improved outcome is highly schema and implementation-dependent.

An inherent limitation of this systematic review approach is that a single researcher performed this methodology. Any researcher will likely have inherent biases that only collaboration can address. To minimize the potential for intrinsic bias given the resource constraint, the author recorded and published lab notes and earlier versions of this manuscript to peers for comment to receive feedback. In addition, a two-stage eligibility screening process was performed to select publications from the search strategy results. The works screened out first by the cursory review are enumerated in the 'Works Screened by Selection Criteria' appendix, and the secondary list of publications screened out by subsequent review is enumerated by the 'Works Screened by Manual Review'. The author shared notes for the rationale for each screening decision with peers for review before this publication to support an open and collaborative research effort where feedback was available.

This chronological systematic review span was extensive, ranging from 2009 to 2023. In those fourteen years, powerful smartphones became ubiquitous, ushering in an age of privacy concerns as spyware, stalkerware, and data brokers encroach on personal anonymity. As such, the importance of privacy preservation in mobile computing environments has

increased in society and influenced the development of differential privacy in fundamental ways. Local differential privacy, a model that treats centralized data collection authorities as untrusted, has seen significant development generally in differential privacy and related explicitly to microdata streams. The development of related literature also shows the increased frequency of research into crowdsensing applications, where firms use peer-to-peer mobile data transfers to track individuals, as in the case of Apple AirTag and their contacts, in the case of epidemiological contact-tracing applications.

Unlike static, demographic data published infrequently by centralized authorities, differential privacy is simultaneously considered the 'gold standard' of data privacy. It is evolving to address myriad deployment modes in environments that are always-on, real-time, and rich in highly contextual metadata. As potentially every application developer can collect private data from mobile devices and precipitate privacy harms, not just carriers, device manufacturers, or mobile operating system developers, robust differential privacy tools that protect microdata streams are essential to develop and adopt. Even as of 2023, few widely deployed toolkits enable or require data processors to safeguard information with this proven mechanism. As the body of knowledge develops, there are opportunities for the practice and related policies to support adoption across various verticals, including but not limited to mobile computing, IoT, and edge computing.

2.5 Conclusion

As examined in the limited scope of this chronological, systematic literature review, the research field of differential privacy has developed significantly since 2009. The review demonstrates the shifting focus in the field and its broad application to developing areas of computer science. Whereas earlier work focused on refining additive noise mechanisms to maximize utility and privacy outcomes, widening application necessarily segmented research to define domain-specific utility functions and address unique problems in each,

from trajectories to genomic data. This refined focus demonstrates the versatility of differential privacy generally but also highlights the difficulty of addressing the challenges inherent in microdata streams in each. Notably, just as there is no singular optimal utility-privacy tradeoff across differentiated data sources, there is also no apparent uniform approach for minimizing knowledge, inference, or correlation attacks in microdata for each. The body of knowledge reflects the current state of streaming microdata privacy: new, open problems are still identified and receiving significant research interest. These avenues hold promise for the development of knowledge itself, and many represent real-world opportunities to minimize data privacy harms in an increasingly interconnected, real-time exchange of sensitive data in microdata streams.

Chapter 3

Methodology

This chapter aims to introduce and detail the methodology for technical action research (TAR) study regarding the limits of ϵ-differential privacy in preserving privacy guarantees when microdata series are cross-correlated. This approach allowed for the development of a research artifact that identified related microdata, such as the geolocation movements or heartbeat biometric data of hospital patients, in large data sets and allowed for the iterative, empirical analysis of the efficacy of additive noise functions in preserving privacy. The applicability of technical action research and a postpositivist approach for this study are discussed in-depth in this chapter. The research plan, including the methodology, research context, problem, research and inference design and validation, and analysis plan, are the primary components of this chapter.

3.1 Methodology Selection

ϵ-Differential privacy is mathematically defined as the probability that a given element (where an element is a datum or a subset) is or is not present in a privacy-preserving transform of that data set within a given privacy loss budget. To answer the first research question, how the number of multiple, related microdata attributes in a data set improves the ability for an artifact to make inferences that correlate them, one needs both an artifact that can make such inferences and a sensitivity analysis to establish the limits of efficacy for the artifact given changes in related microdata attributes. To answer the second research question, an artifact's dual-engineering cycle of iterative development to

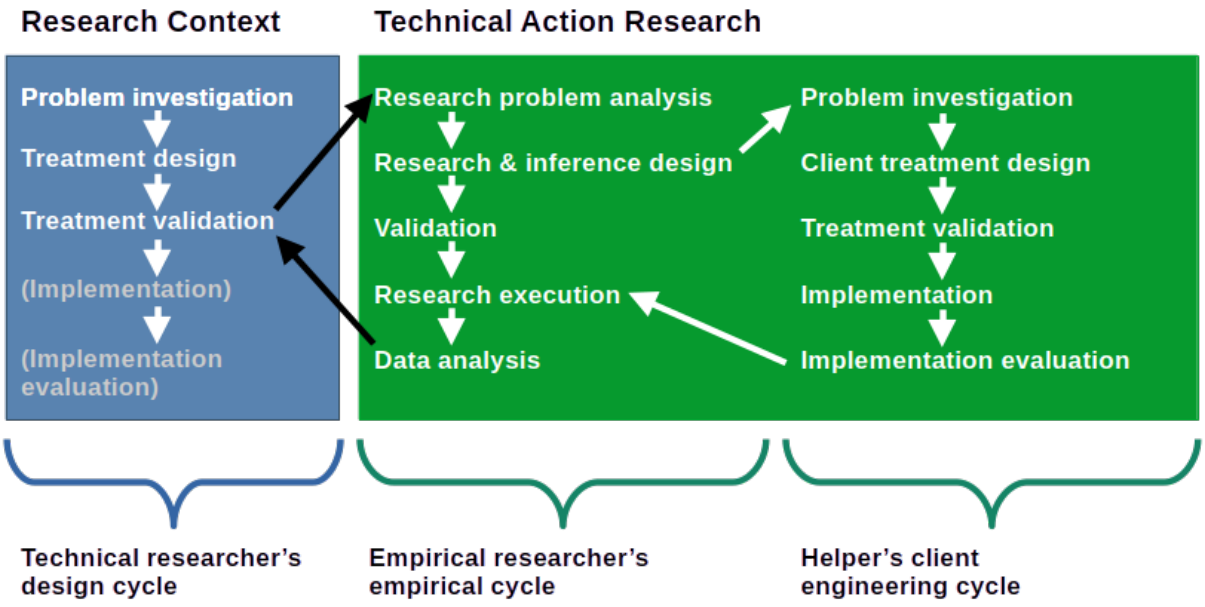


Figure 3.1: Technical action research methodology diagram [13]

solve this problem for a client in a real-world problem space is appropriate and necessary. Technical action research is well-suited to empirically validating an experimental artifact [13]. Unlike multimethod and mixed-method approaches, TAR provides for an iterative cycle of design and validation rather than more traditional, sequential approaches.

The research question has two distinct dimensions: Can an experimental artifact detect cross-correlation of related microdata series in a data set with ϵ-differential privacy applied, and under what circumstances can one accurately detect them? The first dimension represents a knowledge question that can be answered by a program, algorithm, or applied method. Design science approaches are generally suited for this dimension, as "design science iterates over solving design problems and answering knowledge questions" [13]. However, the second dimension, 'under what circumstances', requires an experimental and empirical approach, which is a form of studying the "utility of an intervention" or "understanding the best predictors of outcomes" [19]. Because the research experiments need to validate both the robustness of the ϵ-differential treatment against the artifact's efficacy for establishing limits of the treatment guarantees in specific microdata contexts,

the iterative artifact refinement cycle characteristic of technical action research is the best methodological fit for this research question. Furthermore, TAR is well-suited to validating an artifact in a real-world context, and since ϵ-differential privacy toolkits, such as OpenDP, are available and becoming more widely available, ensuring the methods they employ are used with appropriate contexts is vital to successful implementations that preserve privacy within an expected privacy loss budget.

3.2 Design Cycle

3.2.1 Research Context

3.2.1.1 Knowledge Goal

Both dimensions of the theory that ϵ-differential privacy guarantees may be unachievable with certain types of microdata cross-correlations present in data streams are researchable with a postpositivist approach to empirically examine the relationship among numerical variables. Conversely, while privacy-enhancing technologies and privacy harms relate to human societal problems, the specific theory and knowledge questions of this research are unrelated to "the meaning individuals or groups ascribe to a social or human problem" [19] and so a postpositivist approach is not suited for qualitative research. This technical action research methodology uses a quantitative and postpositivist approach, which allows for an empirical cycle, similar to a single-case mechanism, to iteratively validate and improve upon an artifact using a client engineering cycle. Because this study is quantitative, a postpositivist approach is fitting.

It is given that the mathematical guarantees of the ϵ-differential privacy treatment are sound [11]. However, the knowledge question this research seeks to answer is: Under what circumstances is this true for data streams where there are M many different, related records belonging to N smaller (M>N) data subjects, and for what privacy loss budgets?

Given that some seminal literature on this topic states this guarantee should allow one to incur almost no quantifiable risk by joining a data asset, research the conditions under which a marginal new data subject may imperil other data subjects within the same research context. This outcome may be well-validated and understood for single-record and single-data subject use cases of the differential privacy treatment, where adding a data subject may add many additional microdata elements. These use cases are internally correlated and cross-correlated with other data subjects, such as those with familial, fraternal, or work-related demographic or behavioral relationships the knowledge goal is then to understand the conditions and parameters of this treatment required to accommodate this type of underlying data set.

3.2.1.2 Improvement Goal

Once this frontier is identified, the improvement goal is to determine how to impair the ability of the experimental artifact to identify it subsequently through different applications of the differential privacy transformation. An iterative validation and evaluation cycle will be required to test various approaches. These approaches could include changing transformation parameters, such as increasing the privacy loss budget, experimenting with alternative additive noise mechanisms, such as trading out a Laplace mechanism for a Gaussian mechanism or applying other limitations to the data set, such as dropping out microdata elements too-heavily clustered on a dimension, such as time, for a given data subject.

3.3 Technical Action Research Empirical Cycle

3.3.1 Problem Analysis

3.3.1.1 Conceptual Framework

The primary constructs of this research are statistical structures, which are "phenomena that can be described by variables, [with values having] a probability distribution over the set of possible phenomena" [13]. Specifically, this research focuses on microdata streams cross-correlated with data subjects. In the illustrative case of mobile device geolocation data, the association of timestamped ping in a sample is related to the probability that all other future-timestamped pings relate to the previous one. Various characteristics of a ping, such as the latitudinal and longitudinal position, velocity, and time-delta, influence the probability that other pings future-dated may represent the same data subject.

Composition, cardinality, and process constructs, such as environmental factors, also influence the probability; for instance, if a ping's position is known to be on a park trail or busy city street, it is unlikely the relative change in velocity to nearby candidate pings would happen at high rates of relative velocity change or a high absolute speed. Conversely, a ping with a high velocity on a known interstate freeway may rapidly fall to zero in a subsequent ping but is unlikely to rapidly drop to a negative velocity (going in the reverse direction). Relatedly, one-way graph junctures (such as one-way streets) are unlikely to be violated, and commercial or residential buildings will unlikely experience high-speed transits.

Event-related constructs are significant influences on the probability assignment as well. Intuitive patterns one might expect in geolocation data, such as a nightly return to a home and a predictable return to a place of work, worship, or commerce, may help disambiguate data points recorded with similar values. By building behavioral profiles into the artifact's selection of probable ping associations, these 'centers of gravity' for

individuals may significantly improve associative accuracy.

Data streams need not only to be considered in terms of anonymized timestamped geolocations but could be data points of human heart rates or other biometric data. Similar constructs would apply to these differing contexts, such as a probability distribution that conforms to the biography of the data subject, such as their height, weight, sex, and medical history. Other context-dependent associations may be encoded in an artifact, such as a consideration that sleeping heart rates are lower, which may be difficult to generalize for other contexts like geolocation data. This difficulty is a notable callout for the following discussion on treatment design, as an artifact that can handle generalized cases with an unknown number and type of data elements may be challenging to build without employing machine learning techniques. However, by creating a context-specific artifact, such as one attuned to geolocation pings, more relevant features may be predictably present or calculable for either heuristic or machine-learning artifact designs.

In summary, the conceptual framework entails a "set of sets" of structured microdata belonging to fewer data subjects. Each subject set within the data set has several continuously related records representing a data stream of elements about a data subject over time. This data stream may either be one-dimensional (such as a heart rate or absolute speed) or multi-dimensional (such as a geolocation stream with latitude, longitudinal, and altitude values) and additionally includes a stable anonymous identifier to distinguish related microdata elements belonging to the same data subject. A client who possesses this data in a raw and precise form, called the data provider client, wishes to share data with a data consumer client in a manner that preserves the identity of data subjects and maximizes the utility for the data consumer client, thus its economic value. These are problem concepts. The conceptual framework contains specialized concepts related to privacy violation harms [14], such as surveillance, secondary use, decisional interference, and exposure.

3.3.1.2 Knowledge Questions

Because technical action research must solve a problem for the client, in this case, both the data provider client and the data consumer client, of primary concern is how the former can apply the ϵ-differential privacy treatment to highly correlated data streams while preserving the privacy loss budget and maximizing the non-private information knowable from a transformed data set with the treatment applied. It is not enough to know the treatment can be used; it is essential to understand the limits of the treatment and, importantly, how to apply it. Specifically:

1. What are the characteristics of microdata streams that most erode the privacy guarantees of ϵ-differential privacy for the experimental artifact tasks by thwarting these protections? This question applies both to the limits of the treatment and its manner of application.

2. Can clients reliably apply the developed treatments in industry settings?

3. Is the treatment externally valid? Can the treatment be applied to other microdata stream contexts with different dimensionality, variances, and populations and yield the same privacy protections?

4. Can clients use the experimental artifact to validate that they have applied the technique correctly?

3.3.1.3 Population

The population of data provider clients for which this technique is intended is all that have large data sets of microdata, which, if exposed, could cause privacy harm as enumerated in Solove's taxonomy of privacy harms and related records for the same data subject with a stable anonymous identifier. Additionally, these data provider clients must exhibit a need to allow internal agents or affiliates to analyze this data or a need to share

this data with external parties. This definition would include most data processors that transmit or store biographical and behavioral information, including medical providers, retail establishments, telecommunications providers, and increasingly connected vehicles: automobile manufacturers and the related ecosystem of vehicle support and maintenance services. Accordingly, the population of data consumer clients, including those who desire access to this microdata, do not have the sophistication to perform their own privacy transformations or cannot be trusted to do so in a verifiable and effective manner.

3.3.2 Design and Validation

3.3.2.1 Client Selection

Many financial technology companies have rich data sets that could enable privacy harm without proper use and access controls that they wish to monetize through pattern recognition, classification, and predictive analytics. This monetization need not be the wholesale reselling of personal information but the generation of personalized approaches for service delivery or advanced fraud detection. Depending on the jurisdiction of the data subjects represented in these data sets, both the provider and consumer clients interacting with these data sets face legal, compliance, and reputational risks related to the privacy harms they may subsequently cause. Few have implemented differential privacy techniques and rely instead on anonymization and sampling techniques, which have been shown insufficient to protect both protected health information and nonpublic personal information.

While 'fintechs' are not the only clients who can benefit from this technical action research, they are an ideal selection for this research because they possess the required data and have the requisite problem concepts noted in the conceptual framework. Additionally, the researcher has several existing professional relationships with financial technology companies, such as payment processors and digital banking companies, that he anticipates

will be able to overcome the gatekeepers and other challenges an unsolicited research proposal may encounter. Because U.S. fintechs often possess several types of microdata streams in great volumes across a significant portion of the U.S. population relevant to the knowledge questions, namely geolocation data and transactional purchase histories in a highly structured and labeled format, the researcher anticipates the inferences drawn from both the differential privacy treatment and experimental artifact would generally apply to other U.S. clients. While cultural variances in behavior are typically observable in these data sets, because this technical action research focuses on specific descriptive statistics broadly applicable to all such data subjects, the researcher anticipates these inferences are more generally applicable outside of the fintechs and outside of U.S.-based clients and would be repeatable for samples with similar demographic characteristics.

Critically, research into privacy harms must not create privacy harm if it is ethically performed. United States-based fintechs and the financial institutions they serve are subject to many regulatory regimes, including the Gramm–Leach–Bliley Act (GLBA). This act contains The Financial Privacy Rule, which places requirements for consumer privacy notices that detail how personal information covered by GBLA will be used and shared. For this reason, minimally, a willing fintech client that also has an interested financial institution client that also provides for this technical action research in its communicated institutional privacy policy is a prerequisite to perform ethical research. In another way, consent from the fintech, financial institution, and ultimately the consumer, as provided for in an accepted privacy notice, must be demonstrated before interacting with their anonymized data. Limiting client selection in this manner will require no additional data subject notification or consent.

3.3.2.2 Sampling

In this research project, at least two client cycles will be performed for data sets provided by separate financial institutions. For both clients, two different data sets will be

researched, one using multi-dimensional, continuous data grounded by a timestamp and anonymized identifier (e.g., Timestamp, ID, Latitude, Longitude, Altitude) and another using a single categorical dimension grounded by the same (e.g., Timestamp, ID, Merchant Address). These samples will contain a complete set of microdata for data subjects in a 90-day window to provide sufficient context for any weekly and monthly periodic behavioral patterns to emerge. Data subjects from the sampled client will be the entire population of microdata, except for those subjects that were not present in the data set by the start of the time window, those that ended their relationship with the financial institution before the end of the time window, and those that rescind their relevant consent for the use of their data any time during or after the window until the end of the data analysis activities.

