**1) Overall Comments**

**The purpose of the paper is clear and its primary example is easy to follow.**

**I think there are a number of minor technical inaccuracies, though, and places where wording could be**

**clearer. Below, I've included my remarks page-by-page, separated between "Substantive Comments" and**

**"Editorial Comments".**

**2) Substantive Comments**

**pg. 1**

**"Beyond the Constitutionally mandated role of the decennial census, the US**

**Congress has mandated many other purposes for the data. For example, the**

**U.S. Department of Justice uses block-by-block counts by race for enforcing the**

**Voting Rights Act. More generally, the results of the decennial census, combined**

**with other data, are used to help distribute more than $675 billion in federal**

**funds to states and local organizations."**

**Does Congress explicitly mandate that the Decennial Census be used for enforcement of the VRA,**

**or is that a decision that was made in implementing an interpretation of the VRA? It often seems**

**unclear which of these is the case.**

**pg. 2**

**"The Bureau has traditionally used cell suppression to**

**protect privacy in situations such as this: the cells of statistical tables that result**

**from small counts are suppressed and not report"**

**The transition from talking about reporting the average salary of a number of people**

**to talking about suppressing counts (rather than averages) is unclear. I'm also unsure why**

**cell suppression is the only legacy technology discussed here. Why are legacy swapping, legacy**

**noise infusion, legacy top-coding etc not mentioned?**

**pg. 2**

**"In 2003, Dinur and Nissim showed that simple cell suppression is not sufficient**

**to protect the underlying confidential data collected and used by a statistical**

**agency to produce official statistics [2]."**

**The kinds of reconstruction attacks considered by Dinur and Nissim would certainly work**

**against most cell suppression systems, but Dinur and Nissim don't specifically consider cell**

**suppression (or any specific legacy technique) at all, and this sentence makes it sound like they did.**

**In Dinur & Nissim's models, they assume that subset-sum queries are perturbed by noise of bounded**

**magnitude.**

**pg. 2**

**"To the contrary, they showed that once an**

**agency publishes more than a critical number of**

**statistics, the underlying confidential data can be**

**reconstructed by simply nding a consistent set of**

**microdata**

**that, when tabulated, produce the official statistics."**

**Dinur & Nissim look for a data set consistent with noisy estimates of subset-sum queries;**

**they don't look for data that exactly matches the tabulated statistics, although the two**

**approaches are closely related.**

**pg. 2**

**"While it is mathematically impossible prevent reconstruction of the under-**

**lying data"**

**As stated this is not true. What is true is that it is mathematically impossible to prevent**

**a highly accurate reconstruction from being carried out with high probability while also**

**publishing "too many" highly accurate statistics.**

**pg. 2**

**"So how much noise needs to be added to protect privacy? Three years later,**

**Dwork, McSherry, Nissim and Smith answered that question."**

**This is misleading; it makes it sound as if it is possible to protect or not protect privacy,**

**but a major part of the point to the DP literature is acknowledging that privacy and accuracy are**

**both on a sliding scale. What Dwork et al answered was more like "how much noise needs to be added to**

**guarantee a specified degree of privacy."**

**pg. 4**

**"If statistics are**

**highly constrained, the only a single reconstruction will be possible, and that**

**reconstruction should be the same as the underlying microdata used to create**

**original table."**

**It's not the statistics that are constrained; they simply are what they are. Rather, the released**

**statistics (assuming no noise infusion) tightly constrain the space of possible solutions to**

**the SAT problem being used for the reconstruction. Also a few grammatical/spelling errors in**

**this sentence (e.g. the -> then), and 'should' should be replaced by 'will'.**

**pg. 4**

**"For example, statistic 2B states that there are 3 males living in the geography.**

**Because age is reported to the nearest year, and age must necessarily be [0..115],**

**there are only a inite number of possible age combinations, specically:"**

**The constraints on age (0-115 and integer) were not stated previously in the paper. They appear**

**suddenly and without motivation; should preface with an explanation.