# Pain-Free Random Differential Privacy with Sensitivity Sampling

Benjamin I. P. Rubinstein
University of Melbourne, Australia

Francesco Aldà
Ruhr-Universität Bochum, Germany

## Problem & Contribution

- Generic mechanisms provide differential privacy, but require bounding global sensitivity of target.
- New sensitivity sampler instead probes target
  → Automatic + Random DP + Improved utility
- R package diffpriv released on CRAN, GitHub.

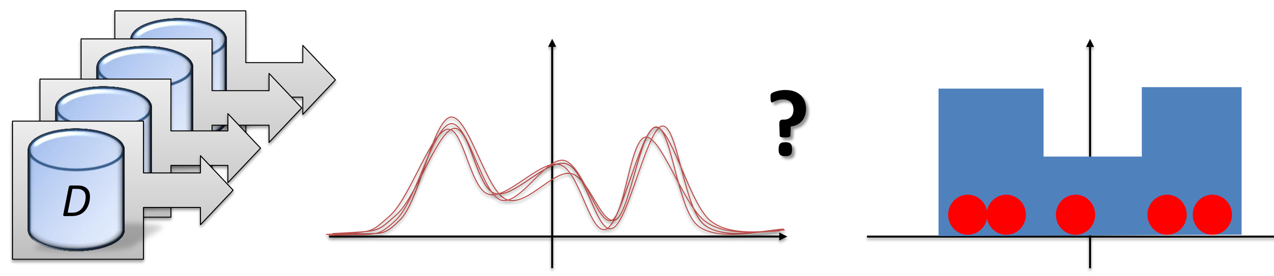
## Privacy: Who Cares?


- DP deployed: Google, Apple, Uber, etc.
- Active groups: Harvard, Berkeley, CMU, Weizman, Oxford, UCSD, Stanford, etc.
- 2017 Gödel Prize to Dwork et al.

## Differential Privacy [Dwork et al. 2006]

*Release aggregate info, protect individual data.*

- Database $D$: a sequence of $n$ records, some domain
- Neighbouring DBs $D \cong D'$: differ on one record
- Mechanism $M$: maps DB $D$ to random response $R \in B$ some normed space
- M has $\varepsilon$-differential privacy if, $\forall D \cong D', \forall R \subseteq B$ $\Pr(M(D) \in R) \leq \exp(\varepsilon) \cdot \Pr(M(D') \in R)$ where $\varepsilon > 0$




*Response indistinguishable on changing one record*

- Semantic guarantee: Limits what adversary can do with: unbounded computation; knowledge of DB up to a record; knowledge of $M$ up to randomness.

## Bounding Sensitivity for Generic Mechanisms

Prohibitive math analysis

- Privatise a target function $f$ maps DB $D$ into $B$
- Sensitivity $\Delta f(D, D') = \|f(D) - f(D')\|_B$
- DP: calibrate randomisation to $\bar{\Delta} f = \sup_{D \cong D'} \Delta f(D, D')$
- Laplace mechanism: add zero-mean $\mathrm{Lap}(\bar{\Delta} f / \varepsilon)$ to $f$
- Others: Gaussian, exponential, Bernstein mechanisms

## Random Differential Privacy [Hall et al. 12]

M has $(\varepsilon, \gamma)$-RDP for $\varepsilon > 0$, $\gamma \in (0,1)$ if whp $1-\gamma$ over $D \cong D'$: $\forall R \subseteq B$, $\Pr(M(D) \in R) \leq \exp(\varepsilon) \cdot \Pr(M(D') \in R)$

- DP: indistinguishable responses over all DB pairs
- RDP: indistinguishability over all–*but pathological*-DBs

## Sensitivity-Induced Private $M$: if for $D \cong D'$,

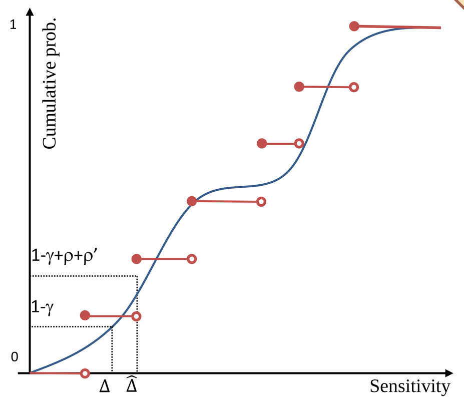
$\Delta f(D, D') \leq \Delta$ implies $\varepsilon$-DP holds for $M_\Delta$ on pair $D, D'$

- $\Pr(\Delta f(D, D') \leq \Delta) \geq 1 - \gamma$ implies $M_\Delta$ has $(\varepsilon, \gamma)$-RDP
- Given CDF of $\Delta f(D, D')$ get $\Delta$ by inverting CDF at $1-\gamma$
- Empirical CDF of iid sample estimates CDF uniformly