Following, multiple data sets are required from each client to allow for the design and validation of the experimental artifact:

1. A file of structure microdata, normalizable into the schemas mentioned above, AND

2. A key-file that relates private demographic data to anonymize identifiers in the microdata file, such as the actual physical address of the data subject, to validate that the artifact accurately associates microdata before and (potentially) after ϵ-differential privacy is applied.

Notably, there are limits to analogic inference this representative sampling creates. Users of financial technology services are not equally stratified by product category or data subject demographic. For example, 82% of Americans use digital payments [71], but only 76% use digital banking [72]. There are significantly different use patterns in the digital banking vertical alone: In May 2021, 27% of seniors 76 years of age or older used this financial technology, but 95% of Gen Z (18-25) did [73]. Moreover, a significant number of Americans, 63 million, are considered "unbanked" or "underbanked", meaning they have no or insignificant relationships with traditional financial institutions [74], excluding them

from this sampling. While the researcher does not anticipate this sampling condition will impair the efficacy of the treatment when applied to microdata streams of the unbanked or underbanked, these experiments alone cannot independently validate this.

3.3.2.3 Treatment Design

In this research project, the data provider client's problem was that they wanted to provide access to data and apply differential privacy but ensure the application appropriately accommodates the privacy budget when many microdata elements for the same data subject are repeatedly present. This cycle must maximize the utility for the data provider and the data consumer client, requiring a customized approach. The respective clients will determine the value with competing aims (providers want to limit liability, and consumers want to maximize information gain), which can be measured objectively in the context of a single client-client relationship as the agreed upon per record price before and after the treatment.

The treatment will be two-fold in iterative research execution cycles:

1. **Unmask:** An experimental research artifact, in the form of a software tool, will be developed that uses heuristic and probabilistic approaches to attempt reidentification of related microdata both (1) when the standard anonymous identifiers are stripped to determine the ability to associate microdata on other correlated dimensions of microdata and (2) when the data set anonymous identifier is present, leveraging cross-correlation characteristics to reassociate them to the identity in the associated key-file.

2. **Mask:** A treatment, potentially before the application of differential privacy using OpenDP, potentially after, or potentially at both points in the workflow to attempt to thwart the ability of the experimental research artifact to reassociate individual data subject-stripped microdata or to reidentify microdata sets for the same subject to their identity in the key-file.

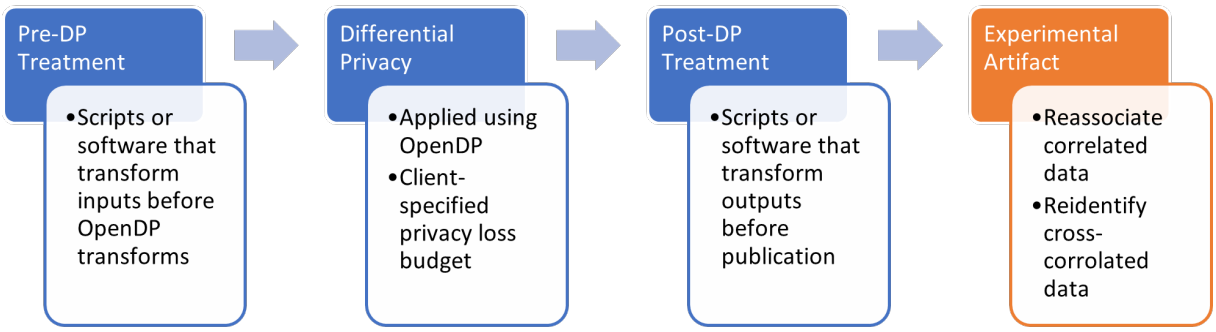


Figure 3.2: Mask (blue) and Unmask (orange) empirical cycle of the iterative TAR methodology

This cycle progressively refines the Pre-DP and Post-DP treatments, referred to as the "DP Streaming Enhancement", using an iterative, adversarial approach. The first object of study is the raw data set that is transformed with the DP Stream Enhancement treatment in conjunction with a differential privacy transform in the 'Mask' phase. The second object of study is the output, which the experimental artifact assesses to determine the relative strength of the DP Streaming Enhancement treatment. This second object of study is not the input back into the process; instead, the empirical cycle is the refinement of both the treatment and the artifact in a 'cat and mouse' development.

Provided the empirical cycle sufficiently answers the research question, the client engineering cycle can initiate. It involves both the data provider and the data consumer client validating that the experimental artifact meets their requirements. Of critical concern in this cycle, which should have shown in the empirical cycle that privacy is preserved per the provider client's privacy loss budget, is that the data consumer client can realize sufficient utility from the output to substantiate a mutually beneficial economic value for both clients. For example, if the DP Streaming Enhancement reduces the number of microdata elements or the resolution of the attributes such that it is not helpful for the data consumer client to draw necessary insights, then it may be of low value or so devalued that it is not demanded from the provider.

The validity of the DP Streaming Enhancement treatment will be highly dependent

on the unknown, unstated, or incompletely stated needs of the data consumer client. One data provider client may serve multiple clients in the same differentially-private data set. For this reason, this treatment design must carefully consider the magnitude of impact in pre-treatment and post-treatment data sets because validation for one consumer client may not be a generalizable inference for other clients with differing needs. In an extreme example, the pre-DP streaming enhancement could significantly reduce the size of the post-DP treatment published data set. While this might preserve privacy properties and be sufficient for one data consumer client, it may be unacceptable for others who depend on adequate sample sizes to draw inferences from the provider's data set.

By measuring the success of the experimental artifact to reassociate and reidentify stream-based microdata, the DP Streaming Enhancement mechanisms for conditioning or transforming OpenDP inputs and outputs become the deliverable to the data provider client as part of this technical action research. Provided with these mechanisms, the data provider client can, on their own, use them to harden a published data set before a data consumer client accesses it. Separately, with the experimental artifact in hand, they can validate that the DP Streaming Enhancement treatment resulting from this research continues to uphold the privacy loss budget, particularly as the characteristics of microdata may evolve over the lifetime of a system collecting and storing it.

The architecture and implementation of the DP Streaming Enhancement treatment must be specified and approved by the client. For example, the use of esoteric or specialized statistical tools standard in academia may not be readily available or usable by industry practitioners seeking to harden their microdata streams, so the DP Streaming Enhancement treatment cannot depend on them in the final client deliverable. Similarly, if the DP Streaming Enhancement uses programming languages or operating environments unfamiliar to the client's technicians, it is unlikely they will be adopted or repeatably and successfully used, potentially leading to privacy harm through this 'design fault'.

3.3.2.4 Measurement Design

A core tenant of differential privacy is that private data is immune to post-processing, that is, "a data analyst, without additional knowledge about the private database, cannot compute a function of the output... [to] make it less differentially private" [11]. This facet is what the experimental artifact seeks to do by leveraging weaknesses in the characteristics of microdata streams with a high degree of associative correlation and cross-correlation. As further noted by Dwork and Roth, "differential privacy is not a binary concept, and has a measure of privacy loss", mainly due to its use of additive noise mechanisms that draw from probability distributions. Because this TAR design is empirical and quantitative in nature, the critical measurement is the dependent variable for the probability that the experimental artifact is more statistically successful than random chance at reassociating and reidentifying differentially private microdata streams with no or specific DP Streaming Enhancement treatments applied.

Given this, measurement instruments include standard statistical packages, such as SPSS, of data sets processed with the DP Streaming Enhancement treatment and the experimental artifact. Moreover, with a key-file (as mentioned in the Sampling subsection above) that contains additional structured demographic metadata, such as date of birth (which can be transformed into a categorical 'generation'), additional independent variables can allow for subsampling (replication) from the sample data provider client with randomized selections across these categories to rule out demographic variances from the measurement. Notably, TAR cannot support causal inferences, but in this case, measurement using replication is not intended to test or suggest a cause-and-effect relationship; instead, construct validity can be demonstrated with this approach.

3.4 Summary

This methodology chapter outlined the research method utilized to answer the research questions. This chapter detailed the research context, including the knowledge and improvement goals necessary for technical action research, the research problem and knowledge questions, and how a client would be engaged and enhanced by the deliverables of this research. Care was taken through the design phases of this methodology to research the limits of privacy in microdata sets without creating undue ethical violations or further privacy harm. By establishing precise inference design characteristics and considerations, the results in Chapter 4 demonstrate adherence to this methodology and illuminate the results and subsequent inferences the researcher can draw from them.

Chapter 4

System Design

4.1 Methodology and Design Alignment

As outlined in Chapter 3, technical action research (TAR) requires three cycles that culminate in a treatment designed and validated empirically in a research setting that solves a real-world client's problem, as illustrated below in Figure 4.1. The treatment design must first and foremost align with the research context and goals, then pass empirical validation, and finally, client treatment validation. ϵ-Differential privacy (DP) is mathematically defined as the probability that a given element (where an element is a datum or a subset) is or is not present in a privacy-preserving transform of that data set within a given privacy loss budget. Given the research context of differential privacy, as with much computer science or technical privacy research, validation steps in this field are well-supported by quantitative analysis and traditional statistical validation methods.

The results of the empirical cycle must support the research questions outlined in Chapter 1 and the methodological requirements of TAR. TAR requires an explicit design for the descriptive, abductive, and analogic inferences that drive the design and implementation of the treatment. As it relates to the design of these three forms of inferences applicable to TAR, the system's design is outlined, followed by a proposed design of the treatment itself and the analytical framework that will be used for validation.

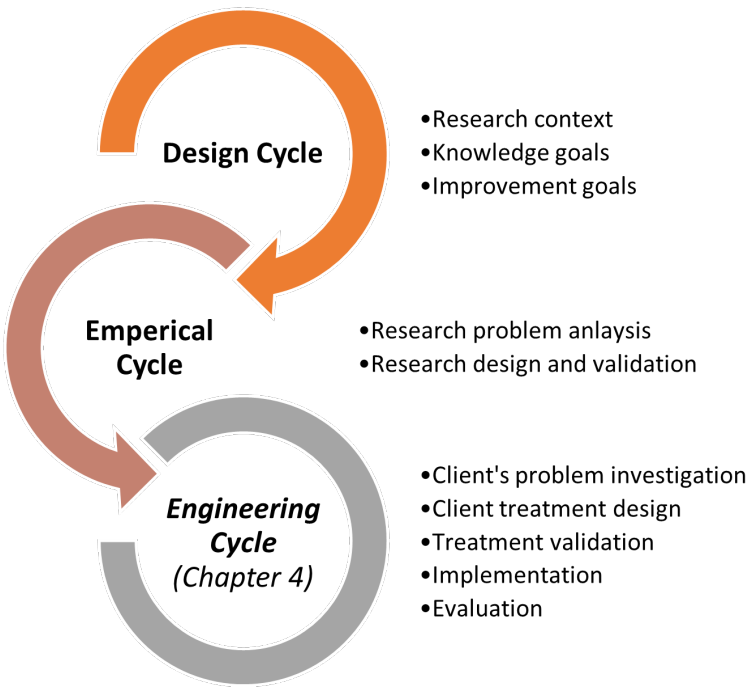


Figure 4.1: Technical action research methodology diagram with chapter mappings

4.2 Descriptive Inference Design

The DP Streaming Enhancement treatment will be observed and described in terms of marginal changes in the privacy loss, as defined by the formal, algorithmic definition [11] of differential privacy, relative to whether or not the treatment was applied, but when the experimental artifact is always used to attempt to increase privacy loss, given a constant target privacy loss budget (ϵ) and a constant target accuracy. Dwork & Roth define privacy loss in differential privacy formally as[11, p. 18]:

$$= ln\left(\frac{Pr[M(x) = \xi]}{Pr[M(y) = \xi]}\right) \tag{4.1}$$

In the preceding, this privacy loss is the relative likelihood that a private database (x) and an alternative private database (y), which differ by a single data subject (which in this research case might be more than on microdata element in a data stream) where a mechanism M applied (discussed in the next paragraph), are observed in the same

output database with differential privacy applied (ξ). The absolute value of this output is bounded by ϵ and has a probability of at least 1. (Or, for relaxed, approximate definitions of differential privacy that use parameter δ, this has a probability of at least 1-δ) [11], [75].

Given this, descriptive inferences will first be drawn based on the Standard Means Difference (SMD) statistical test across two probability distributions: one in which the mechanism M_1 includes the application of the experimental artifact (ostensibly which can reassociate or reidentify some of the microdata elements) and the other in which the mechanism M_2 does not. If these two distributions are statistically dissimilar, we infer that the experimental artifact successfully reassociated or reidentified microdata streams in a manner that harms differential privacy guarantees for the streaming case.

Subsequently, by running a second SMD across different probability distributions, M_1 from above and M_3, a mechanism that includes *both* the application of the experimental artifact and the DP Streaming Enhancement Treatment. Statistical dissimilarity infers privacy is significantly enhanced. In the best possible case, the dissimilarity between M_1 and M_2 that is corroborated by a third SMD showing similarity between M_2 and M_3 would infer that the experimental artifact substantially harms privacy and that the DP Streaming Enhancement Treatment substantially restores it to a pre-artifact level of privacy loss. Ideally, the research finds $M_1 \not\sim M_2$, $M_1 \not\sim M_3$, and $M_2 \sim M_3$ through SMD, which infers that both the treatment and the artifact are effective in protecting and validating this protection for microdata streams, respectively.

4.3 Abductive Inference Design

Because this technical action research is based on a treatment and an experimental artifact that produces empirical data analyzed through standard statistical approaches, discrete outcomes are expected: either the null hypothesis of each Strictly Standardized Mean

Difference (SSMD) test is rejected. Inferences are generated under the auspices of general probability theory with a frequentist interpretation. Because this technical action research does not depend on direct human interactions or interventions and is not a measurement of attitude or other qualitative measures, the inferences are unlikely to be affected by data subject biases, except to the extent that there may be sampling influences.

Privacy is a difficult concept for the public to define, and as interpretations vary significantly among individuals, individual data subjects may exhibit different behaviors or use privacy-enhancing technologies that impact specific data subjects' streams in microdata samples. For instance, geolocation data may have a lower resolution or incidence rate among those who use VPNs, turn off GPS sensors, or use technology intended to provide incorrect data. Random samples that include data subjects who exhibit these behaviors may impair the ability of the experimental artifact to reassociate or reidentify data.

Because the client selection and sampling methods will not involve data subject awareness and will operate on historical data, the researcher expects no regressions from data subjects or clients. Neither clients nor researchers will receive compensation or any substantial non-monetary benefit, so no effects are anticipated on the client cycle of this TAR. The data provider client, a fintech, and their downstream client, a U.S. financial institution, may delay, pause, or terminate their participation at any time. In addition, the client may demand immediate destruction of any data during the research activity. This event would interrupt the client cycle and could require the selection of an alternative with different data subjects or microdata stream characteristics. Such changes may trivially change the treatment designs. Still, they could substantially alter the design of the experimental artifact, which could have domain-specific heuristics encoded into it that are client-specific. Such changes would require a restart of the empirical and client helper cycles to ensure inferences drawn from any of the M_1, M_2, or M_3 mechanisms are valid and comparable. As data analysis and research execution operate on offline data sets provided by the client, the DP Streaming Enhancement treatment development, the

experimental artifact, and data analysis activities, have no anticipated effects or influences on the client.

The dual cycles of this technical action research will be scaled up first from contrived research lab sample data sets to validate client data schemas and requests and the data processing pipeline of the DP Streaming Enhancement treatment, the experimental artifact, and the statistical testing tools used for SSMD. The architectural model may require specialized transformers to be built to translate and normalize data provider client data sets into this processing pipeline. Provided the microdata streams are internally consistent for data types and bounding (e.g., numeric fields can be parsed into numeric values, and latitudes are within the range of valid and practical latitudes), the researcher expects that the architectural model for the data processing pipeline that supports the treatment and the artifact shall align to real-world use cases.

Notably, the data provider client must understand the possible inferences this research will make and how they may or may not benefit the client. In the best case, the client may receive a working DP Streaming Enhancement treatment and experimental artifact for optional treatment validation, which they can immediately implement in their environment. In the worst, unlikely case, neither the treatment nor the experimental artifact is practically or provably effective. A less desirable but more probable outcome is that a treatment is developed, but the client lacks the resources to achieve the desired effect. For this reason, collaboration with the client's technicians is vital in the client engineering cycle to ensure a deliverable is provided that has the greatest chance for adoption into the client's operating environment.

4.4 Analogic Inference Design

The objective of this technical action research is, first and foremost, to create a generalizable approach for treating a dataset of streaming microdata, either with preprocessing

or post-processing methods, to resist attempts to reassociate or reidentify microdata elements once they have ϵ-differential privacy applied. Secondly, this research aims to produce an experimental artifact that validates the success of the treatments, as described in the measurement design above. While the treatment should be generally applicable and practical for time-series, data-subject-grouped data across dimensions, the experimental artifact may not be so flexible for microdata sets.

For example, with heuristic approaches for reassociating or reidentifying data, domain knowledge of the specific microdata attributes may be helpful in reassociation or reidentification. For instance, a vector of floating-point numbers representing geolocation has specific, predictable characteristics. For example, the bounds of these values are known. Their moment changes are also bounded: speeds cannot exceed the speed of light and are unlikely to go faster than an airplane, for instance, and they are unlikely to suddenly reverse direction multiple times over a brief period given the physical laws of inertia and practical life patterns of data subjects. However, any clever heuristics encoded into the experimental artifact will not apply. They could render false positive or negative results if applied to a vector of floating-point numbers representing other values, like temperature, respiratory rate, and pulse.

