Three-way optimization of privacy and utility of location data

1st Sayan Biswas
INRIA, LIX, École Polytechnique
Palaiseau, France
sayan.biswas@inria.fr

2nd Catuscia Palamidessi
INRIA, LIX, École Polytechnique
Palaiseau, France
catuscia@lix.polytechnique.fr

Abstract—With the recent bloom of data and the drive towards an information-based society, the urge of and the advancements in data analytics is surging like never before. And with this, the risks of privacy violation of various kinds are also increasing manifold. Most of the methods to mitigate the privacy risks for location data resort to adding some noise to the location, like the planar Laplace used to achieve geo-indistinguishability. However, the noise should be calibrated carefully, taking into account the implications for utility, because it is far from ideal for the service providers to completely lose the utility of the collected data succumbing to the privacy requirements of the users. Similarly, the quality of service for the users should be optimized with their personalized needs of privacy protection used to shield their sensitive information. In this paper, we address this age-old battle between privacy and utility from three ends: privacy of the users’ data, the quality of service (QoS) received by them in exchange for sharing their privatized data, and the statistical utility of the privatized data for the service providers who wish to perform various kinds of analysis and research on the data collected from the users. We propose a method to produce a geo-indistinguishable location-privacy mechanism that advances to optimize simultaneously between the level of privacy attained, the QoS, and the statistical utility achieved by the obfuscated data. We illustrate the soundness of this three-way privacy-utility optimization mechanism both analytically and with experiments. Apart from the novelty of the proposed method, this work is aimed to engender an analytical perspective to bridge between geo-indistinguishable location-privacy, QoS, and statistical utilities used in standard data analytics, from an information theoretical, probabilistic, and statistical perspective.

Index Terms—Location Privacy, Information Theory, Privacy-Utility Optimization, Probability Theory.

I. INTRODUCTION

As the need and advancements of various kinds of analysis and research using sensitive personal data are becoming more and more popular and significant, the risk of privacy violations is also increasing manifold. One of the most successful proposals to address the issue of privacy protection is differential privacy (DP) [1], [2], a mathematical property that makes it difficult for an attacker to detect the presence of a record in a dataset, and which is typically achieved by adding noise to the results of queries performed on the dataset. With advancements in research, the local variation of differential privacy (LDP) [3] has gained substantial popularity in the community, thanks to the fact that the noise is applied at the user’s end and therefore it does not need a trusted curator. The local model of privacy is particularly suitable for the situations in which the user communicates her personal data in exchange for some service. One such scenario is the use of location-based services (LBS), where the user typically sends her location in exchange for information like the shortest path to a destination, points of interest in the surroundings, traffic information, friends nearby, etc. The local model of differential privacy can be implemented directly on the user’s device (tablet, smartphone, etc.) and the fact that the user can control directly her privacy-protection mechanism is very appealing. However, the drawback of injecting noise locally to the datum is that it decreases also the utility from the perspective of the user (besides that of the data collector) because the quality of service (QoS) is usually affected negatively by the lack of accuracy of the data. Therefore, in the local model of privacy protection, taking into account the utility of the data both on the users’ and the service providers’ sides is essential.

A lot of research has been done to address the privacy-utility trade-off in the local model of privacy. In standard LDP, typically the focus is on optimizing the utility from the point of view of the data collector, i.e., devising mechanisms and post-processing methods that would allow deriving maximally accurate statistics from the collection of the noisy data [3], [4]. Statistical precision is essential for various kinds of studies and analytics performed by data consumers, for reasons including and not limited to improving and upgrading the standard of service, providing useful statistics to companies and research institutions, training machine learning models [4], [5], etc.

In contrast to the above, in other domains, such as location-privacy, the focus is usually on optimizing the QoS, i.e., the utility from the point of view of the user. Notably, this is the case for the framework proposed by Shokri et al. [6], [7], and for geo-indistinguishability [8], a variant of LDP that takes into account the distance between locations [9], [10]. The preservation of the best possible quality of service despite the obfuscation operated on the data is what motivates these efforts.

Notably, the optimization of statistical utility does not necessarily imply a substantial improvement in the QoS, nor vice-versa (although they go in the same direction, in the sense that both tend to preserve as much as possible the original information, under the privacy constraint). A counterexample is provided by Example II.1 in the Related Work Section.
Thus, we acknowledge and appreciate the existence of a three-way entanglement between the privacy level of the obfuscation, the QoS that is still fostered by a datum after being obfuscated, and the statistical information that can be extracted from a collection of such obfuscated data. To the best of our knowledge, the problem of devising a privacy-protection mechanism that optimizes at the same time the users’ QoS and the statistical utility, has never been addressed by the research community.

In this paper, we aim to explore this three-way conflict between privacy and the two kinds of utility, and we propose a method to find a mechanism for location-privacy that satisfies geo-indistinguishability and strives towards optimizing this triadic privacy-utility trade-off. We use information-theoretic notions to quantify location-privacy and QoS (mutual information and distortion, respectively), and a statistical notion (the divergence between distributions) to quantify statistical utility. Since the data distribution is typically unknown, we start by assuming a uniform distribution, and find the Pareto-optimal channel between privacy and QoS for this uniform distribution, using the Blahut-Arimoto algorithm (that, indeed, depends on the input distribution). Using this channel as an obfuscation mechanism, we let the user obfuscate their data and collect them. Then we post-process these obfuscated data to best estimate the original distribution, using an expectation-maximization (EM) method known as the iterative Bayesian update. We then repeat this procedure starting, this time, from the estimated original distribution, in order to get a channel with a better Pareto-optimality (between privacy and QoS) in the sense that it is for a distribution closer to the true one. Continuing to repeat this procedure, we get a more and more refined channel and a better and better estimation of the true distribution. We formally prove the convergence of our method by providing a probabilistic characterization of its limiting behaviour via translating our model into a Markov chain. The convergence then comes as a consequence of the unique probability distribution property of Markov chains. We also validate this result experimentally.

In the process of establishing the soundness of our method, we have also proved various desirable mathematical properties, like its uniform continuity. Most notably, we have discovered that the two seemingly unrelated algorithms mentioned above, the Blahut-Arimoto and the iterative Bayesian update, are actually duals of each other, thus establishing a bridge between the QoS and the statistical notion of utility.

Finally, we perform experiments on real location data from the Gowalla datasets for San Francisco and Paris, and empirically show the convergence of our method and the achievement of a three-way optimality between privacy, QoS, and statistical utility, thus confirming the theoretical results. The experiments also show the efficacy of the combination of the proposed mechanism and the post-processing method (the iterative Bayesian update), in that the estimation of the original distribution is very accurate, especially when measured using a notion of distance between distribution compatible with the ground distance used to measure the QoS. Namely, the Earth Mover’s distance.

In summary, the contribution of this paper is as follows:

1) We propose an iterative method (Optima3) that produces a geo-indistinguishable privacy mechanism which maximizes the privacy of the users under a given threshold for QoS and provides a very accurate statistical estimation of the distribution of the original data (i.e., the most likely original distribution), thus advancing towards a three-way optimization of privacy and utility.

2) We prove that Optima3 is uniformly continuous and show its convergence by translating it into the framework of Markov chains. We confirm with experiments on real data that Optima3 has the desired behaviour.

3) We show that the Blahut-Arimoto algorithm and the iterative Bayesian update are duals of each other, thus establishing a connection between the information-theoretic field of Rate-Distortion Theory and the Statistical EM method.

The paper is organized as follows: Section II discusses some related work. Section III introduces some preliminary notions related to privacy and various information theoretical concepts relevant to our work. Section IV illustrates the duality between Blahut-Arimoto algorithm and iterative Bayesian update. Section V lays the foundation to our method. Section VI demonstrates the translation of our method to the framework of Markov chains to study its limiting behaviour. Section VII is dedicated to the mathematical soundness of our proposed method, illustrating, with proof, some desirable mathematical properties it satisfies. Section VIII exhibits the experimental results using Gowalla check-in data from Paris and San Francisco, reassuring that our method converges and engenders a geo-indistinguishable privacy channel that achieves a three-way privacy-utility optimality. In Section IX, we present the conclusion.

II. RELATED WORK

The clash between privacy and utility has been brought to attention and widely studied in the literature [11], [12]. Optimization techniques for differential privacy and utility in the context of statistical databases have been intensively analyzed from various perspectives and have been investigated by the community in the recent past [13]–[15]. There has been some recent work focusing on devising privacy mechanisms that are optimal to limit the privacy risk against Bayesian inference attacks while maximizing the utility [6], [7]. In [16] Oya et al. examine a two-way optimal location-privacy preserving mechanism and analyse it with respect to different privacy and utility metrics.

In [17], Oya et al. consider the idea of the optimal location-privacy preserving mechanisms (LPPM) proposed by Shokri et al.
al. in [6], which maximize the average adversary error (used as the notion of privacy) under some bound on the QoS loss. Oya et al. [17] then use the EM method to design blank-slate models that they empirically show to outperform the traditional hardwired models. However, a fundamental problem with this approach is that there can exist LPPMs which are optimal in the sense of [6], but the EM method would fail to converge or would not give sensible results. Such examples have been explored by ElSalamouny et al. in Section II, of [18]. Indeed, [18] points out the several mistakes in the theoretical results of [19], which Oya et al. intrinsically rely on, in order to prove the convergence of their proposed method in [17].

Example II.1. An example of a location-privacy mechanism that achieves Shokri et al.’s optimality in terms of QoS, but has no statistical utility at all, is the following. Consider three locations that achieve Shokri et al.’s optimality in terms of QoS, but would not give sensible results. Such examples have been explored by ElSalamouny et al. in Section II, of [18]. Indeed, [18] points out the several mistakes in the theoretical results of [19], which Oya et al. intrinsically rely on, in order to prove the convergence of their proposed method in [17].

The metrics we considered for privacy, QoS and statistical utility are fairly standard in the literature. A typical information theoretic quantification of privacy is done using mutual information (MI) (a.k.a. conditional entropy) between the original and the noisy data exploiting the compatible relationship between MI and DP [20]. The approach to measure privacy with MI is widespread in the literature: to gauge anonymity [21], [22], to estimate privacy in machine learning complementing typical loss function used for training, i.e., cross entropy [23]–[26], to assess location-privacy [16].

Different metrics to measure QoS for the users have been proposed and studied of late. One of the most popular choices of such a utility-metric to measure quality loss established by a privacy mechanism is the average loss or average distortion, quantifying how much quality a user loses on average, with respect to a chosen metric. This notion has gained the spotlight recently in the community [6], [8], [27]–[29] since it is the most intuitive notion of QoS.

A standard approach to determine the statistical utility of a dataset privatized with an LDP mechanism is by estimating the distribution of the original data from that of the noisy data. One of the most flexible and powerful techniques to do this is by using the EM method of iterative Bayesian update (IBU) [19], [30] that have been studied and analyzed recently [18], [31].

In the quest of resolving this triadic face-off of privacy, QoS, and statistical utility, in this paper, we aim to engender a privacy channel that maximizes MI, which we use to measure privacy for location data, for an allowed threshold of average distortion, which we used to represent the quality loss, and re-construct the distribution of the original data using an EM method like the IBU.

