Differential Privacy in the Real World: The 2018 End-to-End Census Test

John M. Abowd
Chief Scientist and Associate Director for Research and Methodology
U.S. Census Bureau
American Association for the Advancement of Science
Annual Meeting Sunday, February 17, 2019 8:00-9:30

The views expressed in this talk are my own and not those of the U.S. Census Bureau.
Acknowledgments

Differential Privacy
The Disclosure Avoidance System Relies on Injecting Noise with Formal Privacy Rules

- Advantages of noise injection using differential privacy:
  - Privacy guarantees are closed under composition
  - Privacy guarantees are robust to post-processing
  - Privacy guarantees are future-proof
  - Privacy guarantees are provable and tunable
  - Privacy guarantees are public and explainable
  - Protects against database reconstruction attacks (tunable)

- Disadvantages:
  - Entire country must be processed at once for best accuracy
  - Every use of the private data must be tallied in the privacy-loss budget
Technical Challenges

- Hierarchical and table consistency
- Invariants (main algorithmic challenge in combination with hierarchy)
- Asymptotic consistency as $\varepsilon$ (privacy loss) gets large
- Existence proofs for solutions
- Workload optimization, especially for join tables (persons x households)
- Many implementation issues, not discussed here
Summary of Important Technical Details

• Central differential privacy implementation with a controlled total privacy-loss budget

• Relevant algorithmic definition is bounded $\varepsilon$-differential privacy (total population of the largest geographic area is public)

• Semantic privacy guarantee is $[-2\varepsilon, 2\varepsilon]$ by properties of bounded differential privacy
  • Complicated by occupied household invariant that was not removed

• All algorithms, code, and parameter values will be released with the test files for the 2018 End-to-End Census Test

• All parameter and invariant settings to be reviewed based on feedback from the E2E test files and released algorithms
Algorithm Comparison Using Public 1940 Census Data
Two Candidate Algorithms

• Block-by-block (also called bottom-up)
  • DP applied to all tables at the most detailed geographic level (blocks)
  • All aggregations built from those tables
• Top-down
  • DP measurements taken at all levels of the geographic hierarchy
  • Large-scale optimization problem solved to allocate microdata records to solution tables respecting invariants, table consistency, non-negativity, and integer constraints
• In these tests, all invariants were imposed at the enumeration-district level (similar to the modern definition of block groups)
TOP-DOWN DIFFERENTIAL PRIVACY ALGORITHMS
(1940 CENSUS DATA)

DISTRICT-BY-DISTRICT DIFFERENTIAL PRIVACY ALGORITHMS
(1940 CENSUS DATA)
Analyses Supporting the 2018 End-to-End Census Test
Implementation Decisions for 2018 End-to-End Census Test

• Population invariant at the county level (Providence, RI is the only county in the test)
• No voting-age invariant at any level
• Number of housing units invariant down to the block (design constraint due to operation of LUCA and address canvassing)
• Number of occupied housing units invariant (could not be relaxed in time to meet E2E production deadlines)
• Number and type of group quarters invariant down to the block (same design constraint as number of housing units)
• Global privacy-loss budget ($\varepsilon$) 0.25
• Allocation to PL94-171 100% (no other tables being released)
Accuracy v. Privacy Loss for Rhode Island (2010 Census) using the 2018 E2E Test Disclosure Avoidance System PL94-171 redistricting data at the block level
Accuracy v. Privacy Loss for Rhode Island (2010 Census) using the 2018 E2E Test Disclosure Avoidance System

PL94-171 redistricting data at the tract level
Accuracy v. Privacy Loss for Rhode Island (2010 Census) using the 2018 E2E Test Disclosure Avoidance System

PL94-171 redistricting data at the county level
Accuracy v. Privacy Loss for Rhode Island (2010 Census) using the 2018 E2E Test Disclosure Avoidance System

PL94-171 redistricting data at the state level
Accuracy v. Privacy Loss for Rhode Island (2010 Census) using the 2018 E2E Test Disclosure Avoidance System

PL94-171: redistricting data, SF1: P12 age x sex data and P1 population data
Managing the Tradeoff
Basic Principles

• Based on recent economics (2019, *American Economic Review*)

• The marginal social benefit is the sum of all persons’ willingness-to-pay for data accuracy with increased privacy loss

• The marginal rate of transformation is the slope of the privacy-loss v. accuracy graphs we have been examining

• This is exactly the same problem being addressed by Google in RAPPOR or PROCHLO, Apple in iOS 11, and Microsoft in Windows 10 telemetry
Marginal Social Benefit Curve

Social Optimum: MSB = MSC (0.25, 0.64)