The client, a financial technology firm, satisfies the population predicate. As recorded by geolocations, the fundamental nature of the human movement is unlikely to vary by the selection bias that underbanked or unbanked individuals may not be represented in the population. However, care must be taken not to overgeneralize findings based on purchasing behavior a client may share for this research, as the use of payment instruments the client reports on varies by data subject age, income, and macroeconomic conditions over time [76]. External validation of the treatment or the experimental artifact, as applied to geolocation data from fintech samples, can be obtained from other contexts, such as commercial data sets from location data brokers. However, ethical and privacy issues may exist when performing research on these data sets, depending on the conditions

of the microdata notice, consent, and use as aggregated by the broker.

Representative sampling from client data sets will use random sampling techniques repeated with subsampling (replication) at the data subject level. Because there are potentially many records relating to the same data subject in a microdata stream, sampling will be repeated on alternative groups of data subjects and all their associated microdata. Sampling methods will not independently select random microdata records in a manner that could truncate the related records for a single data subject, as the purpose of this research is to draw inferences from the ability to reassociate or reidentify correlated and cross-correlated microdata to their data subjects, not to infer data subjects from unlabeled microdata.

4.5 Component Design

Key to the design of the system used in this research is an adversarial mechanism that cyclically refines pre-DP treatments and post-DP analysis that attempts to reassociate microdata records, as outlined in Chapter 3. This adversarial mechanism requires developing, measuring, and refining two separate systems and using a DP mechanism to perform the privacy-enhancing transformation on the data set. The relationship between the components is detailed below in Figure 4.2, with the orange and bolded components representing the research artifacts generated from this technical action research.

4.5.1 Pre-DP Experimental Artifact

The first experimental artifact (the Pre-DP artifact) attempts to inhibit the efficacy of the second (the Post-DP artifact). The design of this artifact must be novel and not simply adjust the privacy loss budget parameter unless that adjustment is contextual for the preprocessed microdata and generally and repeatably applicable to various input data contexts. Expressly, this Pre-DP artifact is permitted to use the following strategies to

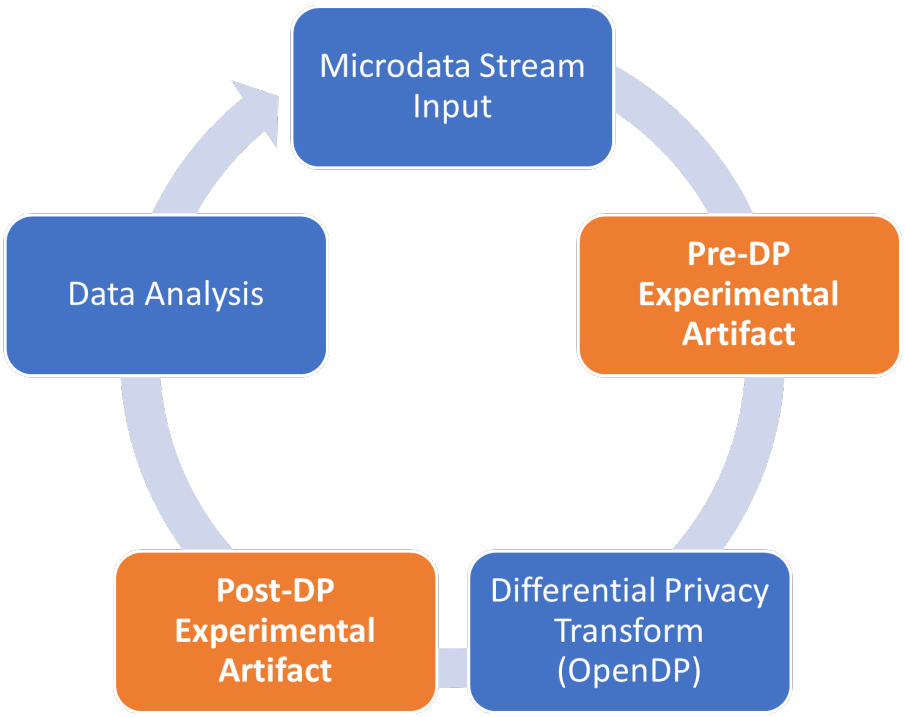


Figure 4.2: Component Relationship Diagram

preprocess microdata streams for differential privacy transformation:

1. Context-based adjustment of the privacy loss budget parameter
2. Partitioning streams into blocks for additive noise application
3. Context-based perturbations of attribute values by an additional additive noise value to pre-apply a skew to attribute values before the DP transformation, such that the privacy-utility tradeoff is substantially preserved
4. Any combination of the three strategies above (provided the privacy-utility tradeoff and key aggregates are substantially preserved)

Figure 4.3 represents the artifact design strategy that utilizes partitioning schemes to determine the qualifying characteristics for dividing buffered stream input into non-uniform blocks with block-local ϵ values. This strategy can output the same set of partitions with varying block-local ϵ values to test varying approaches, provided the resulting

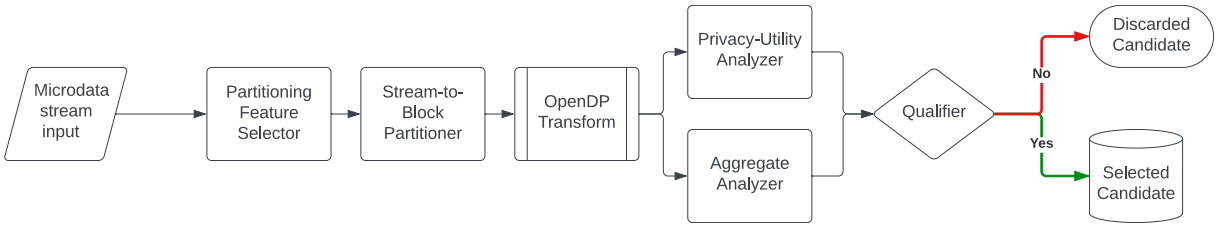


Figure 4.3: Pre-DP Experimental Artifact Logical Flowchart

set can satisfy the threshold requirements of the privacy-utility analyzer and the aggregate analyzer, discussed later. This strategy tests the efficacy of considering microdata streams in buffered chunks, which is a fundamental change to the streaming nature of some data types, such as real-time geolocation data accumulated across a temporal dimension. While valid for analyzing approaches to improve differential privacy, in the client engineering cycle, high bandwidth microdata streams may prohibit some candidates from this strategy if the partitioning scheme requires an intermediate system to buffer large quantities of data to have enough records in each bucket to preserve their event-level privacy.

A key design consideration for the Pre-DP experimental artifact is that it is a reusable tool that can enhance future research on adversarial mechanisms for optimizing differential privacy. It also allows practitioners to strengthen their privacy engineering pipelines. This artifact retains general applicability by designing this component with simple interfaces that take in microdata without prior knowledge or dependencies on its attribute syntax or schema and by producing as its output candidate strategies that are preprocessing directives for microdata stream inputs going into OpenDP. Implementing this experimental artifact will include configuration options to enable selectivity of any of the three strategy pipelines for reusability on other contexts, such as when partitioning, for instance, would not be an appropriate fit for the operating context of an environment not contemplated by this research.

4.5.2 Post-DP Experimental Artifact

The second experimental artifact attempts to reassociate disparate microdata records (event-level data). The generation of reassociation strategies is compromised of a two-part process, whereby a reassociation function is first generated through a genetic algorithm (Figure 4.4), with reinforcement learning from the knowledge of the actual microdata stream values before any differential privacy treatment is applied to evaluate reassociation performance on an OpenDP-treated version of the same microdata stream. The specific threshold in assessing and qualifying the performance of a post-DP strategy for this first pass is highly dependent on the context of the microdata stream, such as how much clustering or variability is present in the stream. For instance, geospatial data sampled over one year in a small city may exhibit significantly different post-additive noise properties in aggregate than the same data sampled over only a month but over a sizeable multi-state region.

Subsequently, algorithms that pass the threshold re-association performance once trained on the delta between differentially private data and the original input microdata stream are tested against the stream with both the Pre-DP experimental artifact and OpenDP treatment applied. While the associative performance is always expected to be worse than the first-pass qualifying test if the pre-DP experimental artifact is effective, the goal for the post-DP experimental artifact is to minimize this spread. By realizing the goal of minimizing that spread, the post-DP experimental artifact seeks to reduce the efficacy of the pre-DP experimental artifact adversarially. Provided repeated cycles of this entire process, illustrated in Figure 4.2, provide more effective Pre-DP experimental artifacts take on their own, and the Post-DP experimental artifacts maintain a minimum spread between the first and second pass qualifications in its cycle, the Pre-DP experimental artifact progressively develops improvements to differential privacy for microdata streams in an empirically measurable way that can be further validated in a client context

in a separate and final TAR engineering cycle.

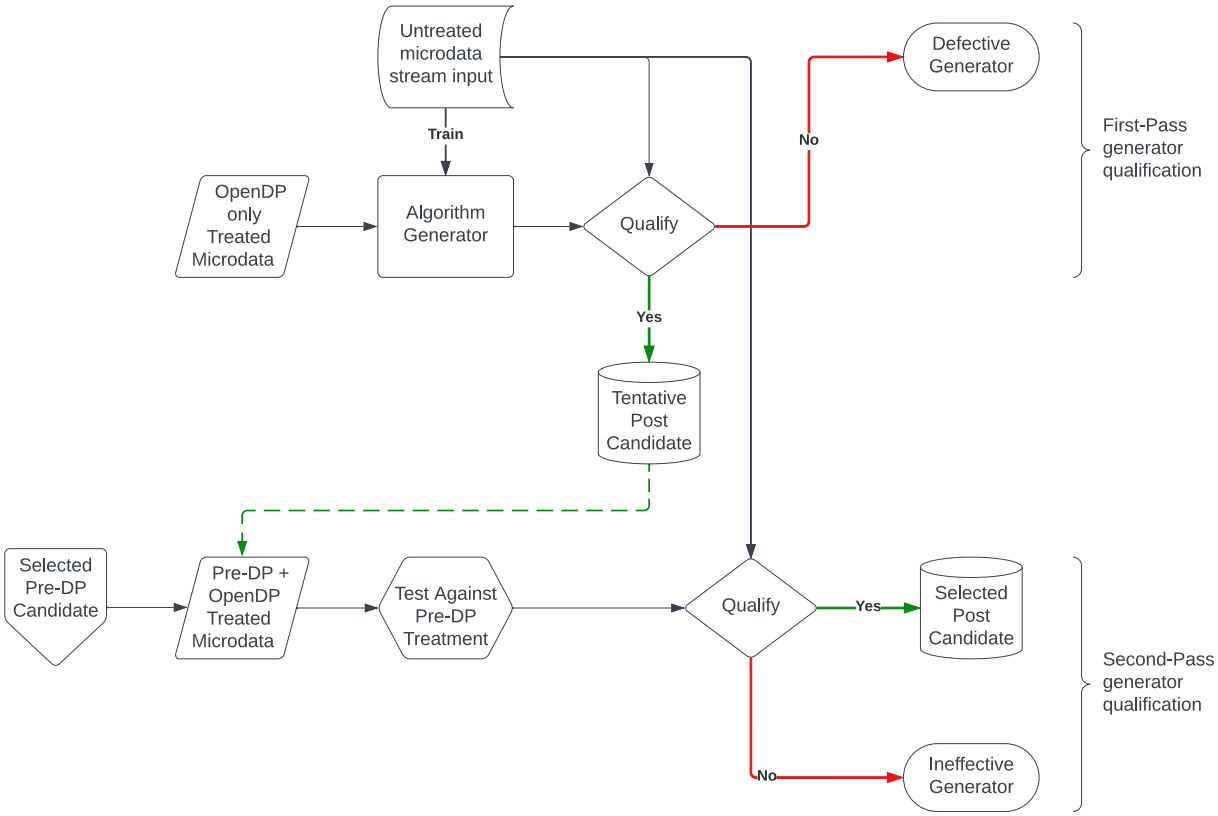


Figure 4.4: Post-DP Experimental Artifact Logical Flowchart

4.6 Data Analysis

The data for this research will be collected into a set of files for each data provider client, as described in the 'Sampling' section in Chapter 3. Where possible, in addition to formatting data into the schemas proposed in the Sampling section, keyed-hashes (HMAC-SHA256) will be applied to personally identifiable information where specific knowledge of the personal data's actual value is unnecessary for the treatment or the experimental artifact. This step further protects privacy through the duration of the research execution where, for instance, it is unnecessary to know a data subject's name is John Doe. Still, it might be helpful to understand which other data subjects have the same last name, as comparable as a one-way computed hash.

For each sampling data set S of n data subjects, each with one or more microdata entries, n number of computations will be performed for each mechanism:

1. First, with the experimental artifact computed in the mechanism M_1 such that a new set of sets T_1 is created, each missing one element (y) from the original set S, or formally: $\{\forall x \in S \backslash \{y\} | M_1(x)\}$.

2. Next, without the experimental artifact as computed by the mechanism M_2 for all elements in set S other than itself such that a new set of sets T_2 is created, each missing one element (y) from the original set S, or formally: $\{\forall x \in S \backslash \{y\} | M_2(x)\}$.

3. Finally, with both the DP Streaming Enhancement treatment and the experimental artifact as computed by the mechanism M_3 for all elements in set S other than itself such that a new set of sets T_3 is created, each missing one element (y) from the original set S, or formally: $\{\forall x \in S \backslash \{y\} | M_3(x)\}$.

The resulting are three distinct sets of sets T_1, T_2, and T_3 to which each will be analyzed with differential privacy using the OpenDP tool for a client-provided constant privacy loss budget (ϵ) and computed using the logarithmic relationship of the differentially-private outputs, previously defined in the descriptive inference design (referred to as function $\wedge(x, y)$ hereafter in this section). The output of three comparisons for $\bigwedge_{i=1}^{n}(T_1, T_2)$, $\bigwedge_{i=1}^{n}(T_2, T_3)$, and $\bigwedge_{i=1}^{n}(T_1, T_3)$. Each function outputs a stream of floating-point numbers that serve as the three distributions for SSMD statistical tests using a 0.95 confidence interval.

Because this TAR will feature an iterative cycle of changes for the treatment and experimental artifact, the researcher will carefully document any change to either aspect in a laboratory workbook and preserve these three output sets from $\wedge(x, y)$ alongside each iteration. The 'action' portion of this methodology provides for repeated analysis whereby the analysis of a given cycle may influence the treatment or artifact design, such

as reverting a previous change or using insights from a subsequent one to inform further experimentation and future analysis.

Chapter 5

Implementation

5.1 Introduction

Differential privacy is an important development that allows for the publication of data in a manner that adds statistical noise to strike a balance between privacy and utility. When differential privacy is applied to a data set, it is not reliably possible to determine whether a given data subject is in a dataset containing many other members. Special problems arise when data sets represent not just one member per data subject but potentially many representations of the same data subject, such as spatiotemporal data points (e.g., timestamped geolocation coordinates). In this case, even though a specific timestamped location may not be known to be truly in a data set, the overall representation of a data subject through many other coordinates could allow for the presence of the data subject to be inferred. This is a known problem with microdata streams, sometimes referred to as "event-level privacy" in the context of differential privacy, and implementation errors in addressing event-level privacy in microdata streams can cause irreparable harm to affected data subjects in published data sets.

This chapter discusses the detailed implementation plan for this research. It outlines how data will be generated, collected, and analyzed using two research artifacts developed as part of the technical action research methodology outlined in previous chapters. Because technical action research has two research cycles, synthetic spatiotemporal data is the subject of the empirical cycle, and real-world spatiotemporal data is the subject of the client cycle, described in the following section. This chapter discusses the methods for

validating the research artifacts for efficacy, including expected outcomes, culminating in a discussion of anticipated contributions. This implementation plan addresses a fundamental need to ensure the application of differential privacy treatments is resilient to certain types of association attacks that can identify individuals in microdata streams. Through an iterative research and development process that refines an artifact that attempts to harm and another that attempts to preserve privacy where differential privacy is applied to test the effectiveness of differential privacy when applied to microdata streams and to develop novel refinements that help preserve privacy in published data sets.

5.2 Data Sets

5.2.1 Empirical Cycle

As described in Chapter 3, technical action research requires three cycles: a design cycle, an empirical cycle, and a client cycle to ultimately solve real-world problems of a client with solution-oriented artifacts validated in a controlled research environment. To support the development and implementation of the Pre-DP and Post-DP artifacts, the researcher will synthesize spatiotemporal data mimicking a time series of interleaving mock users with two-dimensional GPS latitude and longitude points on an arbitrary plane. This synthetic data provides an accurate data set of points that can be compared to a mutation with additive noise applied. The synthetic data tool has already been created by constructing a graph of nodes where agents with preassigned paths and delays move among their respective paths and output timestamps and location coordinates to an output file. An illustration of the synthetic data tool's graph nodes with overlapping agent breadcrumbs is reproduced below in Figure 5.1.

