Detailed Response to Reviewers for TDP Submission #20220620.00

Dear Review Team,

We thank you for your detailed and constructive feedback. This document includes point-by-point responses to each of the review team's comments. For clarity, we reproduced your original comments in black. The Major Changes to the Manuscript are listed below.

Major Changes to the Manuscript

1. **Increased focus and reduced length**: We reduced the length of the main body of the manuscript from 30 to 24 pages. Our revision focuses on the reasonableness of the privacy attacks and data protection considered, and the usefulness of protected data. We rewrote the abstract and discussion with a greater empirical focus.
2. **Improved literature review**: Per the reviewers’ suggestions, we have added citations for uniqueness, record linkage, and attribute disclosure in Section 4. We also added citations for location data privacy in Section 3.
3. **Revised Methodological Section 4**: We clarified the distinction between Singling Out and k-anonymity in the paper. We removed *k* from the Singling Out criterion to reflect this distinction, added discussion on the equivalence of Linkability and *k*-anonymity, and discussed how the prevention of Singling Out is a stronger requirement. Per Reviewer 1’s suggestion, we changed the calculation of Inference risk to use the maximum instead of the average increase in probability.
4. **Revised Empirical Section 5**: We updated Section 5 to reflect the changes in Section 4. To be consistent with our focus on usefulness (Major Changes to the Manuscript #1), we replaced the aggregation to counts method (since it does not produce person-level data) with microaggregation for a fair comparison to location coarsening.

We appreciate the opportunity to revise our manuscript and hope that our changes are satisfactory.

**Reviewer #1:**  
  
*Overall perspective*  
  
This is a clear summary of the legal and practical context of anonymization, some analysis of what GDPR regulations might mean statistically, and a case study applying those statistics to a specific case. It provides a useful example of the compromises necessary in practical anonymisation. However, the statistical analysis is both overly complicated and missing some important elements. Ultimately, this analysis all comes down to "have 2 or more observations on each unique set of identifiers, plus look at class disclosure" - I'm not sure that this is needed section 4 to come to this conclusion, although the actual applied work is of value. So, I think this is a useful addition to the literature, but the middle section needs substantial revision.

Thank you for your review. Per the Major Changes #3 and #4, we have revised Section 4 and 5.

*Specific Comments*

Abstract and sections 1, 2, 3

1. The introduction and section 2 are very clearly written and set out the  
   context very well. I like the continual focus on 'reasonableness'  
   throughout the paper; the authors are continually considering the utility  
   of their solutions.

Thank you, we have expanded the use of reasonableness of data protection and the usefulness of protected data throughout the paper.

1. Is this really the 'first assessment determining whether existing anonymization solutions for location data are capable of legally anonymizing location data? I thought quite a few people had studied it, and the literature review supports this. Is this perhaps the first attempt to define general rules and apply them to geographical data?

Thank you for this clarification. Based on our literature review, this paper is the first attempt to interpret legal anonymization criteria and apply them to anonymized location data. Other papers have examined legal criteria [11] or location data anonymization ([25], [34]) separately. We have edited the text on page 3, paragraph 3, to narrow this claim.

[11] Aloni Cohen and Kobbi Nissim. “Towards Formalizing the GDPR’s Notion of Sin-  
gling Out”. In: *Proceedings of the National Academy of Sciences,* 117 (2020), pp. 8344–  
8352. DOI: 10.1073/pnas.1914598117.

[25] Marco Fiore et al. “Privacy in trajectory micro-data publishing: a survey”. In: *Trans-  
actions on Data Privacy*, 13 (2020), pp. 91–149.

[34] Anna Monreale and Roberto Pellungrini. “A Survey on Privacy in Human Mobility”.  
In: *Transactions on Data Privacy,* 16(1) (2023), pp. 51–82.

Section 4

1. The referencing is a bit confusing here (and in the next section). N is used for columns rather than observations, y[m,n] appears to refer to both the specific row variable indexed by m and n, but also the subvector of matchable characteristics; later on d has two quite different meanings. Would be helpful to review these.

Per Major Change #3, we now use N for the number of rows and P for the number of columns in the data set Y. We use the notation to denote the subvector of matchable characteristics for record (see paragraph 3 of section 4.2). Section 4, pages 7-14 reflect these changes.