III. Preliminaries

A. Standard notions of privacy

Definition III.1 (Differential privacy [1], [2]). For a certain query, a randomizing mechanism $R$ provides $\epsilon$-differential privacy (DP) if, for all neighboring $X'$ datasets, $D$ and $D'$, and all $S \subseteq \text{Range}(R)$, we have

$$P[R(D) \in S] \leq e^\epsilon P[R(D') \in S]$$

Definition III.2 (Local differential privacy [3]). Let $X'$ and $Y$ denote the spaces of original and noisy data, respectively. A randomizing mechanism $R$ provides $\epsilon$-local differential privacy (LDP) if, for all $x, x' \in X'$, and all $y \in Y$, we have

$$P[R(x) = y] \leq e^{\epsilon} P[R(x') = y]$$

Definition III.3 (Geo-indistinguishability [3]). Let $X$ be a space of locations and let $d_{E}(x, x')$ denote the Euclidean distance between $x \in X'$ and $x' \in X$. A randomizing mechanism $R$ is $\epsilon$-geo-indistinguishable if for all $x, x_2 \in X$, and every $y \in X'$, we have

$$P[R(x) = y] \leq e^{\epsilon d_{E}(x_1, x_2)} P[R(x') = y]$$

Definition III.4 (Mutual information [32]). Let $(X, Y)$ be a pair of random variables defined over the discrete space $X \times Y$. The mutual information (MI) of $X$ and $Y$ is given as:

$$MI(X, Y) = \sum_{x \in X} \sum_{y \in Y} \mu(x, y) \log \frac{\mu(x, y)}{p_X(x)p_Y(y)}$$

where $\mu$ is the joint PMF of $X$ and $Y$, and $p_X$ and $p_Y$ are the marginal PMFs of $X$ and $Y$, respectively.

Remark 1. In the context of the location-privacy, we obfuscate the original locations to other locations in the same space. In other words, we consider the space of the original and the noisy data to be the same, i.e., $X = Y$.

B. Notion of utility

Definition III.5 (Quality of service). For a discrete space of locations, $X$, let $d : X \times X \rightarrow \mathbb{R}_{\geq 0}$ be any distortion (loss) metric. Let $X$ be a random variable on $X$ with PMF $p_X$, and let $C$ denote any randomizing location-privacy mechanism with $C_{x|x'}$ giving the probability of a location $x$ being obfuscated as location $x'$, i.e., $C_{x|x'} = P(x'|x)$ for every $x, x' \in X$.

We define the quality of service (QoS) of $X$ for $C$ as the average distortion w.r.t the loss function $d$,

$$\text{AvgDist}(X, C, d) = \sum_{x \in X} \sum_{x' \in X} p_X(x)C_{x|x'}d(x, x')$$

\(^3\)differing in exactly one place
Definition III.6 (Full-support probability distribution). Let $\theta$ be a probability distribution defined on the space $\mathcal{X}$. We call $\theta$ to be a full-support distribution on $\mathcal{X}$ if $\theta(x) > 0$ for every $x \in \mathcal{X}$.

Definition III.7 (Iterative Bayesian update [19]). Let $\mathcal{C}$ be a privacy mechanism that locally obfuscates locations on the discrete space $\mathcal{X}$ such that $C_{xx'} = \mathbb{P}(x' | x)$ for all $x, x' \in \mathcal{X}$. Let $X_1, \ldots, X_n$ be i.i.d. random variables on $\mathcal{X}$ following some PMF $\pi_X$. Let $Y_i$ denote the random variable of the output when $X_i$ is obfuscated with $\mathcal{C}$ for all $i \in \{1, \ldots, n\}$.

Suppose we have a realisation $y = \{y_1, \ldots, y_n\}$ of $Y = \{Y_1, \ldots, Y_n\}$ produced with $\mathcal{C}$. Let $q = \{q(x) : x \in \mathcal{X}\}$ be the empirical distribution of the locations obtained from the observed $y$. Then the iterative Bayesian update (IBU) presents an iterative EM procedure that aims to estimate $\pi_X$ by converging to the maximum likelihood estimate (MLE) for the observed locations under the given mechanism. IBU works as follows:

1) Start with any full-support PMF $\theta_0$ on $\mathcal{X}$ as an “initial guess”.
2) Iterate:

$$\theta_{t+1}(x) = \sum_{x' \in \mathcal{X}} q(x') \frac{\theta_t(x) C_{xx'}}{\sum_{z \in \mathcal{X}} \theta_t(z) C_{xz}}$$

for all $x \in \mathcal{X}$.

The convergence of IBU has been studied in [19] and revised in [18]. In the cases where IBU converges to a MLE, the limiting estimate of $\pi_X$ be called $\hat{\pi}_X$, i.e., $\hat{\pi}_X = \lim_{t \to \infty} \theta_t$, and as, for an observed set of noisy locations, it is determined completely with the privatizing mechanism $\mathcal{C}$ and the starting PMF $\theta_0$, let $\lim_{t \to \infty} \theta_t$ be functionally denoted as $\Gamma_{\text{IBU}}(\theta_0, \mathcal{C})$.

Definition III.8 (Earth mover’s distance [33]). Let $\pi_1$ and $\pi_2$ be PMFs defined over a discrete space of locations, $\mathcal{X}$. For a metric $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$, the earth mover’s distance (EMD) or the Kantorovich–Rubinstein metric is defined as:

$$\text{EMD}((\pi_1, \pi_2)) = \min_{\mu \in \Pi(\pi_1, \pi_2)} \int_{\mathcal{X} \times \mathcal{X}} d(x, y) \, d\mu(x, y)$$

where $\Pi(\pi_1, \pi_2)$ is the set of all joint distributions over $\mathcal{X} \times \mathcal{X}$ whose marginals are $\pi_1$ and $\pi_2$, i.e., $\int_{\mathcal{X} \times \mathcal{X}} \eta(x_0, x) = \pi_1(x_0)$ and $\int_{\mathcal{X} \times \mathcal{X}} \eta(x, x_0) = \pi_2(x)$ for every $x_0 \in \mathcal{X}$.

Definition III.9 (Statistical utility). Suppose we have a privacy mechanism $\mathcal{C}$ that obfuscates location data on the discrete space $\mathcal{X}$. Let $\pi_X$ be the PMF of the original location data sampled from $\mathcal{X}$ and let $\hat{\pi}_X$ be the PMF on $\mathcal{X}$ which estimates of $\pi_X$ using IBU for the mechanism $\mathcal{C}$. Then we define the statistical utility of the privacy mechanism $\mathcal{C}$ as $\emdf(\hat{\pi}_X, \pi_X)$.

C. Optimization of privacy and QoS

We recall that in this work we use mutual information to measure privacy and average distortion to measure QoS of a certain privacy mechanism. Therefore, to optimize privacy and QoS, we wish to find a privacy channel that minimizes mutual information (i.e., maximizes privacy) under an allowed level of average distortion. This optimization problem can be solved using the well-known Blahut-Arimoto algorithm [34, 35].

Definition III.10 (Rate-distortion function [32]). Let $\mathcal{X}$ and $\mathcal{Y}$ be a pair of discrete spaces and $C(\mathcal{X}, \mathcal{Y})$ be the space of all channels encoding from $\mathcal{X}$ to $\mathcal{Y}$. Suppose $X$ is a random variable defined over $\mathcal{X}$ and fix a $d \in \mathbb{R}_+^+$.

The rate-distortion (RD) function for $X$ and $d$ under the distortion metric $d(.)$ is defined as:

$$RD(X, d^*) = \min_{C \in \mathcal{C}(\mathcal{X}, \mathcal{Y})} \frac{\mathbb{E}_{Y \sim C(X)} [\text{MI}(X, Y, C)]}{\text{AvgD}(X, C, d) \leq d^*}$$

where $Y_{X,C}$ is the random variable on $\mathcal{Y}$ that denotes the output of the encoding of $X$ with any $C \in \mathcal{C}(\mathcal{X}, \mathcal{Y})$.

Definition III.11 (Blahut-Arimoto algorithm [34, 35]). Let $X$ be a random variable on the discrete space of locations $\mathcal{X}$ with a PMF $\pi_X$. For a metric $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$, we wish to find a channel $\hat{C} \in \mathcal{C}(\mathcal{X}, \mathcal{X})$ giving $RD(X, d^*)$. In other words, we wish to find a channel $\hat{C}$ such that:

$$\hat{C} = \arg \min_{C \in \mathcal{C}(\mathcal{X}, \mathcal{Y})} \frac{\mathbb{E}_{Y \sim C(X)} [\text{MI}(X, Y, C)]}{\text{AvgD}(X, C, d) \leq d^*}$$

where $\mathcal{C}$ and $Y_{X,C}$ are the same as in Definition III.10 Blahut-Arimoto algorithm (BA) illustrates an iterative method to find such an optimal channel $\hat{C}$, given as follows:

1) Start with any stochastic channel $C^{(0)} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$, i.e., $c_{xy}^{(0)} > 0$ for all $x, y \in \mathcal{X}$.
2) Iterate:

$$c_{xy}^{(t+1)} = \frac{c_{xy}^{(t)} \exp(-\beta d(x, y))}{\sum_{z \in \mathcal{X}} c_{xz}^{(t)} \exp(-\beta d(x, z))}$$

where $\beta > 0$ is the negative of the slope of the RD function for a maximum allowance for $\text{AvgD}(X, \hat{C}, d)$, given as $d^*$. We refer to $\beta$ as the loss parameter which captures and reflects the role of $d^*$ within BA. Let the optimal channel that is obtained this way be functionally represented as $\Lambda_{\text{BA}}(\pi_X, C^{(0)})$, as, for a fixed $d^*$, the limiting channel is uniquely determined by the choices of the original distribution, $\pi_X$, and the initial channel, $C^{(0)}$.

Remark 2. In [36], Csizar proved the convergence of BA when $\mathcal{X}$ is finite, therefore guaranteeing to fabricate $\hat{C} = \lim_{t \to \infty} C^{(t)}$ that maximizes privacy for a given allowance of quality loss in the context of our work.

Remark 3. In [16], Oya et al. proved that the limiting channel of BA, $\hat{C}$, with a loss parameter $\beta$ satisfies 2$\beta$-geoinindistinguishability if the chosen metric $d(.)$ is an Euclidean metric.
TABLE I: List of abbreviations

| Abbreviation | Meaning |
|--------------|---------|
| LPMM         | Location-privacy preserving mechanism |
| PMF          | Probability mass function |
| BA           | Blahut-Arimoto algorithm |
| IBU          | Iterative Bayesian update algorithm |
| MLE          | Maximum likelihood estimate |
| QS           | Quality of service |
| EM           | expectation-maximization |
| MI           | Mutual information |
| EMD          | Earth mover’s distance |
| AvgD         | Average distortion under a given measure |
| w.r.t.       | With respect to |
| a.k.a.       | Also known as |
| w.l.o.g.     | Without the loss of generality |