In Figure 5.1, breadcrumbs of a particular color belong to the same mock data subject. The output data resulting from runs of this synthetic data tool can be overlaid with a version of the same data with a Laplacian additive noise function applied that perturbs

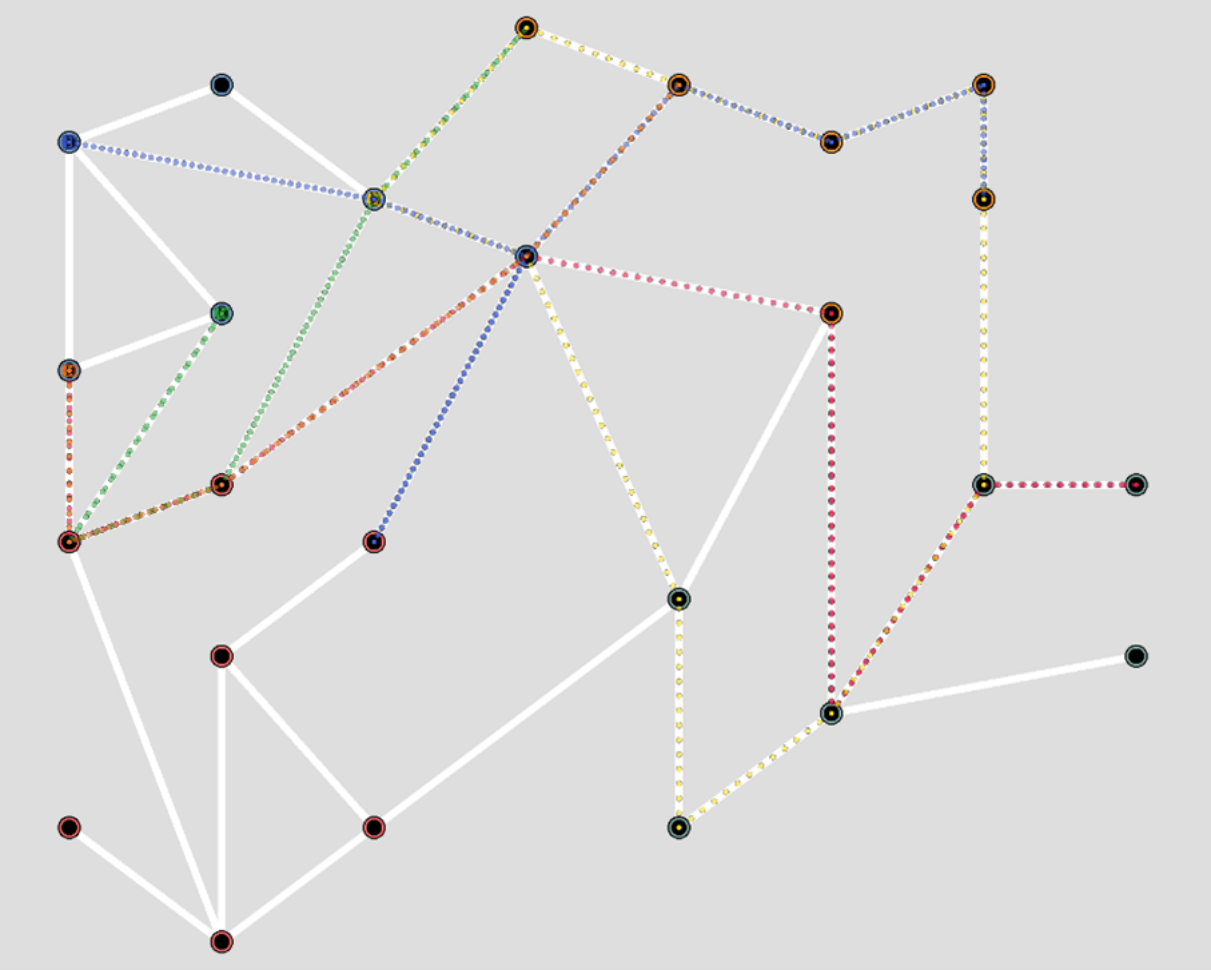


Figure 5.1: Synthetic data creation tool agent path traversal

these 'true' synthetic data points on all spatial dimensions. The resulting illustration in Figure 5.2 demonstrates the comparative scatter of e-differentially private mock data with the actual points. The purpose of the Post-DP artifact, which is described in Chapters 3 and 4 and further outlined in the following sections, is to attempt to reassociate points from the noisy versions of the same color without knowledge of the data subject identifier ("color") through the approaches outlined in Chapter 4.

As described in the preceding chapters, the Pre-DP artifact aims to adjust the noisy variations of original locations in the synthetic data to harm the efficacy of the Post-DP artifact. These artifacts would produce alternative versions if represented as in Figure 5.2, which repositioned the scattered points to preserve the utility of the differentially

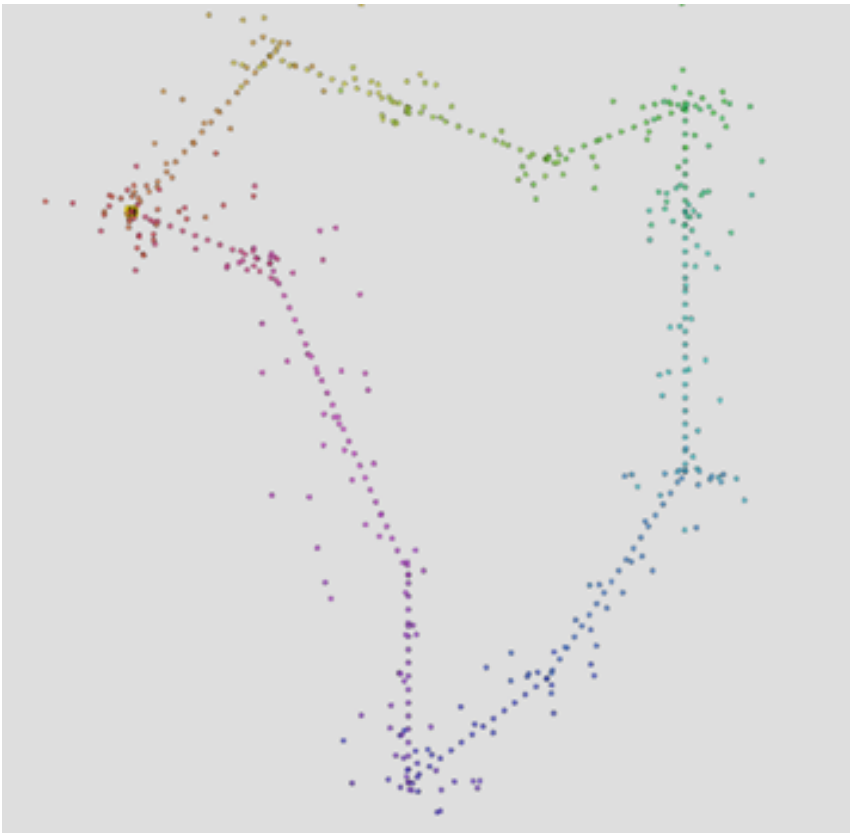


Figure 5.2: Overlaid plot of agents in a closed graph, both with actual and differentially private versions of spatial locations

private publication but thwarted the associative ability of the Post-DP artifact.

5.2.2 Client Cycle

As described in Chapter 3, the artifacts developed as part of the empirical cycle must be validated to solve a client's problem in the client cycle as part of the technical action research methodology. The researcher has identified a fintech client that is interested in applying differential privacy techniques to spatiotemporal microdata streams of consumers' mobile device geolocations captured at critical digital banking events, including registration, authentication, profile changes, money movement requests, and casual service usage, such as where the device is when a user performs "quick balance" inquiries. This dataset consists of only anonymized user identifiers (randomly generated GUIDs),

timestamp data, and latitude and longitude coordinates captured by onboard GPS sensors and reported by the device through the fintech company's native mobile applications. The fields for this client data match the attribute schema of the synthetic data described in the preceding section. Given this congruence, the validation methods described in the following section should generalize the solution from the empirical cycle well when applied to this real-world data set in the client cycle.

5.3 Pre-DP and Post-DP Artifacts

The research will implement these artifacts as a .NET 8.0 C# subroutine executable through a standalone console program and as a Jupyter Labs notebook to allow for reproducible data processing pipelining and iterative development in a research development environment. Data preparation and cleaning routines to support the Pre-DP artifact are implemented as additional C# subroutines or Python scripts utilizing the `pandas`, `numpy`, or similar libraries as needed. Each artifact will be independently developed so different iterations and approaches can be substituted into data processing pipelines to validate them using the methods described in the following sections. Utilizing a lab notebook and a source control repository allows different branches to be retrieved, used, and shelved to support a variety of developments for each throughout the research timeline.

5.4 OpenDP Treatment

OpenDP is a "community effort to build trustworthy, open-source software tools for statistical analysis of sensitive private data" [6]. The primary deliverable of this effort is the OpenDP Library, which is "a modular collection of algorithms for building privacy-preserving applications, with an extensible approach to tracking privacy, and a vetted implementation." [77]. With the support of various academic and industry partners, including the Institute for Quantitative Social Science, Harvard School of Engineering and

Applied Sciences, United Census Bureau, and Mozilla, the implementation is supported by formal proofs evaluated by a board of experts in data privacy. While other differential privacy programming libraries exist, namely `tensorflow-privacy`, the formal verification of this treatment is preferred for this research.

Laplacian and Gaussian mechanisms are traditionally employed in differential privacy to interject additive noise to balance privacy and utility per a privacy loss budget [78]. OpenDP Library supports both mechanisms and for this implementation, the traditional Laplacian mechanism (as implemented by the `make_base_laplace` function in OpenDP Library) is selected. Iterative testing of the Pre-DP and Post-DP artifacts will be performed at varying privacy budgets (ϵ), but validation will be required for acceptance at $\epsilon = 1$. Similarly, OpenDP Library supports multiple aggregates of differentially private data sets, and for this validation method, the geometric mean, as implemented through the use of the OpenDP Library function `make_mean`.

5.5 Methods for Validation

As noted in Chapter 3, an adversarial mechanism developed in an iterative technical action research methodology results in two experimental artifacts: "Pre-DP" and "Post-DP". The Pre-DP artifact is constructed to attempt to improve the application of differential privacy, and the Post-DP artifact is built to try to harm the application of differential privacy. Improvement and harm are measured as a statistically significant distribution in the probabilities of the data set with various treatments applied.

As noted in Chapter 4, the Strictly Standardized Mean Difference (SSMD) test will measure the effect size between probability distributions where various differentially private mechanisms (M) are applied to the data set. Traditionally, the Standard Means Difference (SMD) statistical test, such as Cohen's d, is used to measure effect size between independent groups; however, SMD cannot be applied to two groups that are not

independent, and SMD does not readily estimate the magnitude of effect [79]. For this reason, this research uses SSMD as the validation method, which takes the form [80]:

$$\beta = \frac{\mu_1 - \mu_2}{\sqrt{\sigma_1^2 + \sigma_2^2 - 2\sigma_{12}}}$$

In the preceding equation, β represents the strictly standardized mean difference (SSMD), μ_1 and μ_2 represent means of the first and second data sets for which to compare the effect size, respectively, σ_1^2 and σ_2^2 represent the variance for each data set and σ_{12} is the covariance between the two groups. Three data sets and three comparisons are required for validation. The data set described above is treated in three permutations, resulting in subpopulations and probability distributions for each as described below, per Chapter 4:

1. M_1 is a distribution with ϵ-DP and Post-DP treatments
2. M_2 is a distribution with only ϵ-DP treatment
3. M_3 is a distribution with each of the Pre-DP, ϵ-DP, and Post-DP treatments all applied

Visually represented, these subpopulations used for this SSMD validation method are generated as illustrated in Figure 5.3.

Each subpopulation probability distribution is compared using the SSMD validation measurement described above to determine which treatments have a statistically measurable effect as well as the relative size of the effect. SSMD effect sizes are described with the following threshold ranges and subtypes [81]:

SSMD is a statistical measure of size of effect originally designed for high throughput screening in genomics [81], [82]. The use of SSMD for contrast variables, whereby the sum of mean coefficients is zero, is equivalent to the Standardized Mean of a Contrast

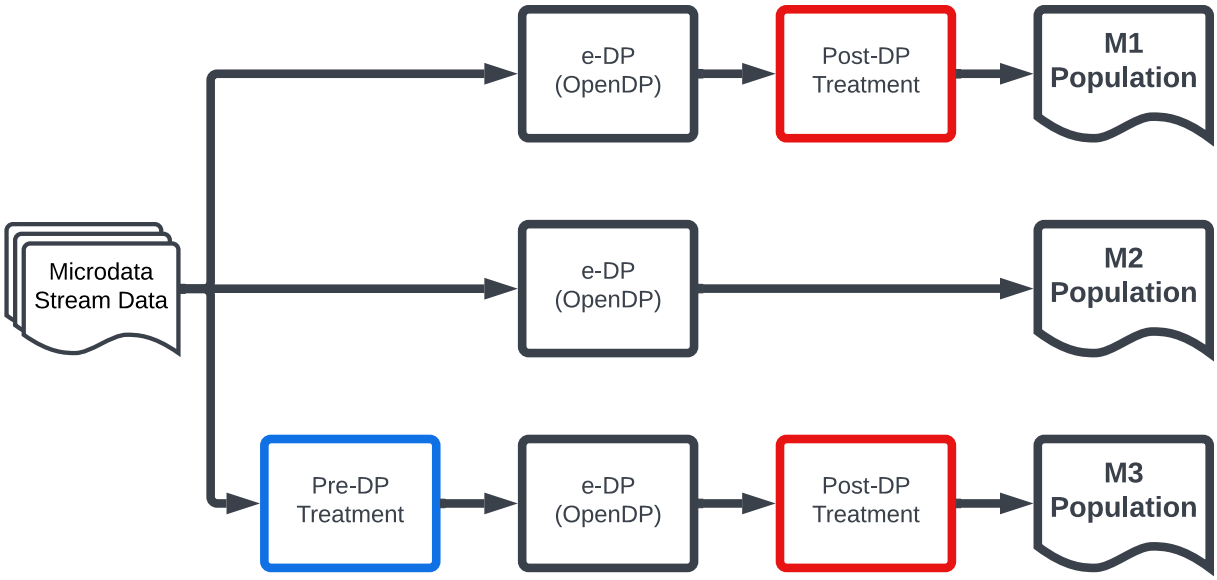


Figure 5.3: Treatment Subpopulations for Validation Methods

Variable (SMCV) when only two groups are involved [83], which is true per the descriptive inference design described in Chapter 4. The size of effect classified in the Table 5.1 represent points of criticality not selected specifically for this research, but are based on the probabilistic relationship between SMCV and the probability of contrast variables resulting in a positive value [82], [84].

The comparison of M_1, M_2, and M_3 will be assessed using the Moderate and stronger thresholds from Table 5.1 for the SSMD validation method. For example, $M_1 \not\sim M_2$ will be validated if $|\beta| \geq 1.28$, and $M_2 \sim M_3$ will be validated if $1.28 > |\beta|$, as measured between the respectively identified probability distributions. In other words, if the effect is "fairly moderate" or weaker, there is not a significant enough difference between the probability distributions to matter for the research questions.

Table 5.1: SSMD Effect Thresholds [81]

Effect subtype	**Threshold of SSMD**
Extremely strong	$\|\beta\| \geq 5$
Very strong	$5 > \|\beta\| \geq 3$
Strong	$3 > \|\beta\| \geq 2$
Fairly strong	$2 > \|\beta\| \geq 1.645$
Moderate	$1.645 > \|\beta\| \geq 1.28$
Fairly moderate	$1.28 > \|\beta\| \geq 1$
Fairly weak	$1 > \|\beta\| \geq 0.75$
Weak	$0.75 > \|\beta\| \geq 0.5$
Very weak	$0.5 > \|\beta\| \geq 0.25$
Extremely weak	$0.25 > \|\beta\| \geq 0$
No effect	$\beta = 0$

5.6 Expected Results

This technical action research posits the development of two independent and successful artifacts: the Pre-DP and Post-DP treatments. These treatments are effective if, after all design and empirical cycles have concluded, the Post-DP treatment harms ϵ-differential privacy, and the Pre-DP treatment improves ϵ-differential privacy respective to the adversarial Post-DP treatment. As noted in Chapter 4, this requires three independent probability distribution comparisons to hold:

1. $M_1 \not\sim M_2$: If these probability distributions have a "fairly moderate" or weaker size of the effect, this indicates the Post-DP artifact meaningfully perturbs the ϵ-differentially private resultset ceteris paribus. Perturbation alone, however, does not infer the efficacy of the Post-DP treatment in its associative ability. For this reason, the Post-DP treatment must demonstrate in a controlled empirical cycle using synthetic data that it can reassociate a statistically significant amount of the data after the additive noise mechanism of OpenDP is applied. This validation of the Post-DP artifact is a prerequisite step of this research protocol before the SSMD validation of M_1 and M_2.

2. $M_1 \not\sim M_3$: If these probability distributions have a "fairly moderate" or weaker size of the effect, this indicates the Pre-DP artifact meaningfully perturbs the final subpopulations even after the OpenDP and Post-DP artifacts are applied. Similar to the aforementioned expected comparison, perturbation alone does not infer the efficacy of the Pre-DP treatment in its privacy-protecting ability. However, this result is expected because if the Pre-DP artifact's size of the effect is not at least measurable after the application of ϵ-differential privacy additive noise, then it is not meaningfully contributing to the dual adversarial mechanism of this methodology and treatment design.

3. $M_2 \sim M_3$: If both treatments comprising the adversarial mechanism are effective, it is still essential that the drift in the ϵ-differentially private resultset, including aggregates such as summations, do not materially differ from the aggregate from the additive noise injected by standard ϵ-differentially privacy mechanisms. In another way, the pre-DP and post-DP mechanisms must substantially perturb the results of the previously documented expected results, but they cannot harm the overall utility of a differentially private data set. Validation of this result would support a conclusion that the treatments are consequential for end-users.