Singling out

1. is eq 2 over complicated? Don't we just need inf[z] >=2?

We believe you are referencing equation 1, not 2. Per Major Change #3, we have simplified Equation 1 to min[z] >=2. As Reviewer #2 suggested, we changed “inf” to “min” since the set **z** is finite, and a minimum value exists in the set. This change highlights the distinction between the singling out criteria (which includes all variables in the identifying set) and *k*-anonymity (which only includes quasi-identifiers).

1. the criterion (of a correct match) assumes that the attacker \*knows\* that it is a correct match - this is a generally unsolved problem in SDC and its legit to assume this but I would note it

Thank you, we now state this assumption in the first paragraph of Section 4.2 on page 9.

1. Table 2 has an obvious attribute inference from the class (group) disclosure in the top two rows - you tackle this later but suggest you note here that this is a later problem (or remove the column)

Thank you for pointing this out. We now mention this disclosure in the paragraph following Table 2 and refer the reader to Section 4.3, where we discuss attribute disclosure (Inference) in greater detail.

1. The authors make an important comment about k-anon vs their equation but surely there is no difference as you would assume that all the identifying/scanning vars are included in both k-anon or their set y[n, m]? If they are not identifying variables, why include them in the uniqueness set?

For singling out, GDPR requires that individuals cannot be isolated on any variable(s) including location data. *k*-anonymity is a popular protection method for location data and it is conservative to include all locations in the *k*-anonymity criterion (as we do for singling-out/linkability) since it is difficult to classify a given location as a QID or PI [34]. The difference between Singling Out and *k*-anonymity/Linkability is that sensitive attributes such as disease status are included in the Singling out criterion, making it a stronger requirement than *k*-anonymity/Linkability. We include this distinction in the paper in Page 11 paragraphs 2, 3, and 4.

Linkability

1. surely many-to-one does allow inference attacks via class disclosure (eg everyone visiting the covid testing centre was found to have covid, or everyone visiting the family planning centre was female)?

Thank you, we now state that the legal definition of linkability does not prevent class disclosure in the second to last paragraph of Section 4.2 (at the bottom of page 11).

1. it seems to me that the linkability criterion is just the Singling out criterion if the N terms used for Singling Out are those in the CI? If the CI has fewer vars than the Singling Out attributes then presumably no singling out => no linkability. I think the linkability criterion is a red herring - it's very closely tied to singling out. The only thing it seems to add is the probability of successful attribution based on the numbers in the set.

We agree that the prevention of Singling Out implies that one-to-one Linkability is prevented, where the probability of a successful attribution is 1/*k* for any CI set.

As described in our response to Point #7 above, the criteria for the prevention of Singling-Out is a stronger requirement than the prevention of Linkability. For example, when one applies k-anonymity to quasi-identifiers only and prevents Linkability for those quasi-identifiers, the probability of correct attribution is not 1/*k* if an adversary also has access to a variable not included in the original quasi-identifying set. We discuss this distinction in paragraphs 2, 3, and 4 on page 11, and provide additional discussion in our empirical analysis in Section 5.6.

1. "In practice, we suggest removing unique rows or non-essential columns in Y to prevent both types of linkages." - not really helpful; we can assume that the researcher would remove non-essential columns as a matter of good practice (if they're not doing that they are not going to get much out of the paper...)

Thank you, we have removed that paragraph from the paper.

Inference:

1. this surely isn't just limited to the dataset X, e.g. we can see in table 2 that there is a class disclosure in the equivalized units

Thank you for pointing this out. We have added an additional variable to the right-hand side of the conditional probabilities that captures any adversary background knowledge on the individual or attribute of interest outside of an external data set. This way, we isolate only the increase in probability of inferring sensitive information that arises from accessing the protected data set Y. We also note near the bottom of page 13 that the class disclosure you describe occurs without considering any external information.

1. p1012 para 1 - if you know the sex of an individual in X, isn't this  
   just linkability again ie the one-to-one?

Thank you, we have removed this statement. In the last paragraph on Page 12 we state that the prior probability should be reasonable to serve as a baseline for assessing Inference.