**

**pg. 5**

**"Once the constraints in the statistical table are turned into s-expressions, Sugar**

**encodes the s-expressions into a set of Boolean constraints that can be fed into**

**a SAT-solver."**

**SAT may be unfamiliar to many readers. It should be formally introduced and explained before**

**being discussed in this fashion.**

**pg. 6**

**"Although this conversion is not space effcient, it is fast,**

**and the uniary notation makes it easy to encode integer inequalities as simple**

**functions of Boolean variables."**

**I would be careful about suggesting that this conversion is fast; some readers may interpret that**

**as suggesting that this unary representation is an approach that will scale comfortablty**

**to very large instances, but that seems unlikely.**

**pg. 6**

**"This is called "breaking symmetry" in the formal methods literature."**

**'formal methods literature' is very general; is this the SAT solver literature specifically,**

**formal logic, some other literature...? Also, the 'breaking symmetry' phrase could use a citation.**

**pg. 7**

**"Sugar then translated this into 6,740 Boolean variables consisting**

**of 252,478 clauses in the conjunctive normal form (CNF)."**

**CNF may be unfamiliar to many readers - should formally define and explain it.**

**pg. 7**

**"Translating the constraints into CNF allows them to be solved using either**

**a SAT (satisability), SMT (satisability module theories), or MIPM (mixed**

**integer programming model) solver."**

**Technically any solver for any arbitrary NP-complete problem could be used, in case you want to**

**point that out. For math programming jargon, I would say MIP or MILP rather than MIPM.**

**pg. 7**

**"Many solvers**

**can now solve CNF systems with millions of variables and clauses in just a few**

**minutes."**

**I would be careful about suggesting this generally, since there is likely to be considerable**

**problem-by-problem variation in modern SAT solvers' performance (similar to the variation seen**

**in solving large-scale MILPs with Gurobi or cplex). Maybe adding the word**

**"some" before CNF here would soften the wording appropriately.**

**pg. 7**

**"If the solution universe contains a single possible solution, then the**

**published statistics completely reveal the underlying condential data"**

**This is true if cell suppression was the legacy technique applied, but it is not true**

**for legacy swapping or legacy noise infusion.**

**pg. 7**

**"If the equations have no solution, the set of**

**published statistics are inconsistent."**

**I think it is important to note here that inconsistency does not imply that a high-quality**

**reconstruction is not possible; it just means that the published information has to be used in a "soft"**

**sense to drive something like an objective function rather than being used as hard constraints.**

**pg. 8**

**"Table 1 is actually over-constrained:"**

**It's not the table that's constrained; rather, the table over-constraints the solution universe.**

**pg. 8**

**"There are three approaches for defending against a database reconstruction:**

**publish less statistical data, and apply noise (random changes) to the statistical**

**data being tabulated, or apply noise to the results after the tabulation. We**

**consider them in order below."**

**The switch between "and" and "or" in the first sentence here is awkward. I think all legacy DA techniques**

**should be listed here as well (cell suppression, swapping, non-provable noise infusion, top-coding, etc),**

**and a distinction should be drawn between those techniques with provable guarantees for very general**

**attacker models (formally private methods) and techniques without those guarantees (legacy DA).**

**pg. 8**

**"Although it might seem that publishing less statistical data is a reasonable**

**defense against the DRA, this choice may severely limit the number of tabula-**

**tions that can be published."**

**This would be more convincing with some kind of quantitative relationship given between how much data**

**can be published while avoiding a highly probable DRA.**

**pg. 9**

**"large population, it may be computationally infeasible to determine when the**

**intersection of all possible reconstructions identies individuals."**

**It's not very clear what is meant by "the intersection of all possible reconstructions".**

**pg. 9**

**"Input noise infusion doesn't prevent**

**database reconstruction, but it limits the value of the reconstructed data by**

**creating uncertainty for each of the reconstructed values."