5.7 Contribution

The contribution of this research is two quantitatively validated artifacts that implementers can use to enhance the application of differential privacy. The Post-DP artifact can be used in other contexts for spatiotemporal microdata streams, as described in the first point in the preceding expected results section of this chapter, to determine whether the expected privacy can be harmed through associative techniques refined as part of this adversarial approach to iterative technical action research. Suppose the Post-DP artifact can harm the privacy of a published dataset treated with OpenDP or another library

that applies additive noise. In that case, this can suggest to implementers that they have selected a privacy loss budget (ϵ) that is too favorable for utility at the expense of privacy or have misused or misconfigured data pipeline components. An alternative explanation could be an implementation error of the additive noise mechanism by the implementer or in the additive noise implementation within a library itself. The availability of such an artifact is vital as it allows both practitioners of differential privacy methodologies and the libraries' developers to gain assurance that they are working as intended.

A secondary contribution is the Pre-DP artifact, which practitioners can use to enhance the privacy of spatiotemporal microdata streams further. If practitioners implement both the Pre-DP artifact transformation, apply an additive noise mechanism, and find utility is equivalently acceptable with and without the Pre-DP artifact, this Pre-DP artifact can improve the resistance of a published data set to other associative attacks. Moreover, the adversarial techniques established in the methodology of this research then serve as a blueprint for future research in different microdata contexts beyond spatiotemporal data to identify and mitigate privacy harms in other domains.

Chapter 6

Evaluation, Results, and Analysis

6.1 Introduction

In this chapter, I present a comprehensive evaluation of the two artifacts designed to address threats to differential privacy in the context of spatiotemporal streams, specifically focusing on timestamped GPS coordinates. The first artifact (Pre-DP) aims to identify correlations that can be inherent in spatiotemporal streams. As noted in previous chapters, "patterns of life" analysis of these microdata can reveal which data points are likely emitted from the same data subject, and by comparing these patterns to external data sources, these vectors could be reassociated to individuals. The second artifact (post-PD) functions to introduce perturbations in microdata while preserving the utility of the final published data set to thwart the efficacy of the Pre-DP artifact. Through the experiment outlined in Chapter 5, an analysis follows both in a synthetic data set and in a real-world data set provided by a client to analyze the effectiveness of both the attack and defense strategies in real-world scenarios, assessing their impact on the utility and privacy of microdata streams. The results from these experiments are presented in detail, followed by a critical analysis of their implications, strengths, and weaknesses. This chapter provides the insights necessary for understanding the practical implications of deploying these artifacts in safeguarding spatiotemporal data, focusing on their performance and the trade-offs between privacy and utility.

6.2 Evaluation of the Empirical Design Cycle

As detailed in Chapter 3, this evaluation used the Technical Action Research (TAR) methodology, which contains both an empirical cycle and an engineering cycle. The empirical cycle consists of five distinct steps [13], which are:

1. Research problem analysis
2. Research and inference design
3. Validation
4. Research execution
5. Data analysis

Chapters 4 and 5 addressed the research problem analysis, research, and inference design aspects of the empirical cycle of TAR. The following subsections detail the validation, research execution, and data analysis steps for each of the artifacts developed as part of this research.

6.2.1 Pre-DP Artifact

The design of the Pre-DP artifact was updated from the original implementation plan visualized in Figure 4.3 through the iterative development in the empirical cycle. The three core components of this artifact were the partitioning feature selector, the stream-to-block partitioner, and the decisions logic in the qualifier. In particular, dynamic feature selection in low-dimensionality spatiotemporal data (which contains timestamps and latitude and longitude was discarded from the design in favor of simple binary space partitioning (BSP) using a point quadtree algorithm that chunked microdata within a time period into approximately equally populated partitions [85].

The results of the combined Pre-DP and Post-DP artifacts analyzed with SSMD (see following section 6.4 for results) supported the conclusion that dynamic approaches that used inferred or calculated attributes in this artifact, such as presumptive velocity or acceleration to link microdata and separate them into separate partitions were not meaningfully more performant than a per-period BSP carving approach. (Note that as visualized in Figure 5.3 and discussed in Chapter 5, this Pre-DP artifact cannot be validated on its own to answer the research questions posted in Chapter 1, but only as a combined result in the M_3 population) The altered approach to this design in this evaluation and result gathering resulted in a Pre-DP artifact that is more generally applicable for spatiotemporal data where the strength of inferred effects, like velocity or acceleration, may not be as characteristically strong as in the synthetic data generated. The final design was unaltered from Figure 4.3, considering the feature selector was simply a time period, and the stream-to-block partitioner used a 2D binary space partitioning algorithm that bucketed points into between 4 and 20 partitions, preferring as many as possible for a given time period provided every partition contained at least 10 points. The number 10 was arbitrarily chosen but is a constraint accounted for in the amount of additional privacy budget to allocate to points within a partition.

For each point in a given partition, a variable additional privacy budget (ϵ) was selected to distribute among coordinate (but not temporal) dimensions of the microdata. This additional Pre-DP artifact privacy budget was allocated on an inverse weighted-average basis considering the relative 2-D distance of the nearest-neighboring point for any time in the period bucket. Said simply, the position of points were perturbed more if they were closer to other points. The rationale behind this additional privacy budget distribution strategy was that the efficacy of perturbing points far away from other points was a relative "waste" of the additional privacy budget, as inferred roadways could still be inferred for points in sparsely populated areas (either in neighboring microdata or in roadway complexity). This additive noise was better spent in denser areas that could

frustrate efforts to correlate data points in congested areas or in complex or overlapping travelways.

6.2.2 Post-DP Artifact

The design of the Post-DP artifact is generally unchanged in the research execution as illustrated in Figure 4.4 with some important clarifications and boundaries imposed during the iterative empirical cycle. The process flow detailed in Figure 4.4 is an algorithm generator with a two-step qualifier. Originally envisioned to support automated or genetic algorithm analysis, the research execution that produced these results was a manual, iterative process for developing theories, implementing them in code, and testing them as part of the full M_1, M_2, and M_3 comparative analysis, provided below as results in section 6.4. The implementation of a genetic or generative AI-based "Algorithm Generator" component as visualized in Figure 4.4 remains as a future development of this work. A revised diagram of the Post-DP Experimental Artifact as actually implemented with the final selected algorithm strategy with an explanation follows.

The key objective of the Post-DP is to 'harm' data privacy by overcoming the additive noise provided by the overlaid effects of the OpenDP differential privacy application of Laplacian noise as well as the Pre-DP effects outlined in the preceding section. As originally envisioned, the experiment for this research was microdata streams for "vehicles" that transport individuals rather than the individuals themselves. The key distinction as it relates to the Post-DP artifact is vehicles, such as planes, trains, and automobiles, tend to travel well-worn paths in 2D and 3D spaces, on existing roadways or flight patterns. In addition, vehicles have an intrinsic inertia and momentum and express speed in a wider range than humans can by walking or running alone. They also express changes in direction more gradually over time at higher velocities, and increases in velocities are capped by mechanical limits, congestion conditions, and legal policy forces (such as speed limits).

The focus on vehicles has several key implications for the research execution: synthetic

data must mimic "vehicular" transport as it relates to these aforementioned characteristics and the validation of this Post-DP artifact in the client engineering cycle must be limited to microdata stream elements that demonstrate superhuman velocities (and are likely to be vehicular travel). However, the limitation allows inferences that aid in the construction of an associative artifact using a Hidden Markov Model (HMM), other multivariate classifiers, and machine learning approaches. Given this opportunity, I selected the Accord.NET statistical analysis framework's HMM classifier. While this framework is now an archived project, it is mature and proven as a sequence classifier. Whereas each actual trajectory of a data subject in the empirical spatiotemporal data set is a sequence of microdata timestamped GPS locations, they also represent time-indexed stochastic processes with behaviors that are not directly observable. Moreover, repeated trajectories that establish a "pattern of life" measured over many trips have qualities both of hidden Markov-models for time series data as well as latent Markov models for longitudinal data [86]. For this reason, predicting whether a future time-index datum in a microdata stream where previous stream components have been associated as part of a sequence of data points belonging to a single data subject on a trajectory can be modeled as a HMM sequence classifier and trained on spatiotemporal microdata streams that are labeled by an opaque data subject identifier. If event-level privacy is not effectively rendered on a differentially private data set, this Post-DP artifact strategy with a trained HMM sequence classifier would demonstrate the ability to associate a substantial subset of a de-identified microdata stream values as belonging to the same data subject.

6.2.2.1 Model Training

The final artifact algorithm used for training the HMM is as follows, and specified in pseudocode in Algorithm 1:

Step I	Split labeled data set into a training and test data set
Step II	For each training datum in the spatiotemporal microdata stream with a future timestamp, calculate absolute distance and time delta.
Step III	From these values, calculate velocity (distance over time), acceleration (first derivative of acceleration), and angular acceleration (change in angle from points $T-2$ to $T-1$ to points $T-1$ to T, all over changes in velocity from $T-1$ to T).
Step IV	Train a model using the Baum-Welch multi-variant empirical distribution "learner" with $Tolerance = 0.001$, $MaxIterations = 100$, and normal fitting options with a regularization of 10^{-6} (required to be specified to overcome an implementation bug in the Accord.NET framework)

6.2.2.2 Model Use

The final artifact algorithm used for the evaluation and result gathering using the trained HMM is as follows:

Algorithm 1 HMM training data preparation algorithm

Require: *labeled*, *training*

$MAX\_VELOCITY = 0.72579$ ▷ Maximum allowable instant velocity
$MAX\_DELTA\_TIME = 934$ ▷ Maximum allowable sampling rate gap
$MAX\_ABS\_ACCELERATION = 0.00170$ ▷ Maximum allowable absolute acceleration
$next\_possibilities \leftarrow \{\}$
for all $t \in \{training\}$ **do**
  $time\_t \leftarrow$ TIMESTAMP(t)
  for all $p \in \{training\}$ **do**
    $time\_p \leftarrow$ TIMESTAMP(p)
    if $time\_p \leq time\_t$ OR $|time\_p - time\_t| \geq MAX\_DELTA\_TIME$ **then**
      continue
    end if
    $distance1 \leftarrow |$ DISTANCE(p, t) $|$
    $delta\_t \leftarrow time\_p - time\_t$
    $velocity1 \leftarrow \frac{distance1}{delta\_t}$ ▷ Distance over time
    if $velocity1 \geq MAX\_VELOCITY$ **then**
      continue
    end if
    $angle1\_change \leftarrow$ GET_ANGLE(t, p)
    for all $p2 \in \{training\}$ **do**
      $time\_p2 \leftarrow$ TIMESTAMP($p2$)
      if $time\_p2 \leq time\_p$ OR $|time\_p2 - time\_p| \geq MAX\_DELTA\_TIME$ **then**
        continue
      end if
      $distance2 \leftarrow |$ DISTANCE($p2$, p) $|$
      $delta\_t2 \leftarrow time\_p2 - time\_p$
      $velocity2 \leftarrow \frac{distance2}{delta\_t2}$ ▷ Distance over time
      if $velocity2 \geq MAX\_VELOCITY$ **then**
        continue
      end if
      $angle2\_change \leftarrow$ GET_ANGLE(p, $p2$)
      $acceleration \leftarrow \frac{velocity2 - velocity1}{delta\_t1 + delta\_t2}$
      if $acceleration \geq MAX\_ABS\_ACCELERATION$ **then**
        continue
      end if
      $angular\_acceleration \leftarrow \frac{angle2\_change - angle1\_change}{velocity2 - velocity1}$
      $is\_correct\_possibility \leftarrow$ CHECK_LABELED($labeled$,t,p,$p2$)
      PUSH($next\_possibilities$, $\{t, p\}$)
    end for
  end for
end for

Step I For each datum in the microdata stream, identify candidate sequence members, which must be in the future and not time-coded more than $2X$ the sampling interval (to prevent illogical associations to trajectories beginning in the vicinity).

Step II Further cull candidates using domain-specific assumptions using calculations of candidates for velocity, acceleration, and angular acceleration, with knock-out conditions defined as:

(a) That from $T-1$ would represent an absolute velocity less than 80 miles per hour.

(b) That from $T-2$ would represent an absolute acceleration less than 20 miles per second.

(c) That from $T-2$ would represent an absolute angular acceleration less than 30 degrees per second per 15 miles per hour increment of velocity. For example, knock out inferred sequences exhibiting 90 degree turns at 45 miles per hour, which are unlikely domain behavior.

Step III If there are multiple future candidates for the given $T-1$ datum, order them by lowest instant acceleration and angular acceleration first, preferring the prediction that previous trajectory behavior remains the same at T. If there are more than four, keep the top 3 and the last 1 candidate.

Step IV For each future datum, evaluate each of the 1-4 possibilities saved in the previous step, and knock out the possibility if there is no satisfiable candidate at that evaluation.

As a result of the modifications to the approach iteratively developed in this cycle, the original Post-DP artifact designed in Figure 4.4 is updated as follows in Figure 6.1

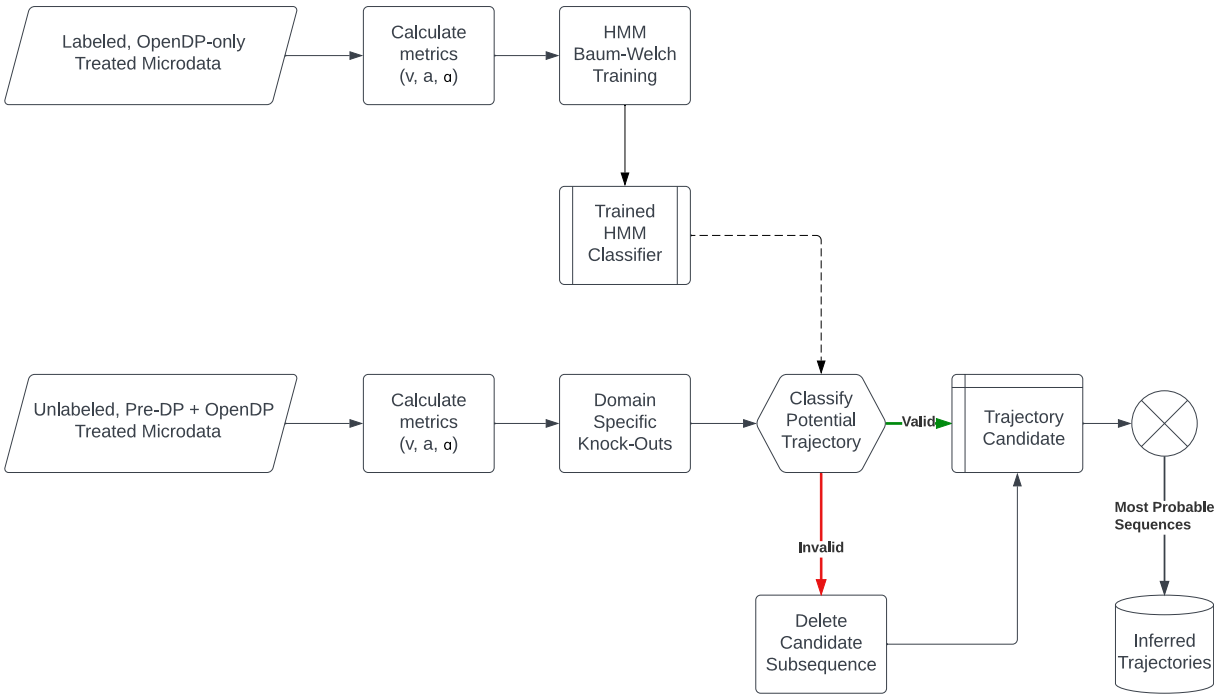


Figure 6.1: Modified Post-DP Experimental Artifact Logical Flowchart

6.3 Evaluation of the Client Design Cycle

6.3.1 Data Handling

With promising results from the empirical cycle (see section 6.4 for details), the next step for validation and research execution for this technical action research was to apply these iteratively-developed artifacts to a real-world client problem, as previously detailed in section 3.3.2.1. The *actual* data handling procedures used to analyze this data were as follows, denoted as 'client' if the procedural step was performed by the client and 'researcher' if I performed the step:

1. **Client:** Extract real-world, historical GPS location data from captured from mobile banking apps, with a numerical EventID, an opaque data subject identifier (a GUID

created by the client's internal systems upon user registration), and spatiotemporal data (timestamp, longitude, and latitude).

2. **Client:** Apply additional blinding techniques to the data fields, which were:

   (a) Create a new GUID for the purposes of this research and replace the internal GUID with this replacement GUID. The client retained the original GUID mapping file and did not share it with the researcher.

   (b) Choose randomized time translation coefficient uniquely and statically profiled for each data subject (GUID). The range of this coefficient was bounded from -7 to $+7$ days. The client added the translation coefficient to microdata stream of each data subject. The client did not share the chosen time translation coefficients with the researcher.

   (c) Choose randomized latitude and longitude translation coefficients and add these static values to every GPS coordinate in the microdata stream. The client did not share the chosen translation coefficients with the researcher.

   (d) Choose randomized rotation coefficient for each data subject, and apply a rotation around the centroid of the full population of spatiotemporal microdata stream events. The client did not share the chosen rotation coefficients with the researcher.

3. **Client:** Provide the blinded to the researcher over a secure file transfer protocol (SFTP) connection.

4. **Researcher:** Parse client files into a CSV format machine-readable by the Pre-DP and OpenDP data pipelines (to prepare testing of M_1, M_2 and M_3 populations, as illustrated in Figure 5.3. Processing and analysis of data then followed the process described in Chapter 5, and training of the HMM was performed as described in section 6.2.2.