TABLE II: List of notations

| Notation | Meaning |
|----------|---------|
| \( X = \{x_1, \ldots, x_m\} \) | Finite space of source locations |
| \( n \) | Size of \( X \) |
| \( C \) | Space of all stochastic channels on \( X \) |
| \( \Pi_X \) | Simplex of all full-support PMFs on \( X \) |
| \( N \) | Number of samples |
| \( X = \{\hat{x}_1, \ldots, \hat{x}_n\} \) | Sample of original locations |
| \( Y = \{y_1, \ldots, y_n\} \) | Noisy locations |
| \( d^* \) | Maximum average distortion |
| \( \beta \) | Slope parameter of RD function |
| \( \pi_X \) | PMF of the original locations (true PMF) |
| \( c(y) \) | Uniform channel over \( X \) i.e., \( c(y) = \frac{1}{|X|} \forall y \in X \) |
| \( \Lambda_{\text{IBU}}(\theta, C) \) | MLE of \( \pi_X \) by IBU starting with \( \theta \in \Pi_X \) under \( C \in C \) |
| \( \Gamma_{\text{IBU}}(\theta, C) \) | Estimate by \( t \)-th iteration of IBU starting with \( \theta \in \Pi_X \) under \( C \in C \) |
| \( N_{\text{IBU}} \) | Number of iterations needed for IBU to converge |
| \( L(\theta, X) \) | Estimate of \( \pi_X \) by Optima3 after \( N \) iterations starting with \( \theta \in \Pi_X \) |
| \( \phi(\theta(t)) \) | Prob. of Optima3 estimating \( \theta \in \Pi_X \) starting from \( \theta \in \Pi_{\theta} \) |
| \( \Phi \) | Transition matrix of Optima3 as a Markov chain over \( \Pi_{\theta} \) |
| \( \psi \) | Stationary distribution of the Markov chain of Optima3 |
| \( S^t \) | PMF in \( \Pi_{\theta} \) estimated by Optima3 after \( t \) iterations |

IV. DUALITY BETWEEN IBU AND BA

Let us consider a finite space of locations and let \( d_B(x, y) \) be the usual Euclidean metric on it. Let \( X \) be a random variable on \( X \) with PMF \( \pi_X \). Recalling the iteration of BA from (3) and (4):

\[
c_t(y) = \sum_{x \in X} \pi_X(x)c_{txy}^{(t)}
\]

\[
C_{txy}^{t+1} = \frac{c_t(y)}{\sum_{z \in X} c_t(z) \exp(-\beta d_B(x, z))}
\]

Therefore,

\[
c_{t+1}(y) = \sum_{x \in X} \pi_X(x)C_{txy}^{t+1}
\]

\[
\Rightarrow c_{t+1}(y) = \sum_{x \in X} \pi_X(x)\frac{c_t(y)\exp(-\beta d_B(x, y))}{\sum_{z \in X} c_t(z) \exp(-\beta d_B(x, z))}
\]

Comparing it with (1), we observe that (4) gives rise to a very interesting equivalence between BA and IBU. In particular, suppose we have a planar geometric metric, \( C_{\text{geo}} \), given as

\[
C_{\text{geo,xy}} = c \exp(-\beta d_B(x, y)),
\]

satisfying \( \beta \)-geo-indistinguishability, as proposed by Ghosh et al. in [13]. Flipping the roles of \( x \) and \( y \), considering \( \pi_X \) to be the empirical distribution of observed locations obfuscated by \( C_{\text{geo}} \), we reduce (4) to the iterative step of IBU. As we consider a finite space of locations, we advantage from the fact that BA converges and, therefore, implying that \( \lim_{t \to \infty} c_t \) exists and, hence, is unique. This equivalence with IBU’s iterative step shows that \( \lim_{t \to \infty} c_t \) gives a unique MLE for \( \pi_X \) under \( C_{\text{geo}} \), i.e., \( \lim_{t \to \infty} c_t = \hat{\pi}_X \). Thus, we discover a wonderful duality between IBU and BA, and exploit this to obtain a new approach to prove following theorem, complementing the proof given by ElSalamouny et al. for Corollary 2 in [18].

Theorem IV.1. [Corollary 2 in [18]] IBU always converges to the unique MLE of the observed distribution for location data on a finite space under planar geometric mechanism with Euclidean metric.

Proof. A direct consequence of the duality between IBU and BA, as described and explained above.

V. THREE-WAY OPTIMAL MECHANISM: OPTIMA3

Being motivated by the duality of IBU and BA, we proceed to propose an iterative method, which we name Optima3, in order to furnish a geo-indistinguishable location-privacy channel that maximizes privacy for a given level of quality loss and preserves the statistical utility of the dataset.

In the scope of this paper, we consider location data being sampled from a finite and, therefore, discrete space \( X = \{x_1, \ldots, x_m\} \). Let the sampling PMF of the original locations be \( \pi_X \) which we shall refer to as the true distribution or true PMF of the data. We assume a black-box setting for sampling from the true distribution, i.e., we assume can sample locations from \( X \), which act as auxiliary data to construct our mechanism, following the true distribution without explicitly knowing \( \pi_X \). Such a setting is common in the literature [13], [31], and is similar to what Oya et al. adapted in [17]. In this work, to be able to achieve geo-indistinguishability, we shall adhere to the classic Euclidean metric \( d_B \) to measure ground distance between two locations. Optima3 proceeds as follows:

1. Start with any stochastic channel \( C^{(0)} : X \times X \to \mathbb{R}^+ \) and a full-support PMF on \( \theta_0 \) defined on \( X \). Set \( C^{(0)} = C^{(0)} \).

2. In step \( t \geq 1 \):
   i) For a fixed the maximum average distortion, \( c^{(t)} = c_{\text{BA}}(\theta_{t-1}, C^{(t)}) \).
   ii) Do a black-box sampling of \( n \) i.i.d. locations from \( X \) following \( \pi_X \), and obtain true location samples \( L_T \).
   iii) Obfuscate \( L_T \) with \( C^{(t)} \) to produce noisy samples \( L_N \) which give the empirical distribution of the observed locations \( q = \{q(x) : x \in X\} \).
   iv) \( \theta_t = \Gamma_{\text{IBU}}(\theta_{t-1}, C^{(t)}) \).

Theorem V.1. The targeted three-way optimal channel obtained with Optima3 exists and it guarantees geo-indistinguishability.

Proof. Immediate from Remarks [2] and [3].
Algorithm 1: Three-Way Privacy-Utility Optimization (Optima3)

**Input:** Full-support PMF: $\theta_0$, Positive stochastic channel: $C^{(0)}$, Loss parameter: $\beta$, No. of iterations: $N$, No. of iterations of BA: $N_{\text{BA}}$, No. of iterations of IBU: $N_{\text{IBU}}$.

**Output:** Estimation of true PMF: $\hat{\pi}_X$.

Set $t \leftarrow 0$;

while $t \leq N$ do

$C^{(t+1)} = \text{BA}(\theta_t, \hat{C}^{(t)}, \beta, N_{\text{BA}})$;

$L_t \leftarrow \{\hat{x}_1, \ldots, \hat{x}_n\}$: Locations sampled following true PMF;

$L_N \leftarrow \{y_1, \ldots, y_n\}$: Noisy locations by obfuscating $L_t$ with $\hat{C}^{(t)}$;

$q \leftarrow \{q(x): x \in X\}$: Empirical PMF of $L_N$;

$\theta_{t+1} \leftarrow \text{IBU}(C^{(t+1)}, \theta_t, q, N_{\text{IBU}})$;

$t \leftarrow t + 1$;

$\hat{\pi}_X \leftarrow \theta_N$;

Return: $\hat{\pi}_X$.

Algorithm 2: Blahut-Arimoto (BA)

**Input:** PMF: $\pi$, Initial channel $C^{(0)}$, Loss parameter: $\beta > 0$, No. of iterations: $N_{\text{BA}}$.

**Output:** Channel giving minimum mutual information for maximum avg. distortion encapsulated by $\beta$: $\tilde{C}$.

**Function** $\text{BA}(\pi, C^{(0)}, \beta, N_{\text{BA}})$:

Set $t \leftarrow 0$;

while $t \leq N_{\text{BA}}$ do

$e_t(y) \leftarrow \sum_{x \in X} \pi(x) C_{xy}^{(t)}$;

$C_{xy}^{(t+1)} \leftarrow \frac{e_t(y)}{e_t(y)} \exp \left\{ -\beta e_t(x,y) \right\}$;

$t \leftarrow t + 1$;

$\tilde{C} \leftarrow C^{(t)}$;

Return: $\tilde{C}$.

Algorithm 3: iterative Bayesian update (IBU)

**Input:** Privacy channel: $\hat{C}$, Full-support PMF: $\theta_0$, Empirical PMF from observed data: $q$, No. of iterations: $N_{\text{IBU}}$.

**Output:** MLE of true PMF: $\hat{\pi}$.

**Function** $\text{IBU}(\hat{C}, \theta_0, q, N_{\text{IBU}})$:

Set $t \leftarrow 0$;

while $t \leq N_{\text{IBU}}$ do

$\theta_{t+1}(x) \leftarrow \sum_{y \in X} q(y) \frac{C_{xy} \theta_t(x)}{\sum_{z \in X} C_{xz} \theta_t(z)}$;

$t \leftarrow t + 1$;

$\hat{\pi} \leftarrow \theta_{N_{\text{IBU}}}$;

Return: $\hat{\pi}$.

It is straightforward to observe that the goal of Optima3 is to engender a privacy channel that minimizes mutual information for a maximum average distortion. To circumvent any bias for BA to achieve the minimum mutual information starting with any PMF, we feed BA, in each iteration of Optima3, with a uniform channel, i.e., $C_{xy}^{(0)} = \frac{1}{|X|}$ for all $x, y \in X$. Let the privacy channel generated this way, for a fixed of maximum average distortion and always starting from a uniform initial channel, after $N$ iterations, be functionally represented as $\Lambda(\theta_0, N)$, as the entire Optima3 method is uniquely determined with just the starting full-support PMF $\theta_0$.

To evaluate the statistical utility of $\Lambda(\theta_0, N)$, we measure the EMD between the true distribution and the estimated PMF at the end of $N$ iterations of Optima3. Thus, the quantity $EMD(\hat{\pi}_X, \pi_X)$ parameterizes the utility of $\Lambda(\theta_0, N)$ for the service providers. In this work we use the same Euclidean distance as the underlying metric for computing both the EMD and the average distortion. This consistency of the use of Euclidean distance threads together and complements the notion of utility on the end of the users and that for the service providers. The opportunity to capture the essence of the same metric that quantifies QoS and statistical utility for a privacy channel was one of the motivations to use EMD to compare between the true and the estimated PMFs. On this note, we observe one of the most crucial properties of the optimal channel generated by BA in the context of IBU.

**Theorem V.2.** For a starting PMF $\theta_0$ on finite $X$ and a uniform initial channel $C^{(0)}$, let the limiting channel generated by $\lambda_{\text{BA}}(\theta_0, C^{(0)})$ be $\tilde{C}$. Then there is a unique MLE for a set of observed locations on $X$ which are obfuscated with $\tilde{C}$.

**Proof.** In Appendix A.

**Remark 2** and **Theorem V.2** attest that in a single iteration, Optima3 would spawn a unique channel optimizing location-privacy and QoS, and from there on we would converge to a unique MLE of the observed noisy locations sanitized with that channel. Now, in order to examine the convergence of Optima3, model it as a Markov process.

First of all, we acknowledge that discretizing the probability simplex is reasonable under the realistic computational
boundaries. Let \( \Pi_X = \left\{ \theta : \sum_{x \in X} \theta(x) = 1, 0 < \theta(x) \leq 1 \right\} \) be the probability simplex of full-support PMFs on the finite space of locations \( X \). We discretize the interval \((0, 1]\) in \( k \) equal intervals, meaning we allow \( \theta(x) \) to take the values from \((0, 1]_k = \{\frac{1}{k}, \ldots, \frac{k-1}{k}, 1\}\) for every \( x \in X \) and for every \( \theta \in \Pi_X \). Note that according to our need or complying to the available computational capacity, \( k \) can be made as large as desired – the only requirement is to have a finite \( k \).

For example, in the case of using Python as a computational resource, \( k \) could be assigned something as large as \( \approx 1 \times 308 \).