1. I'm very confused about this metric for risk. Why are you using the  
   average probabilities? If I were the data owner, I would be much more  
   concerned that some individuals can have their attributes identified with  
   probability 1, and not that most people have no significant prob of  
   attribute identification.

Thank you for this critique. To protect against the worst-case scenario, we altered the risk metric to measure the maximum increase in probability rather than the average. We have also adjusted our empirical analysis to show the maximum and results are on page 22.

1. as the authors note, k-anon doesn't prevent attribute disclosure  
   (especially via class disclosure - it would perhaps be better to consider  
   as a specific attack)

To address this concern, we have reframed the discussion around calculating our inference metric. We require specific attacks to be reasonable (see paragraph 1 of Section 4.3) and only study one specific attack. We refer the reader to more sophisticated attacks in the literature.

Legality

1. [28]'s definition of uninformativeness is very closely tied to the differential privacy definition; so it is not helpful when considering attack context (which the authors do in the rest of the paper)

Thank you, we have removed this paragraph from the paper. This is also consistent with the feedback from reviewer #2 that differential privacy “is likely above what would be determined as reasonable."  
  
Section 5 case study

I found this section clearly structured and written and would be suitable  
and useful to circulate to a wider audience.

1. Table 8 - would be really helpful to see the quantiles split between  
   SK vs Seoul so that we can get a better sense of how coarsening affects  
   utility - I'm guessing that within Seoul it has much less effect even at  
   97.5% than in SK as a whole

Thank you, we have made the change as suggested and have included the new table below. Note that we have replaced our aggregating to counts method with a microaggregation method (see our response to point 17 below).

The quantiles under location coarsening are dependent on the proximity of the original locations to a grid that is defined by the digits at any given number of decimals. The quantiles under microaggregation are dependent on the proximity of the original locations to each other (location density). So, we see lower quantiles for location coarsening when the area of interest is close to points on the grid (*e.g.*, in Seoul, see Figure 1 in the paper) and higher quantiles when the area of interest is far away from points on the grid (*e.g.*, in Seoul). For microaggregation, the quantiles are almost always smaller in the Seoul data than the full data since the location density of Seoul is much higher.

A screenshot of a computer

Description automatically generated with medium confidence

1. The coarsening analysis is interesting and instructive; however, I'm not  
   sure about the aggregation analysis. It seems to me that the key element  
   is dropping of the longitudinal component, not the aggregation. Wouldn't  
   you get the same results for both coarsening and aggregation if you  
   dropped the longitudinal links from both, as one should be the inverse of  
   the other?

Thank you, your question is correct. The two methods are equivalent if we drop the longitudinal links and do not convert to a counts data set. Since aggregating to counts produces data that is not at the individual level, we removed this method from the paper. In our new analysis, we drop the longitudinal component and perform microaggregation on the individual location tuples using the sdcMicro package in R. This allows us to focus on reasonable protection methods that keep person-level data. We include the new results on pages 16-22.

1. p1022 "one-to-one linkage or a many-to-one linkage, which prevents  
   Linkability" - only the latter prevents linkability but phrasing implies  
   both?

Thank you, we made the correction.  
  
Discussion

1. As the authors note, the Working Group also looked at randomization as well as generalization - this paper only considered the latter. Would be useful just to add a sentence explaining why (not enough space, too many options, not feeling it's a good idea?)

Per Major Changes to the Manuscript #1, we rewrote the discussion to focus more on our study's empirical findings and limitations. We added this limitation in paragraph 2 of the Discussion on page 23.  
  
Typos

1. p1001: "(Id.) "? Is this a missing reference?  
   p1021: second "d=1" should be "d=2"?

Thank you, we have corrected these typos.

We hope that the above changes are satisfactory and sincerely appreciate your review.

**Reviewer #2**

The introduction is very long about the discussion personal data vs. non-personal data, and this is further extended in Section 2. Then, Section 3 and 4 is also about topics and concepts well known. References are missing.

Thank you for your review. Please see the Major Changes to the Manuscript. We hope that we have satisfactorily addressed all your concerns.