Production Technology
Production Possibilities and Social Benefit Curves

Social Optimum:
MSB = MSC
(0.25, 0.64) Block
(0.25, 0.98) Tract

Production Technology
Legislative Redistricting

• In the redistricting application, the fitness-for-use is based on
  • Supreme Court one-person one-vote decision (All legislative districts must have approximately equal populations; there is judicially approved variation)
  • *Is statistical disclosure limitation a “statistical method” (permitted by Utah v. Evans) or “sampling” (prohibited by the Census Act, confirmed in Commerce v. House of Representatives)? Answer: statistical method (permitted)*
  • Voting Rights Act, Section 2: requires majority-minority districts at all levels, when certain criteria are met

• The privacy interest is based on
  • Title 13 requirement not to publish exact identifying information
  • The public policy implications of uses of race, ethnicity and citizenship tabulations at detailed geography
More Background on the 2020 Disclosure Avoidance System

• September 14, 2017 CSAC (overall design)
  https://www2.census.gov/cac/sac/meetings/2017-09/garfinkel-modernizing-disclosure-avoidance.pdf#

• August, 2018 KDD’18 (top-down v. block-by-block)
  https://digitalcommons.ilr.cornell.edu/ldi/49/

• October, 2018 WPES (implementation issues)
  https://arxiv.org/abs/1809.02201

• October, 2018 ACMQueue (understanding database reconstruction)
  https://digitalcommons.ilr.cornell.edu/ldi/50/ or
  https://queue.acm.org/detail.cfm?id=3295691
Thank you.

John.Maron.Abowd@census.gov
Selected References


Backup Slides
Hierarchical and Table Consistency

• Tables are consistent at all levels of geography and for all coarsening of detail
• The DP noise is infused into measurements (contingency tables) at each level of geography (uses closure under composition)
  • Global privacy-loss budget is shared across all measurements with correct accounting
  • Geometric mechanism noise (discrete version of Laplace noise)
• Resulting tables are post-processed (uses robustness to post-processing)
  • To satisfy all invariants
  • To contain only non-negative value
  • To add up properly along all dimensions
  • The large-scale optimization problem is solved partially analytically and partially using Gurobi
• One set of consistent micro-data is produced that tabulates exactly to the post-processed tables
• These micro-data are sent to the production tabulation system
Invariants

• An invariant is an output of the disclosure avoidance system that exactly matches the query answer in the confidential data
  • Shorthand: no disclosure avoidance was applied

• Public documents confirm that total population, voting-age population, number of housing units, number of occupied housing units, and number and type of group quarters were all invariants at the block level in 2000 and 2010 Census publications. (These, plus race and ethnicity, were also invariant in the 1990 Census.)

• We now understand that invariants seriously compromise the confidentiality protection (differential privacy or traditional disclosure avoidance)
How Invariants Compromise Confidentiality

• For traditional methods: database reconstruction is much easier

• For differential privacy:
  • Secrets like (Alice lives in block A and Alice is a citizen) do not get the differential privacy protection if either block population or citizen population is an invariant
  • Unrelated secrets (those not involving invariants at all) can also be compromised
  • When the differential privacy protection does not apply, the meaningful bounds on the accuracy of inferences about Alice’s residence or citizenship are much more complex than when there are no invariants

• Eliminating invariants eliminates this problem, allows for more efficient use of the privacy-loss budget
Hierarchical Consistency + Invariants

- The combination makes the post-processing algorithms extremely complicated
- There are integer, equality and inequality constraints in the equation system
- Proofs of existence are not available for every invariant and/or consistency configuration
- When existence fails empirically, the system reverts to an approximate solution for a configuration that has the smallest feasible subset of the problem
Asymptotic Consistency

• The system should have the property that when the global privacy-loss budget goes to infinity, the solution goes to the exact answer to the query workload (perfect accuracy)

• That is not automatic for the top-down algorithm

• To achieve asymptotic consistency, the most general histogram must be estimated at every level of geography with a proportional allocation of the privacy-loss budget

• As \( \varepsilon \) grows, the accuracy of the most general histogram also improves at every level of the geographic hierarchy
Existence Proofs

• Differential privacy can always be applied to every measurement needed by the top-down algorithm

• However, the equation system used for the post-processing need not always have a solution consisting entirely of non-negative integers

• We have existence proofs for some configurations

• In general, when there are inequality constraints, existence is not guaranteed

• Approximate solutions are computed over a minimal subset

• Rate of approximation will be in the error metrics
Workload Optimization

• Most of the work for the 2018 End-to-End Census Test was done at the person-level, and for the PL94-171 (redistricting) workload

• There are many more person-level tables in the proposed Summary File 1

• There are also household-level tables (based on householder/person 1), and joins of household and person tables (counts of persons by characteristics of the householder)
  • The household tables will require workload optimization (probably using the high-dimensional matrix method https://arxiv.org/abs/1808.03537)
  • The joins will require other algorithmic extensions (probably using hierarchical counts-of-counts technique https://arxiv.org/abs/1804.00370)