The client did not share personally-identifiable information of data subjects shared with the researcher. No data subjects were contacted and no actual observation of data subjects occurred as part of this research. The client determined the use of blinded (derivative) data was explicitly authorized by data subjects under existing privacy policy terms established that allow for the development of enhancements to their service and to which data subjects provided positive consent as a condition for their user registration. The blinding techniques described above were established through mutual agreement between the client and researcher to provide reasonable assurance that in the event of unintentional disclosure of the client data set that the identities of data subjects could not be reassociated to real-world individuals or locations. As a condition of this research, the researcher permanently deleted all client-provided data in accordance with NIST Guidelines for Media Sanitization, using cryptographic erase, at the conclusion of this analysis [87].

6.4 Results

Results were first gathered for the empirical cycle during iterative development of the Pre-DP and Post-DP artifacts, detailed in Table 6.1. Because even small changes to either artifact could significantly alter the size of effect as measured by SSMD, and because the additive noise generated by OpenDP was randomized with each run, the effect magnitude as measured against Table 5.1 had the potential to vary significantly between runs. Each 'run' in Table 6.1 represents a set of code (or 'release') for both artifacts, with the results provided across the row the worst performance for that release, if multiple executions of the OpenDP pipeline (and associated randomness) were obtained for a given release. The last three rows indicate success with re-validation runs of the 2024-12-19, 2024-12-20, and 2025-02-04 release versions independently re-run 6, 13, and 2 times, respectively. For these last three versions, the worst performance across all 21 runs were effective.

Table 6.1: Empirical Cycle Iterative Run SSMD Effects

Run	$M_1/M_2\beta$	$M_1/M_3\beta$	$M_2/M_3\beta$	**Outcome**
2024-08-12	0.630 Weak	1.698 Fairly strong	2.301 Strong	Ineffective
2024-08-30	0.591 Weak	1.444 Moderate	2.013 Strong	Ineffective
2024-09-22A	2.430 Strong	1.293 Moderate	1.248 F. moderate	Ineffective
2024-09-22B	2.171 Strong	1.278 F. moderate	1.241 F. moderate	Ineffective
2024-09-22C	0.540 Weak	1.395 Moderate	3.918 V. strong	Ineffective
2024-09-22D	0.662 Weak	1.993 F. strong	3.128 V. strong	Ineffective
2024-09-23A	0.439 V. weak	1.571 Moderate	0.476 V. weak	Ineffective
2024-09-23B	0.299 V. weak	1.913 F. strong	0.500 Weak	Ineffective
2024-09-28	0.657 Weak	0.759 F. weak	0.702 Weak	Ineffective
2024-10-18	0.246 E. weak	0.511 Weak	0.336 V. weak	Ineffective
2024-11-09A	1.870 F. strong	0.603 Weak	0.747 Weak	Ineffective
2024-11-09B	0.528 Weak	0.698 Weak	0.556 Weak	Ineffective
2024-12-19	0.300 V. weak	0.732 Weak	1.733 F. strong	Effective
2024-12-20	0.521 Weak	0.230 V. Weak	2.012 Strong	Effective
2025-02-04	0.487 Weak	0.748 Weak	1.839 F. strong	Effective

The client data set was large, with microdata events `n=864,180,432` representing 1,203,401 anonymously and uniquely labeled data subjects within the total set of trajectories. These spatiotemporal events were time-sorted and split into four equally-sized batches of `n=216,045,108`, respectively, to aid in process analysis. The artifacts versioned from the 2024-12-20 empirical run were used to process each of these four client data set batches, with results detailed below in Table 6.2. Batches are denoted as B1, B2, B3, and B4 in the Run column.

Table 6.2: Client Cycle Iterative Run SSMD Effects

Run	$M_1/M_2\beta$	$M_1/M_3\beta$	$M_2/M_3\beta$	**Outcome**
2024-12-26 (B1)	0.473 V. weak	0.878 F. weak	1.833 F. strong	Effective
2024-12-29 (B2)	0.617 Weak	0.977 F. weak	2.454 Strong	Effective
2024-12-31 (B3)	0.595 Weak	0.739 Weak	2.350 Strong	Effective
2025-01-04 (B4)	0.460 V. weak	0.753 F. weak	1.752 F. strong	Effective

6.4.1 Efficacy

As noted in Chapter 5 and illustrated in Figure 5.3, the Pre-DP and Post-DP artifacts are effective when the size of effect as measured by SSMD in three subpopulations M_1, M_2, and M_3 are related in certain ways. Specifically, $M_1 \not\sim M_2$ and $M_2 \not\sim M_3$ when the size of effect (β) is "fairly moderate" (abbreviated as "F. moderate" in Tables 6.1 and 6.2 above) or weaker, as specified in Table 5.1. In addition, $M_1 \sim M_3$ must hold at a moderate or higher effect subtype. This is true for empirical runs with artifact versions 2024-12-19, 2024-12-20, and 2025-02-04, and every run of the client cycle using the 2024-12-20 artifacts.

These findings support conclusions that the Post-DP artifact is statistically effective in reassociating event-level metadata to infer data subject trajectories ($M_1 \not\sim M_2$). They also support conclusions that the Pre-DP artifact is effective in defending against this re-association where ($M_2 \not\sim M_3$), and that when both artifacts are applied in the M_3 subpopulation, these artifacts to not unduly shift the underlying utility of the data meaninglessly ($M_1 \sim M_3$).

Importantly, the iterative development methodology of TAR bares out through the successive runs in Table 6.1 the value of using adversarial approaches in strengthening artifacts that can test and defend against probes of naı"vely-implemented differential privacy in microdata streams. While the use of SSMD alone does not necessarily guide developers of artifacts in adversarial contexts towards better outcomes, as even minute changes can cause significant β swings in a pipeline with multiple components (including OpenDP or any random additive noise mechanism), the approach yields measurable design artifacts that have more utility than nuanced approaches to distribution of a privacy loss budget (ϵ) in a domain-specific way. While this research focused on spatiotemporal microdata streams, the methodology in this research (but not these specific Pre-DP and Post-DP artifacts) can be applied to the development of artifacts for any event-level

microdata stream.

6.4.2 Internal Validity

Internal validity measures how well a study is conducted (its structure) and how accurately its results reflect the studied group. For research involving human subjects, a variety of internal validity threats exist, such as the history effect, maturation effect, attrition, or diffusion of treatment alter the ways in which participants respond. In this research which does not involve human subjects but use an iterative TAR methodology, the primary threat internal validity is the testing effect. Testing effects occur when repeated test exposure influences measured performance.

This type of manual over-fitting did not appear to occur during the empirical design cycle which used the same synthetic data set for all runs noted in Table 6.1 except 2024-12-20 and 2025-02-04. The final two runs were both the 2024-12-20 version of the artifact, but each used a regenerated set of synthetic data to provide assurance the artifacts' performance was not over-fitted to the generated data used for all prior empirical cycle iterative runs.

6.4.3 External Validity

External validity relates to how applicable the findings are in the real world. The TAR methodology provides some assurance of external validity through the validation of research artifacts through the client engineering cycle. However, for empirical experiments that do not use attitudinal scales or other social sciences data collection processes, the major threat is a lack of reproducibility by anyone but the researcher [88].

To address this threat, the researcher created a virtual machine image with the M_1 (Post-DP only) and M_2 (OpenDP only) pipelines configured and a subset of the client's population ($n = 864,180,432$) records and instructions to execute the file. The pipelines were chosen because they would provide $M_1/M_2\beta$ SSMD effect metric that should be

weak if the test was valid, and because the intermediate output from M_2 could be saved for a comparison of the SSMD effect for the first of the three comparisons of the overall effectiveness test without additional client processing. The first 100,000 records, in comma separated value format, from run `2024-12-26 (B1)`, as used to generate the first client cycle iterative run in Table 6.2 was baked into the virtual machine image. The client chose a number between 1 and 25,000 and cut out a subset of the 100,000 records using a Linux `head(1)` command. The client chose the number 23,456, which produced a subset file of the first 23,456 records of the `B1` run file.

The client then ran the pipeline in the virtual machine image with the subset file they created to generate results. Afterwards, the client provided the chosen numbers so the researcher could perform the same operation for comparative results. The test was considered externally valid for the client if the SSMD effect for the pseudorandomly-selected subset of the B1 run was fairly moderate or weaker outcome, as detailed in Section 5.6. The specific results or areas of effect need not be same for external validity for this client to be true, since the additive noise process of OpenDP makes each run's outputs vary in accordance with the Laplaican distribution it uses to distribute the privacy loss budget, *ceteris paribus*. The results are provided in Table 6.3. Both runs were effective in part, and only in part because they tested only the $M_1 \not\sim M_2$ component. However, both were consistently passing in this regard.

Table 6.3: Comparative Validity Run and SSMD Effects

Run	$M_1/M_2\beta$	**Outcome**
2024-12-26 (B1 1-23456) Client	0.611 Weak	Effective in part
2024-12-26 (B1 1-23456) Researcher	0.586 Weak	Effective in part

A different type of external validity test would be to test the research artifacts with data from a different client, as some of the assumptions coded as constants in Algorithm 1 may not hold if, for instance, the vehicles were predominately watercraft or spacecraft as opposed to retail banking consumers who were more likely to transit in the data set by

automobile. This would be an interesting future validity test and expansion on the work to generalize the artifacts for other types of real-world data sets.

6.4.4 Performance

To assess the performance of the research artifacts, the Pre-DP and Post-DP components, the researcher performed multiple serial runs of the M_3 pipeline at various sizes of input records from the `2025-01-04 (B4)` run referenced in Table 6.2. For each run, the process to execute any scripts and executable files for each of the Pre-DP and Post-DP components were grouped into shell scripts that were executed using the Linux `time(1)` command. The `user` and `sys` outputs were summed into a result that recorded the actual execution time for each component's run, as detailed in Table 6.4.

Performance test results were collected from a Framework 16 Ryzen™ 9 7940HS - Radeon™ RX 7700S - 180W Power Adapter laptop. The machine had 64GB (2 x 32GB) of DDR5-5600 RAM, a WD_BLACK™ SN850X NVMe™ 2TB M.2 2280 solid state drive. The machine had an AMD Radeon™ RX 7700S graphics module, although neither the Pre-DP nor the Post-DP artifacts had GPU-accelerated algorithms. The laptop operating system was Ubuntu 24.04.1 LTS (Linux Kernel 6.8.0-52).

Using a visual comparison on a logarithmic chart of common "Big-O notation" timings by records, the "Controlled Run" data series represents the "Total (minutes)" column from Table 6.4 compared to common benchmarks including $O(n^2)$, $O(n * log(n))$, $O(n)$, and $O(log(n))$. Ideally, algorithms are sublinear such that they do not perform increasingly longer disproportionately to an increase in inputs[89]. Given "Combined Run" of Figure 6.2 is lower than the linear benchmark of $O(n)$, this is the case for the Pre-DP and Post-DP artifacts. This is presumed to be because the Accord.NET framework used to train the Baum-Welch HMM, detailed above in Section 6.2.2.1, uses parallelization internally to take advantage of multiple cores and threads on the test device. Note that this visual analysis and comparison to Big-O notational benchmarks is not the entire M_3

Table 6.4: Algorithm Performance at Varying Input Sizes

Input size `n`	Pre-DP (minutes)	Post-DP (minutes)	Total (minutes)
100	0.00	0.00	0.00
200	0.00	0.00	0.00
500	0.00	0.01	0.01
1,000	0.01	0.01	0.02
2,000	0.02	0.03	0.05
5,000	0.05	0.08	0.13
10,000	0.10	0.16	0.27
20,000	0.20	0.34	0.54
50,000	0.48	0.92	1.40
100,000	0.96	2.03	2.99
200,000	1.91	4.14	6.05
500,000	5.08	11.23	16.31
1,000,000	10.41	23.92	34.33
2,000,000	20.94	48.97	69.91
5,000,000	47.84	131.65	179.49
10,000,000	101.25	295.33	396.57
20,000,000	193.26	619.23	812.49
50,000,000	485.96	1556.45	2042.41
100,000,000	1036.48	3092.20	4128.68
216,045,108	2144.58	7610.35	9754.94

processing pipeline timing, as the OpenDP timing was not recorded, since its implementation is outside the scope of this research and the efficiency therefor is not material for the evaluation of the performance efficiency of the adversarial artifacts.

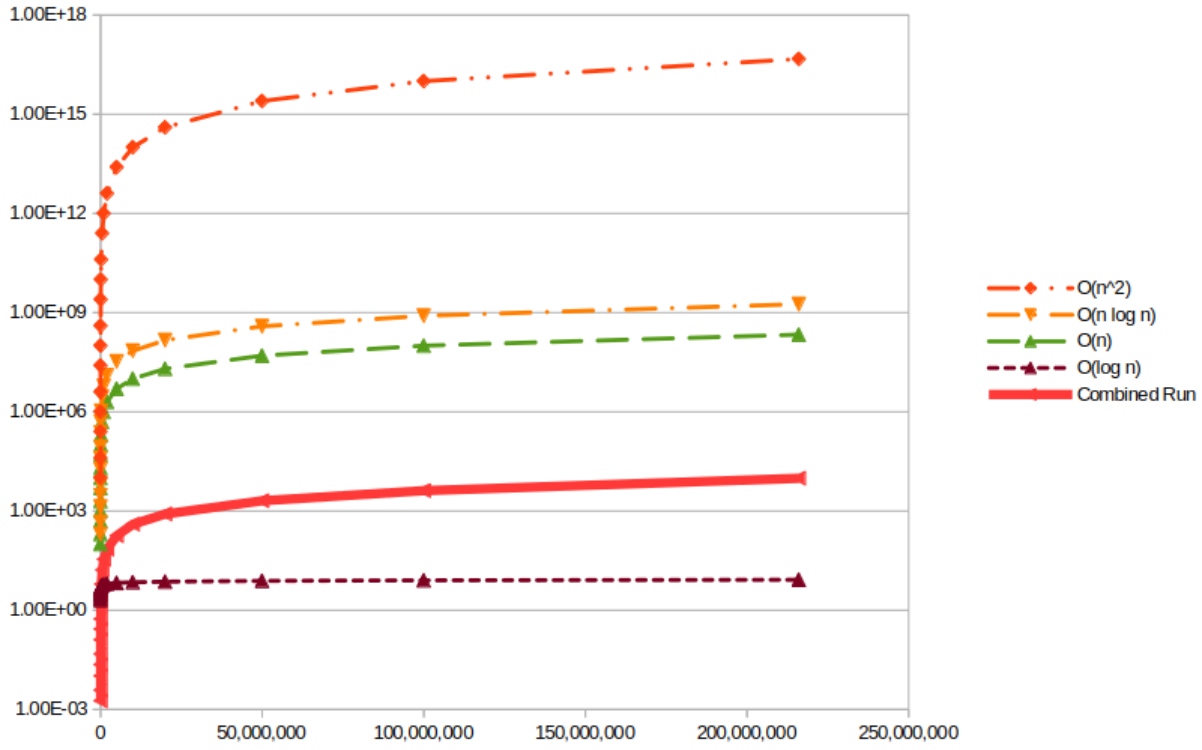


Figure 6.2: Comparative Performance vs. Common Big-O Notations

6.5 Analysis

The evaluation, results, and analysis of this research address both research questions, which as restated from Chapter 1 are:

Question 1: How well does ϵ-differential privacy generally protect microdata streams containing many records correlated with the same data subject or cross-correlated to each other?

Question 2: Are there treatments that better preserve the privacy loss budget and the utility of ϵ-differentially private microdata streams at scale and across domains?

As for Question 1, as established in Chapter 2, there are various threats to ϵ-differential privacy when naïvely implemented with privacy loss budgets that do not account for the patterns of life present in spatiotemporal data or that partition data and apply a privacy loss budget in ways that do not sufficiently distribute additive noise to account for correlation attacks [10], [51], [57], [69]. Specialized approaches to developing domain-specific correlation or inference attacks, such as the Post-DP artifact developed as part of this research, can also generally erode the privacy guarantees of differential privacy in small-world, empirical contexts, as represented in Table 6.1.

As for Question 2, adversarial approaches to developing defensive artifacts, such as the Pre-DP artifact developed through this technical action research, can yield treatments that better preserve private microdata streams, even at large scales, as represented in Table 6.2. However, adversarial approaches that yield complementary artifacts, such as those developed through this research, converge on their problem space and may not be generally applicable across domains. While specific artifacts at the end of a TAR cycle may not have general applicability, the adversarial and iterative treatment development approach is generally applicable to customize treatments for other problem spaces.

Studies of trajectory or spatiotemporal microdata streams are reviewed in Chapter 2, and several focus on the distribution strategy of the privacy loss budget in novel, often domain-specific ways. As opposed to theoretical approaches with lemmas[34], adversarial approaches, particularly those that use the technical action research methodology and those that utilize machine learning approaches to discovering locally optimized solutions depart from rigorous proofs and embrace organic and probabilistic approaches. However, over-fitting is a real risk to the validity of artifacts developed through approaches such as the one detailed in this dissertation [7]. For this reason, measurements of utility are critical in the development of new treatments, as even adaptive approaches can have dramatic falloffs in utility due to nuances in underlying data characteristics, such as landmarks that create disproportionate nexuses of trajectories [62].

No other research to date have used the SSMD approach to measuring utility, although some other research into protecting location privacy in spatiotemporal microdata streams have acknowledged the potential for the approach [90], and none have considered adversarial approaches to the development of supplemental treatments. The SSMD analysis, while computationally expensive in real-time scenarios, can serve as an important tool both in the development of differential privacy applicative technologies done in iterative, adversarial contexts as well as those generated through machine-learning or agentic artificial intelligence approaches as a check against over-fitting or other threats to internal validity.