An alternative perspective to this is that the size of the discretized probability simplex is finite \( \sum_{x \in X} \theta(x) = 1\), let the size of the discretized probability simplex \( |\Pi_X| = |X| - 1\), and, hence, \( k \leq \sum_{x \in X} \theta(x) = 1\). An alternative perspective to this is that \( |\Pi_X| = |X| - 1\), and, hence, \( k \leq \sum_{x \in X} \theta(x) = 1\).

Now we relate this idea of making the probability simplex finite with the aim to model the long-term behaviour of Optima3. Probing the functionality of our proposed method, we see that starting with any PMF \( \theta_0 \in \mathcal{P}_{X,k} \), the chance of ending up at some \( \theta' \in \mathcal{P}_{X,k} \), at the end of one iteration, is determined by the noise injected by the channel generated by \( \lambda_{BA} (\theta_0, C^{(0)}) \). In other words, in \( t \)th iteration of Optima3, feeding \( \theta_{t-1} \) to BA and implementing it with the uniform channel \( C^{(0)} \), the limiting channel of BA, \( C^{(1)} \), is uniquely determined (Remark 2), and once we have the noisy locations obfuscated with \( C^{(1)} \), the limiting distribution produced with IBU is the unique MLE of the observed locations under \( C^{(1)} \) (Theorem 2). Thus, the only door of randomness in the \( t \)th cycle of Optima3 is the addition of noise done by the geo-indistinguishable LPPM \( C^{(1)} \). In particular, the probability of ending up in certain \( \theta' \in \mathcal{P}_{X,k} \) after one cycle of Optima3 starting from some \( \theta \in \mathcal{P}_{X,k} \) is some function \( F(.) \) of the optimal channel that BA converged to within this cycle, i.e., \( \mathbb{P} (\Lambda(\theta, 1) = \theta') = F (\lambda_{BA} (\theta, C^{(0)})) \).

Let us a step ahead to make the notion of probability distributions a level more abstract by introducing \( \phi : \mathcal{P}_{X,k} \times \mathcal{P}_{X,k} \mapsto \mathbb{R}^{+} \), such that \( \phi(\theta' | \theta) = \mathbb{P} (\Lambda(\theta, 1) = \theta') \) for every \( \theta, \theta' \in \mathcal{P}_{X,k} \). Essentially, \( \phi(\theta' | \theta) \) gives the probability of a cycle of Optima3 landing up in a certain PMF \( \theta' \in \mathcal{P}_{X,k} \) starting from some PMF \( \theta \in \mathcal{P}_{X,k} \). This immediately enables an environment to look at Optima3 as a Markov chain over the finite space \( \mathcal{P}_{X,k} \) with a transition matrix \( \Phi \) such that \( \Phi_{\theta \theta'} = \phi(\theta' | \theta) \) for every PMF \( \theta, \theta' \in \mathcal{P}_{X,k} \). With this Markov chain interpretation of Optima3, let \( S_t \) be the random variable denoting the state in \( \mathcal{P}_{X,k} \) at \( t \)th iteration of Optima3.

**Remark 4.** A key element to note here is that due to the discretization of the probability simplex \( \Pi_X \) into \( \mathcal{P}_{X,k} \), Optima3 can be modelled as discrete-time a Markov chain on a finite state space.

**Definition VI.1** (Irreducible Markov chain). A discrete-time Markov chain with a transition matrix \( P \) over finite state space is **irreducible** if for all its states \( x, y \), there exists \( t \geq 0 \) such that \( P^t_{xy} > 0 \), where \( P^t \) denotes the transition matrix for the Markov chain at time \( t \).

**Definition VI.2** (Period of Markov chain). For a discrete-time Markov chain with a transition matrix \( P \) over finite state space, let \( T(x) = \{t \geq 1: P^t(x, x) > 0\} \) for any state \( x \) be the set of all time-steps which have a non-zero probability of the Markov chain to start and end in \( x \). Then the period of state \( x \) is \( \text{gcd} (T(x)) \).

**Definition VI.3** (Aperiodic Markov chain). A discrete-time Markov chain over finite state space is called **aperiodic** if the period of all of its states is 1.

**Definition VI.4** (Stationary distribution). For a discrete-time Markov chain with a transition matrix \( P \) over finite state space, a distribution \( \psi \) on the state space is called a stationary distribution if \( \psi P = \psi \).

**Definition VI.5** (First hitting time). For a discrete-time Markov chain with a transition matrix \( P \) over finite state space, let the first hitting time for a state \( x \) be defined as \( \tau(x) = \min\{t \geq 1: S_t = x\} \).

**Lemma VI.1.** Optima3 is an irreducible Markov chain.

**Proof.** In Appendix A.

\[ \square \]
Lemma VI.2. Optima3 is an aperiodic Markov chain.

Proof. In Appendix A.

Now we have the foundations laid to analyze the long-term behaviour of Optima3 seen as a Markov chain. In particular, we now aim to investigate the limiting behaviour of Optima3 if it is let run for long enough. In this regard, we concede to a well-known result in the theory of Markov chains: an irreducible discrete-time Markov chain over a finite state space has a unique stationary distribution (Theorem 3.3 in [38]). As a consequence, we have the following theorem.

Theorem VI.3. Optima3, seen as a discrete-time Markov chain with transition matrix $\Psi$ over the finite state space $\mathcal{P}_{\mathcal{X},k}$, has a unique stationary distribution $\psi$ over $\mathcal{P}_{\mathcal{X},k}$, and it is given by

$$\psi(\theta) = \frac{1}{E(\tau(\theta))}$$

(5)

for every $\theta \in \mathcal{P}_{\mathcal{X},k}$.

Proof. Immediate from Corollary 39 and Theorem 54 by Serfozo in [39]. Explicitly, Theorem 3.3 in [38].

Exploiting the fact that we elevated Optima3 to a Markov chain over a finite state space, as a direct derivative of Theorem VI.3, we can furnish the following theorem.

Theorem VI.4. Let $\psi$ be the unique stationary distribution for the discrete-time Markov chain of Optima3 over the finite state space $\mathcal{P}_{\mathcal{X},k}$. Then, over time, the estimation of the true PMF given by Optima3 follows the distribution $\psi$, i.e., $\lim_{t \to \infty} S^t \sim \psi$.

Proof. An immediate corollary of the Perron–Frobenius theorem [40]. An explicit proof has been given by Freedman in Theorem 4.9 of [38].

Interpretation:

Let us elucidate the deeper interpretation of Theorem VI.3. One very interesting conclusion we get from the result is that irrespective of what initial PMF we start the first cycle of Optima3 from, after enough iterations our method will estimate the true PMF following a fixed distribution that can be computed independently and beforehand using [3].

Moreover, having a sufficiently large number of samples, in the $t^{th}$ iteration, for an arbitrary $t \in \mathbb{N}$, the black-box sampling of the locations, as described in step 2(ii) in the description of Optima3 in Section V, should empirically approximate the true PMF $\pi_{\mathcal{X}}$. This would also imply that the empirical distribution of the noisy locations, obsfuscated with $C(t)$, is expected to be close to $\pi_{\mathcal{X}}C(t)$.

We are expected to end up in such a scenario as a result of having enough samples, and once we have this, starting from any PMF $\theta_0 \in \mathcal{P}_{\mathcal{X},k}$, the MLE of the observed locations will be, approximately, the true PMF $\pi_{\mathcal{X}}$, and IBU estimates it quite efficiently [18]. To put it down mathematically, as $n \to \infty$, in the first iteration of Optima3

$$q \approx \pi_{\mathcal{X}}C(1) \implies \Gamma_{\text{IBU}}(\theta_0, C(0)) \approx \pi_{\mathcal{X}},$$

(6)

and the cycle repeats in the subsequent iterations of Optima3.

Therefore, as a synopsis, we intuitively understand that for a sufficiently large number of location samples, the expected hitting time for $\pi_{\mathcal{X}}$ in the Markov chain is fairly small, i.e., we are expected to arrive at approximating (hit) the true PMF with a rather small number of iterations as we run Optima3. This implies $\frac{1}{E(\tau(\pi_{\mathcal{X}}))}$ is large and, hence, we can make the following remark.

Remark 5. Combining Theorem VI.3 with the above expounding and, we can say that the privacy channel generated by Optima3, which optimizes privacy and QoS, gives the best statistical utility with a very high probability if we have a sufficiently large number of samples, thus, establishing a three-way optimality. In other words, letting $\tilde{\pi}_{\mathcal{X}}$ to be the unique stationary distribution for a given set of observed locations and a geo-indistinguishable channel generated by BA, for any $\theta \neq \tilde{\pi}_{\mathcal{X}}$ in $\mathcal{P}_{\mathcal{X},k}$, we will have:

$$\lim_{n \to \infty} \mathbb{P}(\psi(\tilde{\pi}_{\mathcal{X}}) > \psi(\theta)) \to 1$$

(7)

VII. FURTHER MATHEMATICAL ANALYSIS

In this section, we aim to dissect further into the mathematical intricacies and the properties that our proposed method follows. In order to measure the distances between PMFs within intermediate steps of Optima3, we shall use the total variation distance and the $L^1$, norm.

Definition VII.1 (Total variation). For any two PMFs $\theta, \theta' \in \Pi_{\mathcal{X}}$, the total variation (TV) distance between them, $d_{TV}(\theta, \theta')$ is defined as:

$$d_{TV}(\theta, \theta') = \frac{1}{2} \sum_{x \in \mathcal{X}} |\theta(x) - \theta'(x)|$$

(8)

Definition VII.2 ($L^1$, norm). For any two PMFs $\theta, \theta' \in \Pi_{\mathcal{X}}$, the $L^1$ norm between them, $d_{L^1}(\theta, \theta')$ is defined as:

$$d_{L^1}(\theta, \theta') = \sum_{x \in \mathcal{X}} |\theta(x) - \theta'(x)|$$

(9)

Remark 6. Note that for any pair of $\theta, \theta' \in \Pi_{\mathcal{X}}$, we have $d_{TV}(\theta, \theta') = \frac{1}{2} d_{L^1}(\theta, \theta')$.

A. Properties of BA under Optima3

In [41], Palaiyanur et al. studied the uniform continuity of the rate-distortion function. In order to elaborate on the analytical behaviour BA under Optima3, we shall aim to take advantage of the results in [41]. In particular, we note that using the any distortion metric $d$ on $\mathcal{X}$, for every location $x \in \mathcal{X}$, we have $\hat{x} = x \in \mathcal{X}$ such that $d(x, \hat{x}) = 0$. Therefore, we satisfy the Condition (Z) proposed by Palaiyanur et al. in Section II of [41]. With this, we immediately place ourselves in the environment to profit from Lemma 2 of [41].

As $\mathcal{X}$ is finite, we can define the maximum distortion on $\mathcal{X}$ as $\Delta = \max_{x,y \in \mathcal{X}} d(x,y)$. Let us fix $d^* \in [0, \Delta]$ as the maximum allowance for the average distortion. Let us, further, define the minimum possible non-zero distortion on $\mathcal{X}$ as $\tilde{d} = \min_{x,x' \in \mathcal{X}} \{d(x,x') : x, x' \in \mathcal{X}, d(x, x') > 0\}$. Then we have the following result.
Lemma VII.1. Let \( \theta_1, \theta_2 \in \Pi_X \) such that \( d_L^1(\theta, \theta') < \frac{\delta}{12} \). Let \( X_\theta \) and \( X_{\theta'} \) be random variables on \( X \) with PMFs \( \theta \) and \( \theta' \), respectively. Then we have:

\[
|RD(X_\theta, d^*) - RD(X_{\theta'}, d^*)| \leq \frac{7\Delta}{d} d_L^1(\theta, \theta') \ln \frac{|X|^2}{d L^1(\theta, \theta')}
\]

(10)

**Proof.** Immediate from Lemma 2 of [11].

Lemma VII.2. Let \( A, B \in \mathbb{R}^+ \) be positive constants. Let \( f: \mathbb{R}^+ \to \mathbb{R}^+ \) be such that \( f(x) = Ax \ln \frac{B}{x} \). Then, \( f^{-1}(x) = \frac{B}{\exp\left\{-W_r\left(-\frac{x}{AB}\right)\right\}} \) where \( W_r \) is Lambert \( W \) function of some integer order \( r \).