**

**But this is all that formal private methods do as well; they create uncertainty about which database**

**is the true database. Whether that uncertainty is created through input or output noise infusion,**

**it still can legitimately defend against a DRA. Choosing between input and output noise infusion is**

**more a matter of efficiency than one being preventative and the other not.**

**pg. 9**

**"For example, if a random oset in the range of ???2 . . . + 2 is added to each**

**record of our census and the reconstruction results in individuals of ages (7, 17,**

**22, 29, 36, 66, 82) or (6, 18, 26, 31, 34, 68, 82)."**

**Why is it assumed in this example that the infused noise is drawn from a bounded domain rather than from**

**a geometric distribution or some such? Also, this is not a complete sentence.**

**pg. 9**

**"An attacker would presumably**

**take this into account, but they would have no way of knowing if the true age**

**of the youngest person is 6, 7, 8, 9 or 10."**

**I'm having trouble following this example. How is this being solved? Are the perturbation bounds**

**being used to loosen some constraints and incorporate them as inequalities? Why is the attacker's**

**uncertainty about the youngest person between 6 and 10 here and not 6 and 7?**

**pg. 9**

**"First, the**

**resulting statistical publication is likely no longer consistent, so the reconstruc-**

**tion of any database may no longer be possible."**

**This is not true; highly accurate reconstructions are possible with inconsistent data. The available**

**information just has to be used to drive something like an objective function rather than as**

**a set of hard constraints. Even in Dinur & Nissim's original work, they assumed a form of output**

**noise infusion and showed that small random perturbations weren't sufficient to protect the true data,**

**even though they yield an inconsistent set of final statistics.**

**pg. 9**

**"Second, even if a database is**

**reconstructed, it is likely not the correct database."**

**This is confusing use of the term 'reconstructed'. I think 'reconstructed' should be reserved**

**for procedures that generate microdata that largely matches the true database. When describing microdata**

**that was generated but is wrong, some other term should be used - perhaps 'constructed' (no 're').**

**pg. 9**

**"In 2003 Irit Dinur and Kobbi Nissim [2] showed that the underlying condential**

**data of a statistical database can be reconstructed with a surprisingly small num-**

**ber of queries."**

**Should indicate the actual number of queries needed to drive their results rather than describe it**

**as "surprisingly small."**

**pg. 9**

**"Statistical tables create the possibility of database reconstruction because**

**they form a set of constraints for which there is ultimately only one exact**

**solution"**

**This is the kind of reconstruction attack exhibited in this paper, and it is similar to the kinds**

**of reconstruction arguments given in Dinur & Nissim, but it is misleading to suggest that this is the**

**only kind of reconstruction attack possible.**

**pg. 9**

**"Dinur and Nissim found that, if a database is modeled as a string of ???? bits,**

**then at least**

**???**

**???? bits must be modied by adding noise to protect persons from**

**being identied."**

**I don't think this is correct. Dinur & Nissim don't assume the underlying database is perturbed**

**and published, but rather that the answers to subset-sum queries taken over the underlying database**

**are perturbed and released.**

**pg. 10**

**"This paper does not use that attack technique, but instead creates a system of**

**constraints and solves them with a solver that can solve NP-hard problems."**

**Since a SAT solver is being used, it might be more precise to say**

**"that can solve NP-complete problems"; there is no general solver for all possible NP-hard problems.**

**pg. 10**

**"The vast quantity of data products pub-**

**lished by statistical agencies each year may give a determined attacker more**

**than enough constraints to reconstruct some or all of a target database and**

**breach the privacy of millions of people."**

**The focus on 'constraints' here is misleading; the issue is the amount of information released,**

**of which exact information that can be used as constraints is just one form.**

**pg. 10**

**"Although a suite of traditional disclo-**

**sure avoidance technique is often suffcient to defend against a cursory attack,**

**cell suppression and generalization are not secure against this kind of attack"**

**It's a bit confusing to only introduce a new DA technique (generalization) in the**

**conclusion of the paper - it should be introduced and explained earlier. Also, 'technique'**

**needs an 's' on it.