Detailed Response to Reviewers for TDP Submission #20220620.00

Dear Review Team,

We thank you for your detailed and constructive feedback and appreciate the opportunity to revise our manuscript. We have revised our paper to address your comments and we believe it has improved significantly based on your feedback. This letter contains a point-by-point response to each of the comments of the review team. We have reproduced your comments in black and our comments in blue.

Sincerely,

The Authors

**Major Changes to the Manuscript**

*All Sections*

* Revise the discussion/abstract/contributions for an empirical focus driven by:
  + reasonableness of protection
  + usefulness of protected data.
* Revised writing for clarity and succinctness.

*Section 3*

* Added citations for location data privacy

*Section 4*

* Removed the notion of k-anonymity from equation (2) and clarified distinction with singling out
* Fixed notation and some definitions in Section 4
* Added citations for uniqueness, record linkage, and attribute disclosure

*Section 5*

* Replaced aggregation to counts method with microaggregation to focus on protecting person-level data which is more useful.

**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 comments, we will address them separately below. Please also see the Major Changes to the Manuscript Addressing Sections 1 – 6.

*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 for this comment. We are glad you agree with our focus.

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 pointing this out. We are the first to attempt to anonymize location data *based on general legal criteria*. Other papers have examined legal criteria (*e.g.*,[12]) or location data anonymization (*e.g.*, [28]) but no one to our knowledge has examined both together. As you state, this is the first attempt to define general legal anonymization criteria and apply them to geographical data. We have edited the text in page 3, paragraph 3 to reflect your suggestion.  
  
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.

Thank you, we have adjusted our notation to remove these inconsistencies. We now use N for the number of rows, and P for the number of columns in the data set Y. We also note that we use the notation to denote the subvector of matchable characteristics for record (see paragraph 3 of section 4.2).

Singling out

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

Yes, inf[z] >= 2 is correct and we have changed equation 2 to this version. This also helps us make the distinction between our criteria (which requires all variables to be considered in the identifying set, in contrast to *k*-anonymity which only includes quasi-identifiers) – see our response to comment 9 below.

Based on the comments of Reviewer #2, we have also changed “inf” to “min” since the set **z** is finite and a minimum value exists in the set.r

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 immediately 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?

Thank you for this comment. We have moved our discussion of k-anonymity (and how it relates to linkability and singling out) to Section 4.2. Your comment highlights the distinguishing feature between the legal criteria for singling out and k-anonymity. The law (GDPR) requires that for singling out to be prevented, individuals cannot be isolated on any variable(s), not just the identifying variables (typically quasi-identifiers for k-anonymity). Page 11 paragraphs 2, 3, and 4 now reflect this difference compared to only using identifying variables.

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)?

We agree that the legal definition of linkability does not prevent class disclosure, and now note this within our paper in the last paragraph of Section 4.2 (at the top of page 12). We refer the reader to the inference section for further discussion.

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.

Thank you for your comment. The prevention of singling out implies that one-to-one linkability is prevented such that the probability of a successful attribution is 1/k for any CI set. However, it is possible to prevent linkability for a certain CI set while singling-out is not prevented, e.g., using k-anonymity applied to quasi-identifiers only. Then the probability of correct attribution is no longer bounded by 1/k if a different set of CI contains one or more of the non-quasi-identifying attributes.

According to our definition, k-anonymity prevents linkability for the CI, but not necessarily singling out. Our criteria for the prevention of singling-out is a stronger requirement than the prevention of linkability and the application of k-anonymity. We discuss this in paragraphs 2, 3, 4 on page 11.

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 for this clear comment. 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.

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, and instead state that the prior probability should be reasonable and conservative 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 comment. To protect against the worst case scenario, we have altered the risk metric to measure the maximum increase in probability rather than the average. We have also adjusted our empirical analysis to reflect this change. For additional clarity, we have removed the calculations of t-closeness and refer the reader to other ways of measuring the risk of inference.

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)

Thank you, we have reframed the discussion around calculating our inference metric using a specific attribute disclosure attack that is reasonable (see paragraph 2 of Section 4.3). We noted on page XXX that the readers can see 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 since we are considering a specific (reasonable) attack context. 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. The results show that…

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 for the helpful comment. We removed the aggregation to counts method from the paper because we want to focus on person-level data that has utility for many use cases, e.g., targeted advertising (cite XXX). You cannot achieve these use cases using aggregated counts data. Instead of aggregation to counts, we drop the longitudinal links from the locations and apply microaggregation using the sdcMicro package in R. Now, both of the privacy methods keep person-level data and we can compare the privacy and utility of locations with and without longitudinal links. We have included our new results below. In addition, we removed a lot of the mathematical notation and simplified the writing of the empirical section to focus on the results.

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, this was a mistake in the writing, and we have corrected it.  
  
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?)

We rewrote the discussion to focus more on the empirical findings instead of Section 4. We also added some sentences including these limitations.  
  
Typos

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

Thank you, we have corrected these typos.

Thank you for your helpful feedback and citation suggestions. We have now included much of the missing literature throughout the text and cited a few of the application-based papers on location/mobility data.

Overall, we have repositioned the abstract and discussion toward our empirical results. In Section 4, we have clarified the distinctions between the singling out and linkability criteria and k-anonymity, as well as changed the calculation of inference risk to use the maximum instead of the average increase in probability. We improved Section 5 by replacing the aggregating to counts method with microaggregation applied to individual locations which are not linked longitudinally. We find that “XXX”. We have reduced our claims at methodological novelty on page XXX and stated our limitations at the end of the discussion on page XXXX.

We hope that the above changes are satisfactory and sincerely appreciated 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 comments, we will address them separately below. Please also see the Major Changes to the Manuscript Addressing Sections 1 – 6.

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 have now included this reference on 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.

Thank you. We now note on page 3 paragraph 2 that the key feature of location data is the longitudinal trajectory. Unlike most identifying attributes, a single location (p=1) could identify someone. When multiple locations for a single person are considered, it is almost guaranteed that this person is unique in the data (we found that over 90% of individuals in our data were uniquely identified based on just two locations). As such, location data is especially difficult to anonymize, and doing so successfully indicates that legal anonymization is feasible for other more standard data bases.

Based on the review of [28] and the reference you suggest above, our work complements the large body of work on protecting location data by considering the protection from a legal (GDPR) perspective.

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 for the insightful comment. We also include this concept of reasonable privacy in the discussion and note that useful data is required.

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

Thank you for pointing this out. We have changed “inf” to “min”. Also, we have used 2 (instead of k) since the law’s interpretation is different than 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 paragraph of Section 4.1.

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. Linkability attacks are listed at the end of Section 4.2 on page 11.

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 our empirical analysis, we replaced the aggregation to counts method (which severely limits the use cases of the data) with microaggregation applied to locations that are not longitudinally linked. Both of these approaches can be considered reasonable since they produce person-level data that is useful for many applications (cite marketing). We have reproduced the tables comparing the protection methods here. The results show that…XXX

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 now included much of the missing literature throughout the text and cited a few of the application-based papers on location/mobility data.

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”. We have reduced our claims at methodological novelty on page XXX and stated our limitations at the end of the discussion on page XXXX.

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