**Proof.** In Appendix A.

Let us fix a maximum average distortion \( d^* \) under a chosen distortion metric \( d \) for the subsequent analysis. Now we are prepared to show a very interesting property for the rate-distortion function by setting \( A = \frac{\delta}{12} \) and \( B = |X|^2 \). Then we can assert that it is uniformly continuous if we are only focusing on the “small jumps” of the RD function.

**Corollary VII.2.1.** For \( \epsilon > 0 \) satisfying \( \frac{B}{\exp\left\{-W_r\left(-\frac{\epsilon}{AB}\right)\right\}} < \frac{\delta}{12} \), there exists \( \delta > 0 \) such that for all \( \theta, \theta' \in \Pi_X \),

\[
d_L^1(\theta, \theta') < \delta \implies |RD(X_\theta, d^*) - RD(X_{\theta'}, d^*)| \leq \epsilon
\]

where \( X_\theta \) and \( X_{\theta'} \) are random variables on \( X \) with PMFs \( \theta \) and \( \theta' \), respectively.

**Proof.** Setting \( \delta = \frac{B}{\exp\left\{-W_r\left(-\frac{\epsilon}{AB}\right)\right\}} \), the result follows immediately from Lemma VII.1 and Lemma VII.2.

**Remark 7.** For a starting PMF and an initial channel, we know BA converges to the channel that estimates the unique RD function [30]. We can, therefore, comment that the uniform continuity of RD function implies the uniform continuity of BA under the same condition of \( \epsilon \) (jump) as in Corollary VII.2.1.

**B. Properties of IBU under Optima3**

For comparing between the successive iterations of IBU we shall use the TV distance between them. For the convenience of notation, let us extend the functional representation of IBU \( \Gamma_{\text{IBU}}(\cdot) \), as introduced in Definition [III.7] as follows. For any LPPM \( \mathcal{C} \) over the finite space \( X \) and starting with any full-support \( \theta \in \Pi_X \), let \( \Gamma_{\text{IBU}}^t(\theta, \mathcal{C}) \) denote the \( t \)-th iteration of IBU, as in [11], for all \( t \in \mathbb{N} \). Therefore, in the context of any cycle of Optima3, in one cycle \( \Gamma_{\text{IBU}}^t(\theta, \mathcal{C}) = \Gamma_{\text{IBU}}^{N_{\text{IBU}}(\theta, \mathcal{C})} \)

**Lemma VII.3.** Suppose \( \mathcal{C} \) is a privacy channel over \( X \). Then, having a sufficiently large number of samples, every step of IBU is probabilistically uniformly continuous w.r.t. \( d_{TV} \), i.e., as \( n \to \infty \), for all \( \epsilon > 0 \), there exists \( \delta > 0 \) w.p. 1 such that for all \( \theta, \theta' \in \Pi_X \):

\[
d_{TV}(\theta, \theta') < \delta \implies d_{TV}\left(\Gamma_{\text{IBU}}^1(\theta, \mathcal{C}), \Gamma_{\text{IBU}}^1(\theta', \mathcal{C})\right) < \epsilon
\]

**Proof.** In Appendix A.

As an immediate corollary of Lemma VII.3, we can elevate the uniform continuity of a single step of IBU to the entire method and formally assert the following.

**Theorem VII.4.** For an optimal privacy channel \( \hat{\mathcal{C}} \), derived with BA, defined over \( X \), if we have a sufficiently large number of samples, IBU is a probabilistically uniformly continuous transformation w.r.t. \( d_{TV} \), i.e., as \( n \to \infty \), for all \( \epsilon > 0 \), there exists a \( \delta > 0 \) w.p. 1 such that for every \( \theta, \theta' \in \Pi_X \):

\[
d_{TV}(\theta, \theta') < \delta \implies d_{TV}\left(\Gamma_{\text{IBU}}^1(\theta, \mathcal{C}), \Gamma_{\text{IBU}}^1(\theta', \mathcal{C})\right) < \epsilon
\]

**Proof.** In Appendix A.

C. **Compiling BA and IBU under Optima3**

Having discussed several very interesting and quite desirable analytical properties of the RD function, BA, and IBU, we are now in a position to comment about the uniform continuity of Optima3.

**Theorem VII.6.** Optima3 is a uniformly continuous transformation w.r.t. \( L^1 \) norm, i.e., supposing Optima3 runs for \( N \) iterations, for all \( \epsilon > 0 \) there exists \( \delta > 0 \) such that for every \( \theta_0, \theta' \in \Pi_X \):

\[
d_{TV}\left(\Gamma_{\text{IBU}}^1(\theta, \mathcal{C}), \Gamma_{\text{IBU}}^1(\theta', \mathcal{C})\right) \leq K d_{TV}(\theta, \theta')
\]

**Proof.** In Appendix A.

**VIII. EXPERIMENTAL RESULTS**

In this section, we describe the empirical results obtained by carrying out experimental analysis to illustrate and validate the working of our proposed method. We perform our experiments on real location data from the Gowalla dataset [42], [43]. We consider Gowalla check-ins from (i) a northern part of San Francisco bounded by latitudes (37.7228, 37.7946) and longitudes (-122.5153, -122.3789) covering an area of 12Km x 8Km discretized with a 24 x 17 grid; (ii) a central part of Paris bounded by latitudes (48.8286, 48.8798) and longitudes (2.2855, 2.3909) covering an area of 8Km x 6Km discretized with a 16 x 12 grid. In this setting, we work with 123,108 check-in locations in San Francisco and 10,260 check-in locations in Paris. Figure 2a shows the particular points of check-ins from Paris and San Francisco and Figure 2b displays the distribution with which these location data are spread across the two cities.

We implemented Optima3 on the datasets from Paris and San Francisco separately to judge its performance on real location data. For the location dataset from Paris, 15 cycles of
Optima3 was run, where each cycle comprised of 8 iterations of BA and 10 iterations of IBU. In the case of San Francisco, we ran Optima3 for 8 cycles with 5 iterations of BA and IBU each under every cycle of Optima3. In both cases, we assigned the value of the loss parameter parameterizing the maximum allowance of average distortion, $\beta$, to be 0.5 and 1. This was done to test the performance of Optima3 in estimating the true PMF under two different levels of privacy. Each experiment was run for 5 rounds to account for the randomness of the sampling and obfuscation. In each cycle of Optima3 across all the settings, BA was initiated with the uniform channel $C^{(0)}$ and a uniform distribution over the locations as the “starting guess” of the true distribution.

$\beta = 1$ gives rise to a geo-indistinguishable location-privacy mechanism with BA that injects less noise than that produced with $\beta = 0.5$. As a result, we obtain a more accurate estimation of the true PMF via Optima3 for the case of $\beta = 1$ than for $\beta = 0.5$ as less local noise has been injected for the former than the latter. However, in both cases, the EMD between the true and the estimated PMF seem very low, insinuating a good performance of the mechanism produced with Optima3 for preserving the statistical utility of the data. Moreover, for both Paris and San Francisco, Optima3 seems to significantly improve its estimation of the true PMF with every iteration until it converges to the MLE of the observed locations.

Comparing Figure 3 with Figure 2b, we see that the estimations of the true distributions of the locations in Paris and San Francisco with $\beta = 0.5$ are much more accurate than those with $\beta = 1$. This is because less local noise has been injected for the former than the latter. However, in both cases, the EMD between the true and the estimated PMF seem very low, insinuating a good performance of the mechanism produced with Optima3 for preserving the statistical utility of the data.

Fig. 4: (a) and (b) show the EMD between the true distribution of the locations in Paris and its estimation by Optima3 in each of its 15 cycles for $\beta = 0.5$ and $\beta = 1$, respectively. (c) and (d) zoom into EMDs for $\beta = 0.5$ and $\beta = 1$, respectively, by focusing on the results from the second cycle of Optima3 onward.
of the entire method. This is a major difference from the work of the locations. This, empirically, suggests the convergence under the channel produced by BA, estimating the true PMF cycle go on to converge to the MLE of the noisy locations PMFs given by Optima3 seem to improve at the end of each true and the estimated PMFs seem to decrease with the number most crucial observations here is that the EMD between the locations datasets of Paris and San Francisco, respectively.

Now we shift our attention to Figures 4 and 5 to analyze the performance of Optima3 in preserving the statistical utility for the locations in Paris and its estimation by Optima3 (Nβ = 8, NIBU = 10): of encountering with a LPPM which is optimal according to the standards set by Shokri et al. in [37] but the EM method used to estimate the true distribution would fail to converge for that mechanism as illustrated in Example [11].

In particular, we observe a significant improvement in the estimation of the true PMF after the first cycle of Optima3, after which the estimated PMF converges to the MLE of the observed locations with following quite a stable trend. In order to visualize this road to convergence of Optima3 more distinctly, in Figures 4d and 4c we focus on the second iteration of Optima3 onward for β = 0.5 and β = 1, respectively.

We observe an exact similar trend for the case of the San Francisco dataset. Figures 5a and 5b show the behaviour of the statistical utility of the privacy channel generated by BA under each of the 8 cycles of Optima3 for β = 0.5 and β = 1, respectively. To magnify the path to convergence, we demonstrate the behaviour of Optima3 from its second cycle onward in Figures 5c and 5d for β = 0.5 and (d) zoom into EMDs for β = 1, respectively.

Table III: EMD between the true and the estimated distributions on locations in Paris by Optima3 (Nβ = 8, NIBU = 10):

| N | Round 1 | Round 2 | Round 3 | Round 4 | Round 5 |
|---|---------|---------|---------|---------|---------|
| 1 | 0.15106 | 0.14271 | 0.14601 | 0.13584 | 0.12413 |
| 2 | 0.21367 | 0.21432 | 0.21537 | 0.21777 | 0.21881 |
| 3 | 0.26091 | 0.26029 | 0.26231 | 0.26180 | 0.26518 |
| 4 | 0.29828 | 0.298370 | 0.30017 | 0.29784 | 0.29859 |
| 5 | 0.37229 | 0.37038 | 0.36784 | 0.36949 | 0.36816 |
| 6 | 0.43588 | 0.43745 | 0.43558 | 0.43704 | 0.43584 |
| 7 | 0.48194 | 0.48299 | 0.47992 | 0.48267 | 0.47791 |
| 8 | 0.51672 | 0.51710 | 0.51735 | 0.51880 | 0.51138 |
| 9 | 0.56896 | 0.57378 | 0.57338 | 0.57125 | 0.56618 |
| 10 | 0.64931 | 0.66292 | 0.65362 | 0.65950 | 0.65285 |
| 11 | 0.79621 | 0.80474 | 0.80219 | 0.80670 | 0.79940 |
| 12 | 7.37595 | 7.37595 | 7.37595 | 7.37595 | 7.37595 |

Table IV: EMD between the true and the estimated distributions on locations in San Francisco by Optima3 (Nβ = 5, NIBU = 5):

| N | Round 1 | Round 2 | Round 3 | Round 4 | Round 5 |
|---|---------|---------|---------|---------|---------|
| 1 | 2.02262 | 2.02262 | 2.02262 | 2.02262 | 2.02262 |
| 2 | 0.21916 | 0.23750 | 0.25035 | 0.25116 | 0.23241 |
| 3 | 0.27104 | 0.27796 | 0.28247 | 0.27758 | 0.26276 |
| 4 | 0.33137 | 0.31749 | 0.34690 | 0.33840 | 0.34028 |
| 5 | 0.35044 | 0.34383 | 0.34818 | 0.35760 | 0.36804 |
| 6 | 0.37818 | 0.35482 | 0.36039 | 0.36375 | 0.38045 |
| 7 | 0.39741 | 0.38771 | 0.37284 | 0.41176 | 0.36953 |
| 8 | 0.51324 | 0.48295 | 0.47043 | 0.51285 | 0.45826 |
| 9 | 0.57738 | 0.57994 | 0.55791 | 0.60717 | 0.56880 |
| 10 | 2.02262 | 2.02262 | 2.02262 | 2.02262 | 2.02262 |

San Francisco by IBU under Optima3 for both the settings of the loss parameter are fairly accurate. However, as we would expect, the privacy mechanism obtained under Optima3 harbours better statistical utility for β = 1 than for β = 0.5 because of the level of local noise injected.