6.6 Conclusion

Through technical action research, two research artifacts were developed and validated using strictly standardized mean difference (SSMD) to improve privacy of spatiotemporal microdata. These artifacts were iteratively in an empirical engineering cycle and tested against large, real-world data sets in a client engineering cycle. The approach is novel, is internally and externally validated, and meaningfully and performantly defends against correlation attacks inherent in event-level data sets. While these specific, bespoke artifacts were developed manually, the approach for treatment validation lends itself to further developments that use automated generation of artifacts that preserve the differential privacy guarantee in the fact of adversarial attacks without adversely impacting utility, through fully automatable, empirically measurable means.

Chapter 7

Conclusion

7.1 Summary

This research used technical action research methodology to create research artifacts that explored the frontier of differential privacy using an adversarial approach. This approach yielded two artifacts, one that attempted to circumvent naïve implementations of differential privacy that cannot fully address knowledge attacks, such as correlation attacks as discussed in Chapter 2, which can use patterns of life or cross-correlations with external databases to positive identify individual members in microdata streams. The other used strategies to prevent the success of the first, and in an iterative development empirical cycle, the efficacy of this technique was validated using empirical measures. The results of this research answered the research questions, made novel contributions to the body of knowledge of differential privacy, and opportunities for future developments were identified.

7.2 Research Answers

Chapter 1 introduced two research questions which were answered by the results detailed in the preceding in 6. The first research question was about how well ϵ-differential privacy protects event-level data, such as spatiotemporal trajectories of GPS locations. This

question was partially answered by surveying the body of knowledge related to inference attacks on itemsets [3], [4], [33], [34]. A method for measuring the the effectiveness of differential privacy over such data sets was proposed in Chapters 3, 4, and 5 using strictly standardized mean difference testing (SSMD). ϵ-differential privacy cannot protect event-level data without additional protections, which can involve domain-specific approaches to the distribution of a privacy loss budget or partitioning microdata streams; however, special care must be given to not harm utility, which could occur if an arbitrary distribution strategy is implemented without use case consideration.

The second research question asked whether there are treatments that better preserve the privacy loss budget and the utility of ϵ-differentially private microdata streams at scale and across domains? The answer is a conditional "yes": the adversarial approach to treatment development employed by this research measurably protect individual privacy in event-level data, including spatiotemporal trajectories. As Chapter 6 detailed, efficacy can be objectively measured with a magnitude of effect approach across both empirical and real-world client data sets. While the approach yielded effective artifacts, the reusability of artifacts with different types of data, such as event-level clickstream data as opposed to GPS trajectories, is limited, and a cross-domain result is not claimed. The algorithm denoted in Algorithm 1 (Chapter 6) uses domain-specific bounds for maximum data subject velocities, sampling rates, and acceleration, which not only may not hold for other data sets of spatiotemporal data (such as sea vessel trajectories), but are not applicable to microdata sets that do not record physical movement, such as web browsing clickstream data. While this is a limitation, the approach of using adversarial approaches and iterative development in an empirical technical action research methodology shows promise as a reusable approach for other domains to generate their own well-fitting artifacts.

7.3 Contributions

This research delivers two primary contributions. The first of which was covered in the preceding section, which bares out that adversarial approaches, which use dueling artifacts that attempt to 'harm' and 'defend' against knowledge attacks to differentially-private microdata streams can yield effective treatments that not only protect personal data privacy in published data sets, but can provide a way to measure the efficacy of naïve applications of differential privacy to event-level data absent bespoke domain-specific considerations.

The second contribution is the use of SSMD as a statistical measure of the effectiveness of differential privacy treatments for microdata streams. SSMD has been notably used in high-throughput screening research, in genomics and pharmaceutical drug development, but it is a generalized measure of effect size that, given its preconditions for use (detailed in Chapter 4, related to contrast variables), can be used for mean distance testing when there are many trajectories to compare potentially-correlated events with the results from inference attacks. SSMD alone is not a qualifier of whether differential privacy is appropriately applied, but it is a useful diagnostic to compare a differentially-private publication of event-level data, in the case with additive noise applied using OpenDP, and a treatment (see Figure 5.3). This relates back to the first research question, answering "how well" this privacy-enhancing technology performs.

7.4 Recommendation for Future Research

There is an exciting future in artificial intelligence (AI) and, in particular, agentic AI, and a natural development of this work would be to develop treatment generators that could, for a given microdata stream, produce research artifacts in an unsupervised fashion. Given the availability of SSMD both a measure of effectiveness and a potential reward

function, agentic AIs that iterative developed competing treatments in an adversarial approach, as used and demonstrated effective by this research, would naturally fit into generative adversarial network (GAN) approaches. If commoditized and bundled into an open and reusable framework, this could have significant benefits not only for the testing of differential privacy treatments of event-level data, but it could to some degree automate its wholesale application, making this strong guarantee both more widely available with an efficacy-testing mechanism built-into treatment development.

References

[1] R. Jarmin. "Census bureau adopts cutting edge privacy protections for 2020 census," The United States Census Bureau. Section: Government. (Feb. 15, 2019), [Online]. Available: https://www.census.gov/newsroom/blogs/random-samplings/2019/02/census_bureau_adopts.html (visited on 07/09/2023).

[2] R. Agrawal, T. Imieliński, and A. Swami, "Mining association rules between sets of items in large databases," in *Proceedings of the 1993 ACM SIGMOD international conference on Management of data - SIGMOD '93*, Washington, D.C., United States: ACM Press, 1993, pp. 207–216, ISBN: 978-0-89791-592-2. DOI: 10.1145/170035.170072. [Online]. Available: http://portal.acm.org/citation.cfm?doid=170035.170072 (visited on 07/17/2023).

[3] J. Li, W. Gan, Y. Gui, Y. Wu, and P. S. Yu, "Frequent itemset mining with local differential privacy," in *Proceedings of the 31st ACM International Conference on Information & Knowledge Management*, ser. CIKM '22, event-place: Atlanta, GA, USA, New York, NY, USA: Association for Computing Machinery, 2022, pp. 1146–1155, ISBN: 978-1-4503-9236-5. DOI: 10.1145/3511808.3557327. [Online]. Available: https://doi.org/10.1145/3511808.3557327.

[4] N. Li, W. Qardaji, D. Su, and J. Cao, "PrivBasis: Frequent itemset mining with differential privacy," *Proc. VLDB Endow.*, vol. 5, no. 11, pp. 1340–1351, Jul. 2012, Publisher: VLDB Endowment, ISSN: 2150-8097. DOI: 10.14778/2350229.2350251. [Online]. Available: https://doi.org/10.14778/2350229.2350251.

[5] A. Robinson, F. Brown, N. Hall, A. Jackson, G. Kemp, and M. Leeke, "CASTLEGUARD: Anonymised data streams with guaranteed differential privacy," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2020, pp. 577–584. DOI: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00102.

[6] The OpenDP Team, *The OpenDP white paper*, May 11, 2020. [Online]. Available: https://projects.iq.harvard.edu/files/opendifferentialprivacy/files/opendp_white_paper_11may2020.pdf (visited on 04/21/2023).

[7] A. Blanco-Justicia, D. Sánchez, J. Domingo-Ferrer, and K. Muralidhar, "A critical review on the use (and misuse) of differential privacy in machine learning," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–16, Aug. 31, 2023, ISSN: 0360-0300, 1557-7341. DOI: 10.1145/3547139. [Online]. Available: https://dl.acm.org/doi/10.1145/3547139 (visited on 07/17/2023).

[8] J. Domingo-Ferrer, D. Sánchez, and A. Blanco-Justicia, "The limits of differential privacy (and its misuse in data release and machine learning)," *Communications of the ACM*, vol. 64, no. 7, pp. 33–35, Jul. 2021, ISSN: 0001-0782, 1557-7317. DOI: 10.1145/3433638. [Online]. Available: https://dl.acm.org/doi/10.1145/3433638 (visited on 05/02/2023).

[9] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1–12, ISBN: 978-3-540-35908-1.

[10] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, ser. STOC '10, event-place: Cambridge, Massachusetts, USA, New York, NY, USA: Association for Computing Machinery, 2010, pp. 715–724, ISBN: 978-1-4503-0050-6. DOI: 10.1145/1806689.1806787. [Online]. Available: https://doi.org/10.1145/1806689.1806787.

[11] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3, pp. 211–407, 2013, ISSN: 1551-305X, 1551-3068. DOI: 10.1561/0400000042. [Online]. Available: http://www.nowpublishers.com/articles/foundations-and-trends-in-theoretical-computer-science/TCS-042 (visited on 01/14/2023).

[12] D. Huang, S. Han, X. Li, and P. S. Yu, "Orthogonal mechanism for answering batch queries with differential privacy," in *Proceedings of the 27th International Conference on Scientific and Statistical Database Management*, ser. SSDBM '15, event-place: La Jolla, California, New York, NY, USA: Association for Computing Machinery, 2015, ISBN: 978-1-4503-3709-0. DOI: 10.1145/2791347.2791378. [Online]. Available: https://doi.org/10.1145/2791347.2791378.

[13] R. J. Wieringa, *Design science methodology for information systems and software engineering*. New York, NY: Springer Berlin Heidelberg, 2014, ISBN: 978-3-662-43838-1.

[14] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, p. 477, Jan. 2006. [Online]. Available: https://papers.ssrn.com/abstract=667622 (visited on 09/23/2021).

[15] J. Brewer and A. Hunter, *Foundations of multimethod research: synthesizing styles*. Thousand Oaks, Calif: Sage Publications, 2006, 206 pp., ISBN: 978-0-7619-8861-8.

[16] S. L. Halverson, "Multimethod approaches," in *The Handbook of Translation and Cognition*, J. W. Schwieter and A. Ferreira, Eds., 1st ed., Wiley, Apr. 19, 2017, pp. 193–212, ISBN: 978-1-119-24143-0 978-1-119-24148-5. DOI: 10.1002/9781119241485.

ch11. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/9781119241485.ch11 (visited on 04/21/2023).

[17] D. Coghlan and M. Brydon-Miller, *The SAGE Encyclopedia of Action Research*. 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd, 2014, ISBN: 978-1-84920-027-1 978-1-4462-9440-6. DOI: 10.4135/9781446294406. [Online]. Available: https://methods.sagepub.com/reference/encyclopedia-of-action-research (visited on 05/02/2023).

[18] K. Lewin, "The research center for group dynamics at massachusetts institute of technology," *Sociometry*, vol. 8, no. 2, p. 126, May 1945, ISSN: 00380431. DOI: 10.2307/2785233. [Online]. Available: https://www.jstor.org/stable/2785233?origin=crossref (visited on 05/02/2023).

[19] J. W. Creswell and J. D. Creswell, *Research design: qualitative, quantitative, and mixed methods approaches*, Fifth edition. Los Angeles: SAGE, 2018, 275 pp., ISBN: 978-1-5063-8670-6.

[20] I. Dinur and K. Nissim, "Revealing information while preserving privacy," in *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, San Diego California: ACM, Jun. 9, 2003, pp. 202–210, ISBN: 978-1-58113-670-8. DOI: 10.1145/773153.773173. [Online]. Available: https://dl.acm.org/doi/10.1145/773153.773173 (visited on 02/14/2024).

[21] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation-TAMC*, ser. Lecture Notes in Computer Science, Edition: Theory and Applications of Models of Computation-TAMC, vol. 4978, Springer Verlag, Apr. 2008, pp. 1–19. [Online]. Available: https://www.microsoft.com/en-us/research/publication/differential-privacy-a-survey-of-results/.

[22] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, S. Halevi and T. Rabin, Eds., red. by D. Hutchison, T. Kanade, J. Kittler, *et al.*, vol. 3876, Series Title: Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, Mar. 4, 2006, pp. 265–284, ISBN: 978-3-540-32731-8 978-3-540-32732-5. DOI: 10.1007/11681878_14. [Online]. Available: http://link.springer.com/10.1007/11681878_14 (visited on 03/02/2023).

[23] P. Kodeswaran and E. Viegas, "Applying differential privacy to search queries in a policy based interactive framework," in *Proceedings of the ACM First International Workshop on Privacy and Anonymity for Very Large Databases*, ser. PAVLAD '09, event-place: Hong Kong, China, New York, NY, USA: Association for Computing Machinery, 2009, pp. 25–32, ISBN: 978-1-60558-804-9. DOI: 10.1145/1651449.1651455. [Online]. Available: https://doi.org/10.1145/1651449.1651455.

[24] S.-S. Ho and S. Ruan, "Differential privacy for location pattern mining," in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ser. SPRINGL '11, event-place: Chicago, Illinois, New York, NY, USA: Association for Computing Machinery, 2011, pp. 17–24, ISBN: 978-1-4503-1032-1. DOI: 10.1145/2071880.2071884. [Online]. Available: https://doi.org/10.1145/2071880.2071884.

[25] R. Chen, N. Mohammed, B. C. M. Fung, B. C. Desai, and L. Xiong, "Publishing set-valued data via differential privacy," *Proc. VLDB Endow.*, vol. 4, no. 11, pp. 1087–1098, Aug. 2011, Publisher: VLDB Endowment, ISSN: 2150-8097. DOI: 10.14778/3402707.3402744. [Online]. Available: https://doi.org/10.14778/3402707.3402744.

[26] G. Barthe, B. Köpf, F. Olmedo, and S. Zanella Béguelin, "Probabilistic relational reasoning for differential privacy," in *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, ser. POPL '12, event-place: Philadelphia, PA, USA, New York, NY, USA: Association for Computing Machinery, 2012, pp. 97–110, ISBN: 978-1-4503-1083-3. DOI: 10.1145/2103656.2103670. [Online]. Available: https://doi.org/10.1145/2103656.2103670.

[27] G. Barthe, B. Köpf, F. Olmedo, and S. Zanella-Béguelin, "Probabilistic relational reasoning for differential privacy," *ACM Trans. Program. Lang. Syst.*, vol. 35, no. 3, Nov. 2013, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 0164-0925. DOI: 10.1145/2492061. [Online]. Available: https://doi.org/10.1145/2492061.

[28] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13, event-place: Berlin, Germany, New York, NY, USA: Association for Computing Machinery, 2013, pp. 901–914, ISBN: 978-1-4503-2477-9. DOI: 10.1145/2508859.2516735. [Online]. Available: https://doi.org/10.1145/2508859.2516735.

[29] F. Kargl, A. Friedman, and R. Boreli, "Differential privacy in intelligent transportation systems," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '13, event-place: Budapest, Hungary, New York, NY, USA: Association for Computing Machinery, 2013, pp. 107–112, ISBN: 978-1-4503-1998-0. DOI: 10.1145/2462096.2462114. [Online]. Available: https://doi.org/10.1145/2462096.2462114.

[30] L. Fan, L. Bonomi, L. Xiong, and V. Sunderam, "Monitoring web browsing behavior with differential privacy," in *Proceedings of the 23rd International Conference on World Wide Web*, ser. WWW '14, event-place: Seoul, Korea, New York, NY, USA: Association for Computing Machinery, 2014, pp. 177–188, ISBN: 978-1-4503-2744-2.

DOI: 10.1145/2566486.2568038. [Online]. Available: https://doi.org/10.1145/2566486.2568038.

[31] M. Jelasity and K. P. Birman, "Distributional differential privacy for large-scale smart metering," in *Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security*, ser. IH&MMSec '14, event-place: Salzburg, Austria, New York, NY, USA: Association for Computing Machinery, 2014, pp. 141–146, ISBN: 978-1-4503-2647-6. DOI: 10.1145/2600918.2600919. [Online]. Available: https://doi.org/10.1145/2600918.2600919.

[32] N. Li, W. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '12, event-place: Seoul, Korea, New York, NY, USA: Association for Computing Machinery, 2012, pp. 32–33, ISBN: 978-1-4503-1648-4. DOI: 10.1145/2414456.2414474. [Online]. Available: https://doi.org/10.1145/2414456.2414474.

[33] F. Tramèr, Z. Huang, J.-P. Hubaux, and E. Ayday, "Differential privacy with bounded priors: Reconciling utility and privacy in genome-wide association studies," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15, event-place: Denver, Colorado, USA, New York, NY, USA: Association for Computing Machinery, 2015, pp. 1286–1297, ISBN: 978-1-4503-3832-5. DOI: 10.1145/2810103.2813610. [Online]. Available: https://doi.org/10.1145/2810103.2813610.

[34] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15, event-place: Denver, Colorado, USA, New York, NY, USA: Association for Computing Machinery, 2015, pp. 1298–1309, ISBN: 978-1-4503-3832-5. DOI: 10.1145/2810103.2813640. [Online]. Available: https://doi.org/10.1145/2810103.2813640.

[35] Y. Xiao, L. Xiong, S. Zhang, and Y. Cao, "LocLok: Location cloaking with differential privacy via hidden markov model," *Proc. VLDB Endow.*, vol. 10, no. 12, pp. 1901–1904, Aug. 2017, Publisher: VLDB Endowment, ISSN: 2150-8097. DOI: 10.14778/3137765.3137804. [Online]. Available: https://doi.org/10.14778/3137765.3137804.

[36] B. Yang, I. Sato, and H. Nakagawa, "Bayesian differential privacy on correlated data," in *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '15, event-place: Melbourne, Victoria, Australia, New York, NY, USA: Association for Computing Machinery, 2015, pp. 747–762, ISBN: 978-1-4503-2758-9. DOI: 10.1145/2723372.2747643. [Online]. Available: https://doi.org/10.1145/2723372.2747643.

[37] M. Abadi, A. Chu, I. Goodfellow, *et al.*, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna Austria: ACM, Oct. 24, 2016, pp. 308–318, ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978318. [Online]. Available: https://dl.acm.org/doi/10.1145/2976749.2978318 (visited on 05/02/2023).