**

**pg. 10**

**"To**

**protect the privacy of respondent data, statistical agencies must use some kind**

**of noise infusion."**

**The phrasing here is misleading. Statistical agencies could just publish the number '1' for every count**

**regardless of what the true count was, and that would protect respondent privacy without needing**

**noise infusion. The issue here just seems to be that noise infusion allows for publshing more data than**

**traditional DA while still defending against reconstruction attacks. Maybe more importantly, formally**

**private noise infusion specifically is the only game in town for doing this and in the process**

**securing mathematically provable, precisely stated privacy guarantees.**

**pg. 10**

**"Formal privacy methods, especially dierential privacy, were**

**specically designed to to control this risk and, as both of our noise-infusion**

**examples illustrate, they do so by systematically expanding the universe of so-**

**lutions to the DBA constraints."**

**Formal and differential privacy should be defined, explained, and referred to much earlier in the paper;**

**it is very confusing to not have referred to them for most of the 10 pages but to begin describing them**

**on page 10 in the concluding paragraphs. I also think 'DBA' should be 'DRA', and the discussion of**

**constraints here be removed, since that kind of reasoning is very particular to the style of attack**

**described in this paper.**

**pg. 10**

**"In this expanded universe, the real condential**

**data are but a single solution, and no evidence in the published data can improve**

**an attacker's guess about which solution is the correct one."**

**This is not true. Very particular to the kind of attack carried out in this paper. Other attacks**

**can take advantage of information to choose a 'most plausible' database when several (or none)**

**are consistent with the published tabulations.**

**pg. 11**

**"Although the SAT problem is not**

**solvable by algorithms in polynomial time"**

**This assumes P != NP, which is widely believed but not known. It would also help to clarify that this is**

**specifically a worst-case description.**

**pg. 11**

**"SAT solvers combine a variety of these**

**techniques into one complex process, resulting in polynomial time solutions for**

**the SAT problem in many cases."**

**'polynomial time' is a property of algorithms, not of solutions, and it would be hard to carefully**

**describe in what sense and for what problems SAT solvers behave similarly to a polynomial-time**

**algorithm. I would just say SAT solvers work well and reasonably quickly for a large variety**

**of problem instances and up to reasonably large instance sizes.**

**pg. 13**

**In the paper the minimum age was given as 0, but here in the code it appears to be 1? Also, duplicate**

**misspelled as dupliate near the bottom of this page.**

**3) Editorial Comments**

**Throughout the paper, I would replace 'reconstruction' with the acronym 'DRA'. You define it early**

**in the paper but rarely use it later.**

**'unary' is misspelled as 'uniary' in several places.**

**pg. 1**

**This is an extremely long, awkwardly worded sentence:**

**"In 2020 the Census Bureau will conduct the constitutionally mandated decen-**

**nial Census of Population and Housing, with the goal of counting every person**

**once, and only once, and in the correct place, and to fulll the Constitutional**

**requirement to apportion the seats in the U.S. House of Representatives among**

**the states according to their respective numbers."**

**Consider breaking it up into several sentences. It would also be helpful to use a more specific term than 'numbers'.**

**pg. 1**

**"In addition to collecting and distributing data on the American people, the**

**Census Bureau is charged with protecting the Privacy condentiality of survey**

**responses."**

**'Privacy confidentiality' is redundant. Privacy should be lowercase and one of these two nouns removed.**

**pg. 1**

**"Specically, all Census publications must uphold the condentiality**

**standard specied by Title 13 of the U.S. Code, which states, in part, that Bu-**

**reau publications are prohibited from identifying \the data furnished by any**

**particular establishment or individual.""**

**The phrasing here is confusing; it makes it sound as if the Bureau is doing the 'identifying', but**

**the Bureau's charge is to stop others from identifying, not to not identify itself.