Now we shift our attention to Figures 4 and 5 to analyze the performance of Optima3 in preserving the statistical utility for the locations datasets of Paris and San Francisco, respectively. Figures 4b and 4a show us the behaviour of the EMD between the true distribution of the locations in Paris and its estimate by IBU under Optima3 in each of its 15 cycles. One of the most crucial observations here is that the EMD between the true and the estimated PMFs seem to decrease with the number of iterations, and finally converge, implying that the estimated PMFs given by Optima3 seem to improve at the end of each cycle go on to converge to the MLE of the noisy locations under the channel produced by BA, estimating the true PMF of the locations. This, empirically, suggests the convergence of the entire method. This is a major difference from the work of [17] which, as we pointed out before, harbours the potential

\[ \text{EMD between true and estimated PMFs for SF locations} \]

\[ \text{EMD between true and estimated PMFs for SF locations} \]

\[ \text{EMD between true and estimated PMFs for SF locations} \]

\[ \text{EMD between true and estimated PMFs for SF locations} \]

\[ \text{EMD between true and estimated PMFs for SF locations} \]

\[ \text{EMD between true and estimated PMFs for SF locations} \]
which is specified with the loss parameter $\beta$. We recall and acknowledge that a higher the value of $\beta$, the lesser the local noise that is injected into the data, staying consistent with our observations in Figure 3.

We continue working with the location data from Paris and San Francisco obtained from the Gowalla dataset in the same framework as described before. We consider $\beta$ taking the values from the set $S_\beta = \{0.1, 0.3, 0.5, 0.7, 0.9, 1\}$, and for each value of the loss parameter, we run Optima3 on the datasets of Paris and San Francisco using the same number of iterations as used in the previous experiments – for the Paris dataset, within each cycle of Optima3 we implement 8 iterations of BA and 10 iterations of IBU, running Optima3 for 15 cycles, and for the San Francisco dataset, we use 5 iterations for each of BA and IBU within a single cycle of Optima3 and run the entire method for 8 cycles. We run the experiments for 5 rounds for each value of $\beta$ to account for the randomness of noise insertion.

At the end of running all the batches of Optima3 correspondingly on the two datasets, we set to dissect the trend of the final estimated distributions for the different loss parameters representing the maximum average distortion w.r.t. the Euclidean distance. Specifically, we plot the EMD between the true and the final estimated PMFs for each of the two datasets after the completion of Optima3 against the different $\beta$ in $S_\beta$.

Fig. 6: (a) and (b) illustrate that the difference between the true distribution of the location data after the empirical convergence of Optima3 sharply decreases and eventually stabilizes with an increase in the value of the loss parameter. In other words, as the intensity of the local noise injected with the privacy channel generated within Optima3 decreases, we will end up estimating the unique MLE of the true PMF giving rise to the best possible statistical utility under the MI-AvgD optimization.

Figures 6a and 6b show us that the statistical utility when plotted against the loss parameter denoting the maximum average distortion, for each the two location datasets, results in producing a Pareto curve. We see that the EMD between the true and the estimated PMFs for a fixed number of cycles of Optima3 run with a given number of iterations for BA and IBU, such that the entire method numerically converges, prominently decreases and becomes stable as $\beta$ increases, i.e., the amount of locally injected noise decreases. This depicts an improvement of the estimated PMF until it advances to converge to the true PMF with an increase of the loss parameter. This observation is consistent with the Pareto-behaviour of mutual information with the maximum average distortion as studied in rate-distortion theory [32], and thus, we empirically bridge together the two ends of utility we focused on in this paper.

B. Connecting the theoretical results

The experimental analysis on the real locations from Paris and San Francisco galvanize the theory developed in Sections V, VI, and VII with validations and visualisations. The very accurate estimate of the true distributions of the data using IBU for the privacy channels produced by BA under Optima3 ensures perceptible evidence towards our goal of furnishing a three-way optimal location-privacy mechanism satisfying geo-indistinguishability.

The outcomes of the experiments reassure the uniform continuity of Optima3 and provide empirical evidence for Theorem VII.6. Moreover, from the experiments, we can draw a very interesting parallel by perceiving Optima3 as a discrete-time Markov chain over the finite space $P_{X,k}$. We recall Theorem VI.4 that suggests that the limiting behaviour of the estimated PMF by Optima3 will follow a unique distribution $\psi$ over $P_{X,k}$ where $\psi$ was obtained with the help of (5) in Theorem VI.3. Furthermore, Remark 5 suggests that this limiting distribution of the estimates, $\psi$, should be reflecting a high probability for Optima3 to estimate the unique, by Theorem VII.2, MLE of the observed locations under the privacy channel generated by BA. Figures 4 and 5 reinforce this point by empirically demonstrating the convergence of Optima3 to the MLE across all the rounds of experiments, embracing the fact that, indeed, the MLE has the highest chance of being estimated by Optima3 at the end of each cycle and empirically backing up (7). This confirms that the privacy channel obtained with BA that optimizes MI and AvgD within each cycle of Optima3 also guarantees the best statistical utility over time with sufficient number of samples and gives a very accurate estimate of the true PMF, evidently heading towards establishing a three-way optimization between privacy and the two notions of utility.

IX. CONCLUSION

In this paper we have considered the triadic conflict between location-privacy, users’ quality of service, and statistical utility of the collected data, addressing the problem of finding the mechanism that would optimize their trade-off. To resolve this three-way optimization, we have proposed an iterative method named Optima3 that would ensure a privacy protection mechanism satisfying the state-of-the-art standard for location-privacy, geo-indistinguishability, and advances to optimize the trade-off between privacy and the two notions of utility. Specifically, Optima3 generates a geo-indistinguishable LPPM
that minimizes mutual information for a fixed maximum average distortion and allows to estimate the most likely distribution of the original data (MLE). We use the model of mutual information to denote location-privacy and the average distortion under a chosen metric to denote the quality loss, which is standard in the literature. The MLE of the original distribution under the privacy mechanism from the observed noisy location data furnished under Optima3 represents the statistical utility of our LPPM.

We have introduced a theoretical setting to characterize the behaviour of our method and prove that the sub-mechanisms under Optima3 converge. Moreover, we have modelled the long-term behaviour of Optima3 from a probabilistic perspective and performed experiments with real location data to show that Optima3 actually converges and proceeds towards achieving a three-way optimality, resolving the three-way battle between privacy and the two notions of utility.

In summary, we have bridged some key ideas from the world of information theory, probability theory, and statistics to provide a three-way optimal location-privacy mechanism, proving its properties via a thorough theoretical and experimental analysis.

We believe that our results can be extended easily to other data and to other notions of distance between them, since the analysis carried on in this paper does not depend crucially on the notion of distance used.

ACKNOWLEDGEMENT

This work was supported by the European Research Council (ERC) project HYPATIA under the European Union’s Horizon 2020 research and innovation programme. Grant agreement n. 835294.

REFERENCES

[1] 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.), (Berlin, Heidelberg), pp. 265–284, Springer Berlin Heidelberg, 2006.
[2] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, “Our data, ourselves: Privacy via distributed noise generation,” in Advances in Cryptology - EUROCRYPT 2006 (S. Vaudenay, ed.), (Berlin, Heidelberg), pp. 486–503, Springer Berlin Heidelberg, 2006.
[3] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, “Local privacy and statistical minimax rates,” in 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, pp. 429–438, 2013.
[4] Ulfar Erlingsson, V. Pihur, and A. Korolova, “Rappor: Randomized aggregatable privacy-preserving ordinal response,” in Proceedings of the 21st ACM Conference on Computer and Communications Security, (Scottsdale, Arizona), 2014.
[5] D. P. T. Apple, “Learning with privacy at scale,” 2017.
[6] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, “Protecting location privacy: Optimal strategy against localization attacks,” in Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS ’12, (New York, NY, USA), p. 671–672, Association for Computing Machinery, 2012.
[7] R. Shokri, “Privacy games: Optimal user-centric data obfuscation,” Proceedings on Privacy Enhancing Technologies, vol. 2015, no. 2, pp. 299–315, 2015.
[8] 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, CCS ’13, (New York, NY, USA), p. 901–914, Association for Computing Machinery, 2013.
[9] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, “Optimal geo-indistinguishable mechanisms for location privacy,” in Proceedings of the 21th ACM Conference on Computer and Communications Security (CCS 2014), 2014.
[10] N. Fernandes, A. McIver, and C. Morgan, “The laplace mechanism has optimal utility for differential privacy over continuous queries,” in 36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021., pp. 1–12, IEEE, 2021.
[11] J. Brickell and V. Shmatikov, “The cost of privacy: Destruction of data mining utility in anonymized data publishing,” in Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD ’08, (New York, NY, USA), p. 70–78, Association for Computing Machinery, 2008.
[12] S. Ioannidis, A. Montanari, U. Weinsberg, S. Bhagat, N. Fawaz, and N. Taft, “Privacy tradeoffs in predictive analytics,” in The 2014 ACM International Conference on Measurement and Modeling of Computer Systems, SIGMETRICS ’14, (New York, NY, USA), p. 57–69, Association for Computing Machinery, 2014.
[13] A. Ghosh, T. Roughgarden, and M. Sundararajan, “Universally utility-maximizing privacy mechanisms,” SIAM Journal on Computing, vol. 41, no. 6, pp. 1673–1693, 2012.
[14] M. Gupte and M. Sundararajan, “Universally optimal privacy mechanisms for minmax agents,” in Proceedings of the Twenty-Ninth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS ’10, (New York, NY, USA), pp. 155–166, Association for Computing Machinery, 2010.
[15] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, “Optimizing linear counting queries under differential privacy,” in Proceedings of the Twenty-Ninth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS ’10, (New York, NY, USA), p. 123–134, Association for Computing Machinery, 2010.
[16] S. Oya, C. Troncoso, and F. Pérez-González, “Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1959–1972, ACM, 2017.
[17] S. Oya, C. Troncoso, and F. Pérez-González, “Rethinking location privacy for unknown mobility behaviors,” in 2019 IEEE European Symposium on Security and Privacy (EuroS P), pp. 416–431, 2019.
[18] E. ElSalamouny and C. Palamidessi, “Full convergence of the iterative bayesian update and applications to mechanisms for privacy protection,” CoRR, vol. abs/1909.02961, 2019.
[19] D. Agrawal and C. C. Aggarwal, “On the design and quantification of privacy preserving data mining algorithms,” in Proceedings of the Twentieth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS ’01, (New York, NY, USA), p. 247–255, Association for Computing Machinery, 2001.
[20] P. Cuff and L. Yu, “Differential privacy as a mutual information constraint,” in Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security (CCS), CCS ’16, (New York, NY, USA), pp. 43–54, ACM, 2016.
[21] Y. Zhu and R. Bettati, “Anonymity vs. information leakage in anonymity systems,” in Proc. of ICDCS, pp. 514–524, IEEE Computer Society, 2005.
[22] K. Chatzikokolakis, C. Palamidessi, and P. Panangaden, “Anonymity protocols as noisy channels,” Information and Computation, vol. 206, no. 2–4, pp. 378–401, 2008.
[23] M. Abadi and D. G. Andersen, “Learning to protect communications with adversarial neural cryptography,” CoRR, vol. abs/1610.06918, 2016.
[24] A. Tripathy, Y. Wang, and P. Ishwar, “Privacy-preserving adversarial networks,” in 57th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2019, Monticello, IL, USA, September 24–27, 2019, p. 495–505, IEEE, 2019.
[25] M. Romanelli, K. Chatzikokolakis, and C. Palamidessi, “Optimal obfuscation mechanisms via machine learning,” in 2020 IEEE 33rd Computer Security Foundations Symposium (CSF), pp. 153–168, 2020.
[26] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, “Context-aware generative adversarial privacy,” Entropy, vol. 19, 12 2017.
[27] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, “Optimal geo-indistinguishable mechanisms for location privacy,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS ’14, (New York, NY, USA), p. 251–262, Association for Computing Machinery, 2014.
proof of observed locations on $X$. Let the empirical PMF of the observed locations be