1. For location privacy, see also the recent paper in the journal (and references therein):  
   A Survey on Privacy in Human Mobility. Anna Monreale, Roberto Pellungrini.  
   Transactions on Data Privacy 16:1 (2023) 51 - 82

Thank you, we now include this reference in multiple locations in the paper, including page 6 in Section 3.

1. I think that the authors need to further justify why they consider this location data and not just a standard database to propose/illustrate their approach.

We now note on page 3, paragraph 2, that the distinguishing features of location data are the longitudinal trajectory and granularity. For granularity, a single location (p=1) could identify someone. For longitudinal trajectory, we find that 90% of individuals in our data were uniquely identified based on just two locations. This contrasts to standard databases where several variables are needed to identify an individual.

As such, location data is especially difficult to anonymize, and our empirical section illustrates how reasonable protection methods for GDPR change the usefulness of location data. Showing that it is possible to legally anonymize location data means it is also feasible for more standard data sets.

1. In Section 3 the authors mention singling out and reference 12. The authors include some criticism to this definition, and I think that it is relevant. That "differential privacy and likely goes above what would be determined as reasonable", I agree (even this is a matter of the epsilon parameter and the big epsilon that some companies use with very simple data!). So, even for particular definitions, what is the appropriate level of privacy is a matter of disagreement.

Thank you, per Major Changes #1, we highlight our requirement for reasonableness of data protection throughout the paper.

1. The authors use "inf" in eq. 1. "min" works as well (the set is finite).

Thank you, we have changed “inf” to “min”. Also, we have used 2 (instead of k) since GDPR’s interpretation of Singling Out differs from k-anonymity.

1. Single out is just about unique records. So, maybe it is worth to refer to definitions of uniqueness by Skinner and  Elliot -- see (J.R.Statist.Soc. B (2002) 64 Part 4 855-867 A measure of disclosure risk for microdata) and references.

Thank you for the reference, we have included this in the last paragraphs of Section 4.1 and 4.2.

1. For linkability and record linkage there is all the literature by Winkler and other authors that have extensively used record linkage to evaluate disclosure risk (e.g. Torra). They discuss worst-case scenarios. Masking/protection does not avoid linkage.

Thank you. We now reference other linkability attacks at the end of Section 4.2 on page 11. We note in paragraph 3 of Section 4.2 that we only focus on a specific linkability attack.

1. Section 4.3 is mainly about attribute disclosure. There are different ways to evaluate disclosure. Authors one is one of them. Interval disclosure is another way (as described by several authors and implemented in e.g. sdcMicro by Templ). See also some of the surveys or books on data privacy.

Thank you for the suggestion. We have included a reference to Templ at the end of Section 4.3 on page 14.

1. There are quite a few alternatives for location data protection. The approach described in Section 5 is one of them. It is difficult to see in what extent the method is "good" in comparison with others, and about the compliance with the regulation, the authors already discuss at the end of the paper the difficulty.

To improve the clarity of our empirical analysis, we remove the aggregation to counts method (which destroys person-level data) and replace it with microaggregation applied to locations that are not longitudinally linked.

Both protection approaches are reasonable since they produce truthful person-level data. The usefulness of the protected location data is discussed on page 18, and location data represents a challenging problem for data protection.

1. In overall, the paper seems more an incomplete survey-like paper with a case study than really proposing something really novel. The discussion is interesting, but incomplete. There is extensive literature on risk assessment that seems to me missing in the text. Also on location/mobility data.

Thank you for your helpful feedback and citation suggestions. We have tried to address these concerns with our Major Changes to the Manuscript. We have now included much of the missing literature throughout the text (see pages 6, 9, and 11) and cited some application-based papers on location/mobility data (see pages XXX).

Overall, we have repositioned the abstract and discussion toward our empirical results. Our motivation is to provide reasonable interpretations of legal privacy criteria (Singling Out, Linkability, and Inference) based on the existing privacy literature. We apply these criteria to two reasonable privacy methods for location data and find that “XXX”. Our paper shows that XXX. We have reduced our claims at methodological novelty on page 2. Rather, as suggested by Reviewer #1, this paper is the first attempt to interpret legal anonymization criteria and apply them to anonymized location data. We have stated our limitations in the discussion Section on page 23.

We hope that the above changes are satisfactory and sincerely appreciate your review.