**

**pg. 2**

**"Upholding this condentiality requirement frequently poses a challenge, be-**

**cause many statistical can inadvertently provide information in a way that can**

**be attributed to a particular entity"**

**Missing a word: statistical \*releases\*?**

**pg. 2**

**"However, if there is only one bricklayer, than reporting the average salary of a**

**bricklayer will allow anyone who sees to statistical product to infer that person's**

**salary"**

**Change "to" to "the"**

**pg. 2**

**"a data publisher can add noise to the published results so that the**

**reconstructed data will not reveal the actual condential responses that was**

**used to create the published tables."**

**"will not reveal" is vague. Would be better to specifically talk about limiting the probability**

**of a highly accurate reconstruction of the true data.**

**pg. 3**

**"To help understand the importance of adopting formal privacy methods, in**

**this article we presents a"**

**Remove the 's' on presents.**

**pg. 3**

**"We show that even a relatively small number of constraints**

**results in an exact solution the blocks' inhabitants."**

**Change 'solution' to 'reconstruction'**

**pg. 3**

**"Finally, we show how differ-**

**ential privacy can protect the published data by creating uncertainty. Finally,**

**we discuss implications for the decennial census."**

**Redundant to say "Finally" twice here. Also, should Decennial Census be capitalized?**

**pg. 3**

**The use of capitalization in Table 1 is inconsistent.**

**pg. 4**

**"To perform the database reconstruction attack, we view the attributes of the**

**persons living on the block as a collection of free variables."**

**'free variables' is a term specific to SAT, logic, and the related literatures;**

**should either define it or just say 'variables' (which is a much more generally recognized term**

**and would convey the same meaning here)**

**pg. 4**

**"However, within the 253,460 possible age combinations, there are 30 combi-**

**nations that satisfy the constraint of having a median of 30 and a mean of 44**

**(see Table 1)."**

**Remove 'However,' add an 's' to constraint, add 'only' before '30 combinations'**

**pg. 5**

**"We use a language called Sugar [8] to encode the constraints into a form that**

**can be processed by our solver."**

**I assume Sugar is only compatible with SAT solvers? Should clarify what is meant by 'solver' here**

**; it's a very general term.**

**pg. 5**

**"For example, equation 1 is can be represented this way:"**

**Drop 'is'.**

**pg. 6**

**"This does a good job**

**;; eliminating dupliate answers that"**

**Duplicate is misspelled.**

**pg. 7**

**"However, in**

**this case, there is a single satisfying assignment that produce the statistics in**

**Table 1."**

**Add an 's' to produce.**

**pg. 8**

**"Statistical agencies have long used suppression (censoring) in an attempt**

**to provide privacy to those whose attributes are presented in the microdata,**

**although the statistics that they typically drop are those that are based on a**

**small number of persons. How effective is this approach?"**

**Why is the term 'censoring' introduced? It seems unnecessary and just complicates the explanation.**

**Also, 'presented' should be 'present'.**

**pg. 9**

**"Considering statistic 1A, input noise infusion might result with a median 28 . . . 32**

**and a mean 36 . . . 40."**

**I think "with" should be "in".**

**pg. 9**

**"In our example, each record is contains 11 bits of data, so the**

**condential database has 77 bits of information."**

**Remove 'is'.**

**pg. 10**

**"With the dramatic improvement in both computer speeds and the effciency of**

**solvers in the last decade, database reconstruction attacks on statistical databases**

**are no longer a theoretical danger."**

**'solvers' is a very general term. Should make it more specific.**

**pg. 11**

**"Addition-**

**ally, CDCL and its predecessor algorithm, DPLL, are both provably complete**

**algorithms and will always return either a solution or \Unsatisable" if given**

**enough time and memory"**

**I would replace "and" with ": ", since the latter half of the sentence is defining what it means**

**for a SAT solver to be complete.**

**pg. 14**

**"So we kow that the average of FEMALE\_AGE2 and FEMALEA3 is 30"**

**'know' is missing an 'n'.**

**pgs. 16, 18, 20, 22**

**Each of these pages have a comment like ";; that each ID maps to a female." I believe female was**

**copy/pasted from earlier pages and is not correct on these pages.**

**pg. 22**

**Comments in Sugar code near the top of the page run outside of the page margins to the right.**