$$q(y) = \frac{\theta_y}{\sum_{z \in X} \theta_z} \exp\{-\beta d_E(x, y)\}$$

for some normalising positive constant $\alpha(x)$ depending on $x$. The rest of the proof proceeds identically as the proof of Corollary 3 in [18] by ElSalameony et al.

In particular, in the proof of Corollary 3, ElSalameony et al. exploited the fact that linear independence of the columns of $G(I')$, defined in the proof of Corollary 2, is preserved even when each column of $G(I')$ is scaled by a positive constant. We note that the $G(I')$ that has been defined is symmetric, i.e., $G(I')^T = G(I')$, i.e., the as columns of $G(I)$ are linearly independent, so are the rows.

We observe from (11) that, in our case, each row of $G(I)$ gets scaled by a positive factor, proceeding with the same idea of $G(I)$ as used in the proof of Corollary 2 of [18]. Or in other words, we could think of having each column scaled by a positive factor by considering $G(I)^T$. As the scaling of the columns preserves the linear independence of the columns of $G(I')$ (or the rows of $G(I)$), we can conclude that the rows of $G(I)$ scaled by a positive factor preserve the linear independence of the rows of the unscaledopen $G(I)$ devised for the simple geometric mechanism by ElSalameony et al.

Thus, we have $v G(I) = v G(I)' = 0$ if $v = 0$, where $G(I)'$ is the matrix where the $x$th row of $G(I)$ is scaled by $\alpha^{-1}(x)$. This reduces us to satisfy the sufficient condition for having a unique MLE given by Theorem 7 of [18] by the exact same line of idea for the proofs of Corollary 2 and Corollary 3 by ElSalameony et al. Thus, by Theorem 7 of [18] we can conclude that there is a unique MLE for a set of observed locations which are obfuscated by $\hat{C}$.

\[ \square \]

Lemma VI.1. Optima3 is an irreducible Markov chain.

Proof. Let $\Phi$ be the transition matrix of Optima3 seen as a Markov chain over $\mathcal{P}_{X,k}$. In a Optima3 cycle, we implement BA with a full-support PMF $\theta \in \mathcal{P}_{X,k}$ and the uniform channel $C(0)$ and we converge to an optimal channel $\hat{C}$ given by $\lambda_{BA}(\theta, C(0))$.

We observe from (3) that $\hat{C}_{xy} > 0$ for every $x, y \in X$. This essentially implies that any given location in $\mathcal{X}$ can be obfuscated to any other location $y \in X$. In other words, from a given set of input (original) locations $X = \{\tilde{x}_1, \ldots, \tilde{x}_n\}$, any set of output (noisy) locations $Y = \{y_1, \ldots, y_n\}$ could be reached via the location-privacy channel $\hat{C}$. In particular, with $\hat{C}$, for any input of location samples $X$, we could give rise to an empirical distribution, $q$, of the observed locations, which, in turn, can obfuscate any MLE $\theta' \in \mathcal{P}_{X,k}$.
Looking at it alternatively, for a given set of original locations, \( X \), for any target PMF \( \theta' \in P_{X,k} \), we have a non-zero probability of fostering a set of noisy locations, \( Y \), produced by locally obfuscating the locations in \( X \) with the channel \( \mathcal{C} \) obtained with \( \lambda_{BA} (\theta, C(0)) \), which would induce \( \theta' \) as its MLE under \( \mathcal{C} \) where IBY will converge to at the end of this cycle of Optima3. Therefore, \( \Phi_{\theta, \theta'} = \phi(\theta | \theta') > 0 \) for every \( \theta, \theta' \in P_{X,k} \), implying that, in this setting, Optima3 induces an irreducible Markov chain. 

Lemma VI.2. Optima3 is an aperiodic Markov chain.

Proof. The idea for this follows very similar line of thought for the proof of Lemma VII.1. Let \( \Phi \) be the transition matrix of Optima3 seen as a Markov chain over \( P_{X,k} \). We showed in the proof of Lemma VII.1 that \( \Phi_{\theta, \theta'} > 0 \) for all \( \theta, \theta' \in P_{X,k} \).

In particular, for every \( \theta \in P_{X,k} \) and for a channel \( \mathcal{C} \) produced by \( \lambda_{BA} (\theta, C(0)) \), where \( C(0) \) is the uniform channel, we can obfuscate any set of true locations \( X \) to produce the noisy locations \( Y \) which would give rise to the output distribution \( q \) over \( \mathcal{X} \), empirically computed on the observed set locations \( Y \), such that \( q(y) = \sum_{x \in X} \theta(x) \mathcal{C}_{xy} \) with a non-zero probability.

A very interesting and beautiful consequence of this is that it would ensure that there is some positive probability that the MLE of an observed locations privatized with \( \mathcal{C} \) is the “starting guess” itself, which was fed into IBU, i.e., \( \mathbb{P}(\Gamma_{IBU}(\theta, \mathcal{C}) = \theta) > 0 \) for every \( \theta \in P_{X,k} \). This shows that the period for every state \( \theta \in P_{X,k} \) in the Markov chain is 1. Therefore, Optima3 gives rise to an aperiodic Markov chain. 

Lemma VII.2. Let \( A, B \in \mathbb{R}^+ \) be positive constants. Let \( f : \mathbb{R}^+ \rightarrow \mathbb{R}^+ \) be such that \( f(x) = Ax \ln \frac{B}{x} \). Then

\[
f^{-1}(x) = \frac{B}{\exp\left\{-W_r\left(-\frac{\ln x}{AB}\right)\right\}}
\]

where \( W_r \) is Lambert W function of some integer order \( r \).

Proof.

\[
y = Ax \ln \frac{B}{x} \implies y = x \ln \frac{B}{x}
\]

\[
\implies y' = \ln x' \quad \text{[where } x' = \frac{B}{x}, y' = \frac{y}{AB}]
\]

\[
\implies y' x' = \ln x' \implies y' \exp\{\ln x'\} = \ln x'
\]

\[
\implies y' = \ln x' \exp\{-\ln x'\}
\]

\[
\implies -y' = z \exp\{z\} \quad \text{[where } z = -\ln x' = -\ln \frac{B}{x}]
\]

\[
\implies z = W_r(-y') = W_r\left(-\frac{y}{AB}\right)
\]

\[
\implies -\ln \frac{B}{x} = W_r\left(-\frac{y}{AB}\right)
\]

\[
\implies \frac{B}{x} = \exp\{-W_r\left(-\frac{y}{AB}\right)\}
\]

\[
f^{-1}(x) = \frac{B}{\exp\left\{-W_r\left(-\frac{\ln x}{AB}\right)\right\}}
\]

Lemma VII.3. Suppose \( \mathcal{C} \) is a privacy channel over \( \mathcal{X} \). Then, having a sufficiently large number of samples, every step of IBU is probabilistically uniformly continuous w.r.t. \( d_{TV} \), i.e., as \( n \to \infty \), for all \( \epsilon > 0 \), there exists \( \delta > 0 \) w.p. 1 such that for all \( \theta, \theta' \in \Pi_\mathcal{X} \):

\[
d_{TV}(\theta, \theta') < \delta \implies d_{TV}(\Gamma_{IBU}(\theta, \mathcal{C}), \Gamma_{IBU}(\theta', \mathcal{C})) < \epsilon
\]

Proof. Let \( \epsilon > 0 \).

\[
d_{TV}(\Gamma_{IBU}(\theta, \mathcal{C}), \Gamma_{IBU}(\theta', \mathcal{C})) = \frac{1}{2} \sum_{x \in \mathcal{X}} |q_{\theta}(x) - q_{\theta'}(x)|
\]

To prove the result, it is enough to show the uniform continuity of the steps of IBU w.r.t \( L^1 \) norm, as \( \frac{1}{2}d_{L^1} = d_{TV} \), as we can always scale \( \delta \) by half and reduce to the total variation distance. Therefore, \( L^1 \), under the \( L^1 \) norm, reduces to:

\[
\sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{X}} q_{\theta}(y) - \sum_{z \in \mathcal{X}} q_{\theta'}(z) \right|
\]

Here \( q^1 \) and \( q^2 \) are the corresponding empirical PMFs generated by the observed locations running IBU starting with \( \theta \) and \( \theta' \), respectively. Note that the black-box sampling and obfuscation of the locations that, in turn, give rise to \( q^1 \) and \( q^2 \) do not depend on \( \theta \) and \( \theta' \) respectively. In particular, since both cases of obfuscating the real locations are done by the same channel, as \( n \to \infty \), we can assume \( \mathbb{P}(q^1 = q^2) \to 1 \). Let \( q = \lim_{n \to \infty} q^1 = \lim_{n \to \infty} q^2 \). Thus, we get an upper bound for \( L^1 \) w.p. 1 in the form of:
\[
\sum_{y \in \mathcal{X}} K_y \leq \sum_{y \in \mathcal{X}} q_y n^2 = n^2. \text{ Hence, using } (15), \ d_{L^1}(\theta, \theta') < \delta, \text{ or, } d_{TV}(\theta, \theta') < \delta/2 \text{ implies: }
\]
\[
d_{L^1} \left( \Gamma_{IBU}^1 (\theta, \mathcal{C}), \Gamma_{IBU}^1 (\theta', \mathcal{C}) \right) < 2M^2 \delta n^2 \implies d_{TV} \left( \Gamma_{IBU}^1 (\theta, \mathcal{C}), \Gamma_{IBU}^1 (\theta', \mathcal{C}) \right) < 2M^2 \delta n^2 \quad (16)
\]

So for the given \( \epsilon \), if we choose \( \delta = \frac{\epsilon}{2M^2n^2} \), we are done. \( \square \)