[38] X. He, A. Machanavajjhala, C. Flynn, and D. Srivastava, "Composing differential privacy and secure computation: A case study on scaling private record linkage," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17, event-place: Dallas, Texas, USA, New York, NY, USA: Association for Computing Machinery, 2017, pp. 1389–1406, ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3134030. [Online]. Available: https://doi.org/10.1145/3133956.3134030.

[39] F. Fioretto, C. Lee, and P. Van Hentenryck, "Constrained-based differential privacy for mobility services," in *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, ser. AAMAS '18, event-place: Stockholm, Sweden, Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2018, pp. 1405–1413. DOI: 10.5555/3237383.3237910.

[40] S. Ghane, L. Kulik, and K. Ramamohanarao, "Publishing spatial histograms under differential privacy," in *Proceedings of the 30th International Conference on Scientific and Statistical Database Management*, ser. SSDBM '18, event-place: Bozen-Bolzano, Italy, New York, NY, USA: Association for Computing Machinery, 2018, ISBN: 978-1-4503-6505-5. DOI: 10.1145/3221269.3223039. [Online]. Available: https://doi.org/10.1145/3221269.3223039.

[41] A. Evfimievski, J. Gehrke, and R. Srikant, "Limiting privacy breaches in privacy preserving data mining," in *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, San Diego California: ACM, Jun. 9, 2003, pp. 211–222, ISBN: 978-1-58113-670-8. DOI: 10.1145/773153.773174. [Online]. Available: https://dl.acm.org/doi/10.1145/773153.773174 (visited on 07/15/2023).

[42] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, Philadelphia, PA, USA: IEEE, Oct. 2008, pp. 531–540, ISBN: 978-0-7695-3436-7. DOI: 10.1109/FOCS.2008.27. [Online]. Available: http://ieeexplore.ieee.org/document/4690986/ (visited on 07/15/2023).

[43] Y. Guo and Y. Gong, "Practical collaborative learning for crowdsensing in the internet of things with differential privacy," in *2018 IEEE Conference on Communications and Network Security (CNS)*, May 2018, pp. 1–9. DOI: 10.1109/CNS.2018.8433181.

[44] X. Liu, Y. Guo, Y. Chen, and X. Tan, "Trajectory privacy protection on spatial streaming data with differential privacy," in *2018 IEEE Global Communications Conference (GLOBECOM)*, ISSN: 2576-6813, Dec. 2018, pp. 1–7. DOI: 10.1109/GLOCOM.2018.8647918.

[45] U. Erlingsson, V. Feldman, I. Mironov, A. Raghunathan, K. Talwar, and A. Thakurta, "Amplification by shuffling: From local to central differential privacy via anonymity," in *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, ser. SODA '19, event-place: San Diego, California, USA: Society for Industrial and Applied Mathematics, 2019, pp. 2468–2479. DOI: 10.5555/3310435.3310586.

[46] X. Zhang, Q. Chen, X. Peng, and X. Jiang, "Differential privacy-based indoor localization privacy protection in edge computing," in *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Aug. 2019, pp. 491–496. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00125.

[47] D. Zhao, H. Chen, S. Zhao, X. Zhang, C. Li, and R. Liu, "Local differential privacy with k-anonymous for frequency estimation," in *2019 IEEE International Conference on Big Data (Big Data)*, Dec. 2019, pp. 5819–5828. DOI: 10.1109/BigData47090.2019.9006022.

[48] M. Mohammady, S. Xie, Y. Hong, *et al.*, "R2dp: A universal and automated approach to optimizing the randomization mechanisms of differential privacy for utility metrics with no known optimal distributions," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20, event-place: Virtual Event, USA, New York, NY, USA: Association for Computing Machinery, 2020, pp. 677–696, ISBN: 978-1-4503-7089-9. DOI: 10.1145/3372297.3417259. [Online]. Available: https://doi.org/10.1145/3372297.3417259.

[49] H. Zhen, B.-C. Chiou, Y.-T. Tsou, S.-Y. Kuo, and P.-C. Wang, "Association rule mining with differential privacy," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, ISSN: 2325-6664, Jun. 2020, pp. 47–54. DOI: 10.1109/DSN-W50199.2020.00017.

[50] J.-H. Hoepman, *Privacy Design Strategies (The Little Blue Book)*. Jan. 27, 2020.

[51] Jianneng Cao, B Carminati, E Ferrari, and Kian-Lee Tan, "CASTLE: Continuously anonymizing data streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp. 337–352, May 2011, ISSN: 1545-5971. DOI: 10.1109/TDSC.2009.47. [Online]. Available: http://ieeexplore.ieee.org/document/5374415/ (visited on 07/17/2023).

[52] T. Wang, J. Q. Chen, Z. Zhang, *et al.*, "Continuous release of data streams under both centralized and local differential privacy," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '21, event-place: Virtual Event, Republic of Korea, New York, NY, USA: Association for Computing Machinery, 2021, pp. 1237–1253, ISBN: 978-1-4503-8454-4. DOI: 10.1145/3460120.3484750. [Online]. Available: https://doi.org/10.1145/3460120.3484750.

[53] J. Zhao, J. Mei, S. Matwin, Y. Su, and Y. Yang, "Risk-aware individual trajectory data publishing with differential privacy," *IEEE Access*, vol. 9, pp. 7421–7438, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3048394.

[54] Y.-T. Tsou, H.-L. Chen, and J.-Y. Chen, "RoD: Evaluating the risk of data disclosure using noise estimation for differential privacy," *IEEE Transactions on Big Data*, vol. 7, no. 1, pp. 214–226, Mar. 2021, ISSN: 2332-7790. DOI: 10.1109/TBDATA.2019.2916108.

[55] J. Domingo-Ferrer and J. Soria-Comas, "From t-closeness to differential privacy and vice versa in data anonymization," *Knowledge-Based Systems*, vol. 74, pp. 151–158, Jan. 1, 2015, ISSN: 0950-7051. DOI: 10.1016/j.knosys.2014.11.011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950705114004031.

[56] E. Bao, Y. Yang, X. Xiao, and B. Ding, "CGM: An enhanced mechanism for streaming data collection with local differential privacy," *Proc. VLDB Endow.*, vol. 14, no. 11, pp. 2258–2270, Jul. 2021, Publisher: VLDB Endowment, ISSN: 2150-8097. DOI: 10.14778/3476249.3476277. [Online]. Available: https://doi.org/10.14778/3476249.3476277.

[57] Y. Chen, A. Machanavajjhala, M. Hay, and G. Miklau, "PeGaSus: Data-adaptive differentially private stream processing," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas Texas USA: ACM, Oct. 30, 2017, pp. 1375–1388, ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3134102. [Online]. Available: https://dl.acm.org/doi/10.1145/3133956.3134102 (visited on 07/22/2023).

[58] T. Cunningham, G. Cormode, H. Ferhatosmanoglu, and D. Srivastava, "Real-world trajectory sharing with local differential privacy," *Proc. VLDB Endow.*, vol. 14, no. 11, pp. 2283–2295, Jul. 2021, Publisher: VLDB Endowment, ISSN: 2150-8097. DOI: 10.14778/3476249.3476280. [Online]. Available: https://doi.org/10.14778/3476249.3476280.

[59] J. Near and D. Darais. "Differential privacy: Future work & open challenges," NIST. Last Modified: 2022-01-24T12:00-05:00. (Jan. 24, 2022), [Online]. Available: https:

//www.nist.gov/blogs/cybersecurity-insights/differential-privacy-future-work-open-challenges (visited on 06/13/2022).

[60] A. Aleroud, F. Yang, S. C. Pallaprolu, Z. Chen, and G. Karabatis, "Anonymization of network traces data through condensation-based differential privacy," *Digital Threats*, vol. 2, no. 4, Oct. 2021, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 2692-1626. DOI: 10.1145/3425401. [Online]. Available: https://doi.org/10.1145/3425401.

[61] J. Cox. "How data brokers sell access to the backbone of the internet," Vice. (Aug. 24, 2021), [Online]. Available: https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru (visited on 07/22/2023).

[62] M. Katsomallos, K. Tzompanaki, and D. Kotzinos, "Landmark privacy: Configurable differential privacy protection for time series," in *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '22, event-place: Baltimore, MD, USA, New York, NY, USA: Association for Computing Machinery, 2022, pp. 179–190, ISBN: 978-1-4503-9220-4. DOI: 10.1145/3508398.3511501. [Online]. Available: https://doi.org/10.1145/3508398.3511501.

[63] X. Ren, L. Shi, W. Yu, S. Yang, C. Zhao, and Z. Xu, "LDP-IDS: Local differential privacy for infinite data streams," in *Proceedings of the 2022 International Conference on Management of Data*, ser. SIGMOD '22, event-place: Philadelphia, PA, USA, New York, NY, USA: Association for Computing Machinery, 2022, pp. 1064–1077, ISBN: 978-1-4503-9249-5. DOI: 10.1145/3514221.3526190. [Online]. Available: https://doi.org/10.1145/3514221.3526190.

[64] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias, "Differentially private event sequences over infinite streams," *Proceedings of the VLDB Endowment*, vol. 7, no. 12, pp. 1155–1166, Aug. 2014, ISSN: 2150-8097. DOI: 10.14778/2732977.2732989. [Online]. Available: https://dl.acm.org/doi/10.14778/2732977.2732989 (visited on 07/22/2023).

[65] E. Yilmaz, T. Ji, E. Ayday, and P. Li, "Genomic data sharing under dependent local differential privacy," in *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '22, event-place: Baltimore, MD, USA, New York, NY, USA: Association for Computing Machinery, 2022, pp. 77–88, ISBN: 978-1-4503-9220-4. DOI: 10.1145/3508398.3511519. [Online]. Available: https://doi.org/10.1145/3508398.3511519.

[66] L. Yao, Z. Chen, H. Hu, G. Wu, and B. Wu, "Privacy preservation for trajectory publication based on differential privacy," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 3, Apr. 2022, ISSN: 2157-6904. DOI: 10.1145/3474839. [Online]. Available: https://doi.org/10.1145/3474839.

[67] R. T. Rockafellar and R. J.-B. Wets, *Variational analysis* (Grundlehren der mathematischen Wissenschaften 317), Corr. 2nd print. Berlin: Springer, 2004, 734 pp., ISBN: 978-3-540-62772-2.

[68] H. H. Arcolezi, S. Gambs, J.-F. Couchot, and C. Palamidessi, "On the risks of collecting multidimensional data under local differential privacy," *Proc. VLDB Endow.*, vol. 16, no. 5, pp. 1126–1139, Jan. 2023, Publisher: VLDB Endowment, ISSN: 2150-8097. DOI: 10.14778/3579075.3579086. [Online]. Available: https://doi.org/10.14778/3579075.3579086.

[69] F. Z. Errounda and Y. Liu, "An analysis of differential privacy research in location data," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, May 2019, pp. 53–60. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00021.

[70] J. W. Kim, D.-H. Kim, and B. Jang, "Application of local differential privacy to collection of indoor positioning data," *IEEE Access*, vol. 6, pp. 4276–4286, 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2791588. [Online]. Available: http://ieeexplore.ieee.org/document/8253434/ (visited on 07/16/2023).

[71] V. Goel, D. Mahajan, M.-C. Nadeau, O. Sperling, and S. Yeh. "New trends in US consumer digital payments," McKinsey & Company. (Oct. 26, 2021), [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/new-trends-in-us-consumer-digital-payments (visited on 05/02/2023).

[72] Business Insider. "The current state of online banking," Business Insider. (May 10, 2021), [Online]. Available: https://www.businessinsider.com/current-state-of-online-banking-industry (visited on 05/02/2023).

[73] R. Shevlin. "Mobile banking adoption in the united states has skyrocketed (but so have fraud concerns)," Forbes. Section: Fintech. (Jul. 29, 2021), [Online]. Available: https://www.forbes.com/sites/ronshevlin/2021/07/29/mobile-banking-adoption-has-skyrocketed-but-so-have-fraud-concerns-what-can-banks-do/ (visited on 05/02/2023).

[74] *Unbanked: What it means to be outside of the banking system*, in collab. with D. Standaert, N. Camper, D. Karlan, and K. Perez, Apr. 5, 2021. [Online]. Available: https://www.npr.org/2021/04/05/984475870/unbanked-what-it-means-to-be-outside-of-the-banking-system (visited on 05/02/2023).

[75] C. Canonne. "What is delta, and what difference does it make?" (Mar. 11, 2021), [Online]. Available: https://differentialprivacy.org/flavoursofdelta/ (visited on 05/03/2023).

[76] K. Coyle, L. Kim, and S. O'Brien. "2021 findings from the diary of consumer payment choice - cash," San Francisco Fed. (May 5, 2021), [Online]. Available: https://www.frbsf.org/cash/publications/fed-notes/2021/may/2021-findings-from-the-diary-of-consumer-payment-choice/ (visited on 05/03/2023).

[77] "OpenDP." (Feb. 8, 2024), [Online]. Available: https://opendp.org/home (visited on 04/04/2024).

[78] N. Fernandes, A. McIver, and C. Morgan, "The laplace mechanism has optimal utility for differential privacy over continuous queries," in *Proceedings of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science*, ser. LICS '21, event-place: Rome, Italy, New York, NY, USA: Association for Computing Machinery, 2021, ISBN: 978-1-66544-895-6. DOI: 10.1109/LICS52264.2021.9470718. [Online]. Available: https://doi.org/10.1109/LICS52264.2021.9470718.

[79] X. D. Zhang, "Strictly standardized mean difference, standardized mean difference and classical t -test for the comparison of two groups," *Statistics in Biopharmaceutical Research*, vol. 2, no. 2, pp. 292–299, May 2010, ISSN: 1946-6315. DOI: 10.1198/sbr.2009.0074. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1198/sbr.2009.0074 (visited on 04/03/2024).

[80] X. D. Zhang, "A pair of new statistical parameters for quality control in RNA interference high-throughput screening assays," *Genomics*, vol. 89, no. 4, pp. 552–561, Apr. 2007, ISSN: 08887543. DOI: 10.1016/j.ygeno.2006.12.014. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0888754307000079 (visited on 04/03/2024).

[81] X. D. Zhang, *Optimal high-throughput screening: practical experimental design and data analysis for genome-scale RNAi research*. Cambridge: Cambridge University Press, 2011, 203 pp., ISBN: 978-0-521-51771-3 978-0-521-73444-8.

[82] X. D. Zhang, "A method for effectively comparing gene effects in multiple conditions in RNAi and expression-profiling research," *Pharmacogenomics*, vol. 10, no. 3, pp. 345–358, Mar. 2009, ISSN: 1462-2416, 1744-8042. DOI: 10.2217/14622416.10.3.345. [Online]. Available: https://www.tandfonline.com/doi/full/10.2217/14622416.10.3.345 (visited on 11/08/2024).

[83] R. E. Kirk, "Practical significance: A concept whose time has come," *Educational and Psychological Measurement*, vol. 56, no. 5, pp. 746–759, Oct. 1996, ISSN: 0013-1644, 1552-3888. DOI: 10.1177/0013164496056005002. [Online]. Available: https://journals.sagepub.com/doi/10.1177/0013164496056005002 (visited on 11/08/2024).

[84] X. D. Zhang, "A new method with flexible and balanced control of false negatives and false positives for hit selection in RNA interference high-throughput screening

assays," *SLAS Discovery*, vol. 12, no. 5, pp. 645–655, Aug. 2007, ISSN: 24725552. DOI: 10.1177/1087057107300645. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2472555222083575 (visited on 11/08/2024).

[85] R. A. Finkel and J. L. Bentley, "Quad trees a data structure for retrieval on composite keys," *Acta Informatica*, vol. 4, no. 1, pp. 1–9, 1974, ISSN: 0001-5903, 1432-0525. DOI: 10.1007/BF00288933. [Online]. Available: http://link.springer.com/10.1007/BF00288933 (visited on 01/04/2025).

[86] F. Bartolucci, A. Farcomeni, and F. Pennoni, *Latent Markov models for longitudinal data* (Chapman & Hall/CRC statistics in the social and behavioral sciences). Boca Raton, FL: CRC Press, Taylor & Francis Group, 2013, 234 pp., ISBN: 978-1-4398-1708-7.

[87] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, "Guidelines for media sanitization," National Institute of Standards and Technology, NIST SP 800-88r1, Dec. 2014, NIST SP 800–88r1. DOI: 10.6028/NIST.SP.800-88r1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (visited on 01/05/2025).

[88] R. Wieringa and A. Moralı, "Technical action research as a validation method in information systems design science," in *Design Science Research in Information Systems. Advances in Theory and Practice*, K. Peffers, M. Rothenberger, and B. Kuechler, Eds., red. by D. Hutchison, T. Kanade, J. Kittler, *et al.*, vol. 7286, Series Title: Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 220–238, ISBN: 978-3-642-29862-2 978-3-642-29863-9. DOI: 10.1007/978-3-642-29863-9_17. [Online]. Available: http://link.springer.com/10.1007/978-3-642-29863-9_17 (visited on 02/08/2025).

[89] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*, Fourth edition. Cambridge, Massachusett: The MIT Press, 2022, 1291 pp., ISBN: 978-0-262-04630-5.

[90] Z. Li, H. Wang, G. Xu, *et al.*, "Privacy-preserving distributed transfer learning and its application in intelligent transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 3, pp. 2253–2269, Mar. 2024, ISSN: 1524-9050, 1558-0016. DOI: 10.1109/TITS.2022.3215325. [Online]. Available: https://ieeexplore.ieee.org/document/9932639/ (visited on 02/08/2025).