**Theorem VII.4.** For an optimal privacy channel \( \hat{\mathcal{C}} \), derived from BA, defined over \( \mathcal{X} \), if we have a sufficiently large number of samples, IBU is a probabilistically uniformly continuous transformation w.r.t. \( d_{TV} \), i.e., as \( n \to \infty \), for all \( \epsilon > 0 \), there exists a \( \delta > 0 \) w.p. 1 such that for every \( \theta, \theta' \in \Pi_X \):

\[
d_{TV}(\theta, \theta') < \delta \implies d_{TV} \left( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU} (\theta', \hat{\mathcal{C}}) \right) < \epsilon
\]

**Proof.** Let \( \epsilon > 0 \). As \( \hat{\mathcal{C}} \) is derived from BA, by Theorem V.2 starting with any PMF in \( \Pi_X \) and an observed set of noisy locations, IBU converges uniquely to the most likely prior under \( \hat{\mathcal{C}} \) which is denoted by \( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}) \). Running two IBUs starting with \( \theta \in \Pi_X \) and \( \theta' \in \Pi_X \), respectively, let \( N_{IBU} \in \mathbb{N} \) be the number of iterations after which they numerically converge to, or are within a desirable threshold of, \( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}) \) and \( \Gamma_{IBU} (\theta', \hat{\mathcal{C}}) \), respectively. Assuming that we observe a sufficiently large number of locations, by Theorem VII.3 for any \( \epsilon_k > 0 \), for every \( k \in \mathbb{Z}_{\geq 0} \), there is \( \epsilon_{k-1} > 0 \) w.p. 1 such that:

\[
d_{TV} \left( \Gamma_{IBU}^{k-1} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU}^{k-1} (\theta', \hat{\mathcal{C}}) \right) < \epsilon_{k-1} \implies d_{TV} \left( \Gamma_{IBU}^{k} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU}^{k} (\theta', \hat{\mathcal{C}}) \right) < \epsilon_k
\]

As \( n \to \infty \), setting \( \epsilon_{N_{IBU}} = \epsilon > 0 \) and \( \epsilon_0 = \delta = \delta \), by induction, we will get \( \{\epsilon_1, \ldots, \epsilon_{N_{IBU}-1}\} \) w.p. 1 such that:

\[
d_{TV}(\theta, \theta') < \delta \iff d_{TV} \left( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU} (\theta', \hat{\mathcal{C}}) \right) < \epsilon_0 \implies d_{TV} \left( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU} (\theta', \hat{\mathcal{C}}) \right) < \epsilon_1
\]

\[
\vdots
\]

\[
d_{TV} \left( \Gamma_{IBU}^{N_{IBU}+1-1} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU}^{N_{IBU}+1-1} (\theta', \hat{\mathcal{C}}) \right) < \epsilon_{N_{IBU}-1} \implies d_{TV} \left( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU} (\theta', \hat{\mathcal{C}}) \right) < \epsilon_{N_{IBU}}
\]

\( \square \)

**Lemma VII.5.** For an optimal privacy channel \( \hat{\mathcal{C}} \) over \( \mathcal{X} \) generated with BA, with a sufficiently large number of samples, IBU is a *Lipschitz continuous* transformation w.r.t. \( d_{TV} \), i.e., as \( n \to \infty \), there exists constant \( K \in \mathbb{R}^+ \) w.p. 1 such that for any pair of PMFs \( \theta, \theta' \in \Pi_X \):

\[
d_{TV} \left( \Gamma_{IBU} (\theta, \hat{\mathcal{C}}), \Gamma_{IBU} (\theta', \hat{\mathcal{C}}) \right) \leq K d_{TV}(\theta, \theta')
\]
Proof. Let \( \theta, \theta' \) be any pair of PMF in \( \Pi_\mathcal{X} \). If some \( K \in \mathbb{R}^+ \) satisfies:

\[
d_{\text{TV}} \left( \Gamma_{\text{IBU}} \left( \theta, \hat{\mathcal{C}} \right), \Gamma_{\text{IBU}} \left( \theta', \hat{\mathcal{C}} \right) \right) \leq K d_{\text{TV}}(\theta, \theta')
\]

Let \( d_L \) denote the \( L^1 \) norm. Then, as \( d_{\text{TV}} = \frac{1}{2} d_L \), the same \( K \) also satisfies:

\[
d_{\text{TV}} \left( \Gamma_{\text{IBU}} \left( \theta, \hat{\mathcal{C}} \right), \Gamma_{\text{IBU}} \left( \theta', \hat{\mathcal{C}} \right) \right) \leq K d_{\text{TV}}(\theta, \theta')
\]

To prove the result, it is enough to show the Lipschitz continuity of IBU w.r.t \( L^1 \) norm. To do this, first we aim to show the Lipschitz of each step of IBU. We proceed like the proof of Lemma VII.3 and, thus, we have:

\[
d_{\text{TV}} \left( \Gamma_{\text{IBU}}^1 \left( \theta, \hat{\mathcal{C}} \right), \Gamma_{\text{IBU}}^1 \left( \theta', \hat{\mathcal{C}} \right) \right) \leq \frac{1}{2} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{X}} q_y \hat{C}_{xy} \left| \frac{\theta(x)}{\hat{C}_{xy}(x)} - \frac{\theta'(x)}{\hat{C}_{xy}(x)} \right| \leq K d_{\text{TV}}(\theta, \theta')
\]

Here \( q^1 \) and \( q^2 \) are the corresponding empirical PMFs generated by the observed locations running IBU starting with \( \theta \) and \( \theta' \), respectively. Note that the black-box sampling and obfuscation of the locations that, in turn, give rise to \( q^1 \) and \( q^2 \) do not depend on \( \theta \) and \( \theta' \) respectively. In particular, since both cases of obfuscating the real locations are done by the same channel, as \( n \to \infty \), we can assume \( \mathbb{P}(q^1 = q^2) \to 1 \). Let \( q = \lim_{n \to \infty} q^1 = \lim_{n \to \infty} q^2 \). Thus, we get an upper bound for \( (\ref{eq:lip-ibu}) \) w.p. 1 in the form of:

\[
\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{X}} q_y \hat{C}_{xy} \left( \frac{\theta(x)}{\hat{C}_{xy}(x)} - \frac{\theta'(x)}{\hat{C}_{xy}(x)} \right) \leq K d_{\text{TV}}(\theta, \theta')
\]

Similar to the proof of Lemma VII.3, we can ignore the columns of \( \hat{\mathcal{C}} \) which are all 0 as they would result in a probability of 0 for observing \( x_r \) in \( X \) in the output, which effectively will have no influence on the limit of IBU. Therefore, we can assume w.l.o.g. \( \min_{y \in \mathcal{X}} \sum_{z \in \mathcal{X}} \hat{C}_{zy}(z) > 0 \) for any \( \theta \in \Pi_\mathcal{X} \).
Therefore, setting \( K \in X \text{ to } C \), where
\[
\sum_{y \in X} q_y n^2 = n^2.
\]
Hence, by setting \( K_1 = 2M^2n^2 > 0 \), we satisfy
\[
d_L: \Gamma_{IBU}^1(\theta, \hat{C}) < K_1d_L: (\theta, \hat{C}) \Rightarrow d_{TV}(\Gamma_{IBU}^1(\theta, \hat{C}), \hat{C}) < K_1d_{TV}(\theta, \hat{C})
\]
As \( \hat{C} \) is generated via BA, by Theorem VII.2, we have a unique MLE that IBU converges to. Assuming IBU converges in \( N_{IBU} \) iterations, for all \( t \in \{0, \ldots, N_{IBU} - 1\} \), we will have positive \( \{K_2, \ldots, K_{N_{IBU}}\} \) satisfying:
\[
d_{TV}(\Gamma_{IBU}^t(\theta, \hat{C}), \hat{C}) < K_{t+1}d_{TV}(\theta, \hat{C})
\]
where
\[
d_{TV}(\Gamma_{IBU}^0(\theta, \hat{C}), \hat{C}) = d_{TV}(\theta, \hat{C})
\]

Therefore, setting \( K = \prod_{i=1}^{N_{IBU}} K_i \), gives us the desired result. □

**Theorem VII.6.** Optima3 is a uniformly continuous transformation w.r.t. \( L^1 \) norm, i.e., supposing Optima3 runs for \( N \) iterations, for all \( \epsilon > 0 \) there exists \( \delta > 0 \) such that for every \( \theta_0, \theta' \in \Pi_X \):
\[
d_L: (\theta_0, \theta'_0) < \delta \Rightarrow d_L: (\Lambda(\theta_0, N), \Lambda(\theta_0, N)) < \epsilon
\]

**Proof.** It is desirable for us to have the optimal channels obtained from BA starting with two close enough PMFs, \( \theta_0, \theta'_0 \in \Pi_X \), to be as close as possible, in order for us to be able to reduce to the setting of Theorem VII.4. We start by choosing a very small \( \epsilon' \) that we need to be able to have the optimal channels produced by BA with the two starting PMFs to be approximately the same, i.e., \( \lambda_{BA}(\theta_0, C_0) \approx \lambda_{BA}(\theta'_0) \). More explicitly, let \( E \) be defined as:
\[
E = \{ \epsilon > 0: d_C(\lambda_{BA}(\theta_0, C_0), \lambda_{BA}(\theta'_0)) < \epsilon \}
\]

where \( d_C \) is some metric to measure the distance between channels over the space \( C \) containing all encodings from \( X \) to \( X' \). Hence, our centre of attention remains at choosing some \( \epsilon' \in E \).

By Remark VII.1 if we have \( \epsilon' \) satisfying (19), there is \( \epsilon'(\epsilon') > 0 \) that satisfies
\[
\left| \text{RD}(X_{\theta_0}, d^*) - \text{RD}(X_{\theta'_0}, d^*) \right| < \epsilon'
\]
where \( X_\theta \) and \( X_{\theta'} \) are random variables on \( X \) with PMFs \( \theta \) and \( \theta'_0 \), respectively. Since we focus on the channels to be almost equal, we gauge the behaviour of the RD function taking very small steps. Therefore, it is reasonable for us to choose \( \epsilon' \) small enough for \( \epsilon'(\epsilon') > 0 \) to satisfy
\[
\exp\left\{ -W_r\left(-\frac{\epsilon'(\epsilon')}{\Delta} \right) \right\} < \frac{\epsilon}{4\Delta}
\]
where \( A, B \) are as in Lemma VII.2.1.

Therefore, by Corollary VII.2.1 and Remark VII.1 we have the uniform continuity of BA. In particular, for \( \epsilon' \in E \), we get a \( \delta_1 > 0 \) such that
\[
d_L: (\theta, \theta') < \delta_1 \Rightarrow d_C(\lambda_{BA}(\theta_0, C_0), \lambda_{BA}(\theta'_0)) \leq \epsilon'
\]

Let \( \epsilon > 0 \). As \( \epsilon' \in E \), we can say \( \lambda_{BA}(\theta_0, C_0) \approx \lambda_{BA}(\theta'_0) \), reducing to the condition needed to deploy Theorem VII.4. Indeed, by Theorem VII.4 and Remark VII.1 we can assert that we have \( \delta_2 > 0 \) such that
\[
d_L: (\theta, \theta') < \delta_2 \Rightarrow d_L: (\Gamma_{IBU}^t(\theta, \hat{C}), \hat{C}) < \epsilon
\]
Choosing \( \delta = \min\{\delta_1, \delta_2\} \) gives us that each step of Optima3 is a uniformly continuous transformation. Now an inductive argument, following the same line of extending the proof of Lemma VII.3 to that of Theorem VII.4 gives us the required result. □