## Algorithm: Sensitivity Sampler

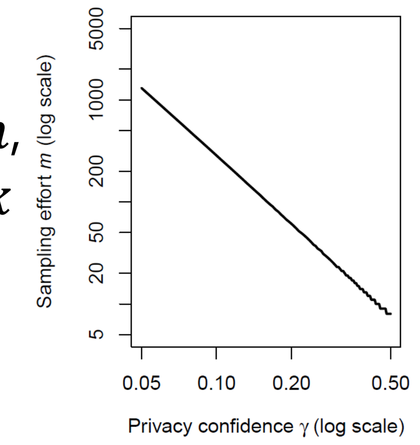
<u>Input:</u> Target $f$, DB size $n$, distribution $P$, sample size $m$, order statistic index $k$,

1. Repeat $i = 1 \ldots m$
   a) Sample $D \cong D'$ from $P$
   b) $G_i = \Delta f(D, D') = \|f(D) - f(D')\|_B$
2. Return estimated sensitivity $\Delta f = G_{(k)}$

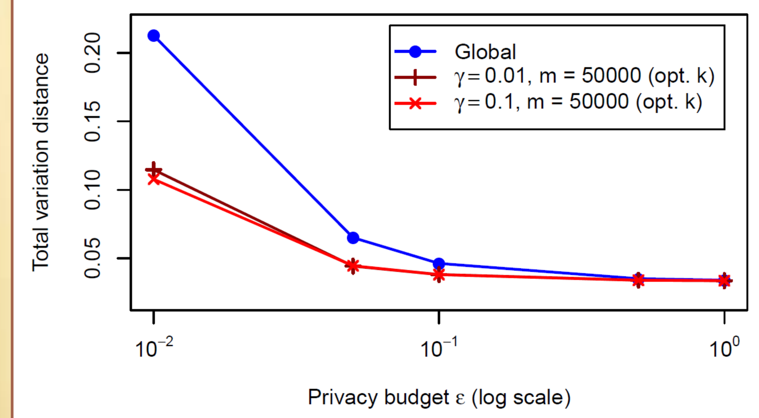


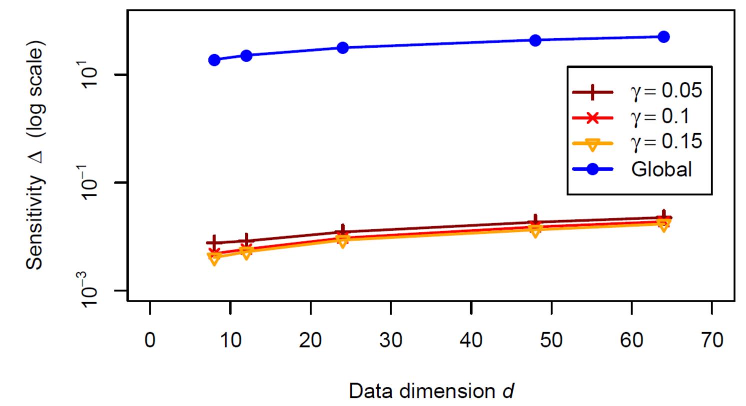

## Results

Can optimise any of: sampling effort $m$, RDP confidence $\gamma$, utility by index $k$




Utility vs Privacy for kernel density estimation

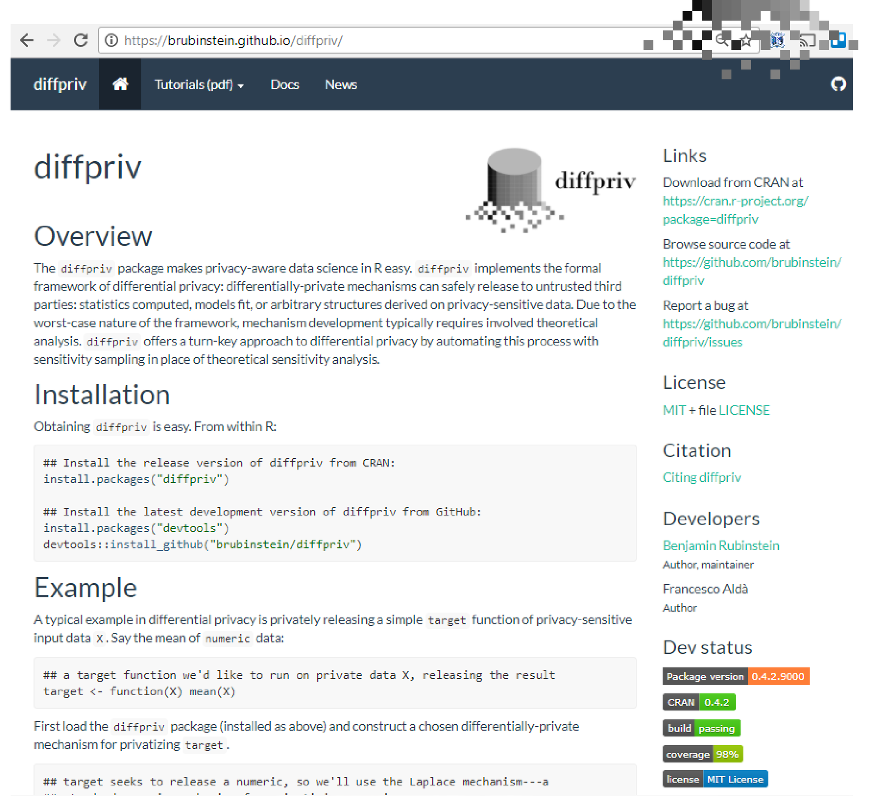


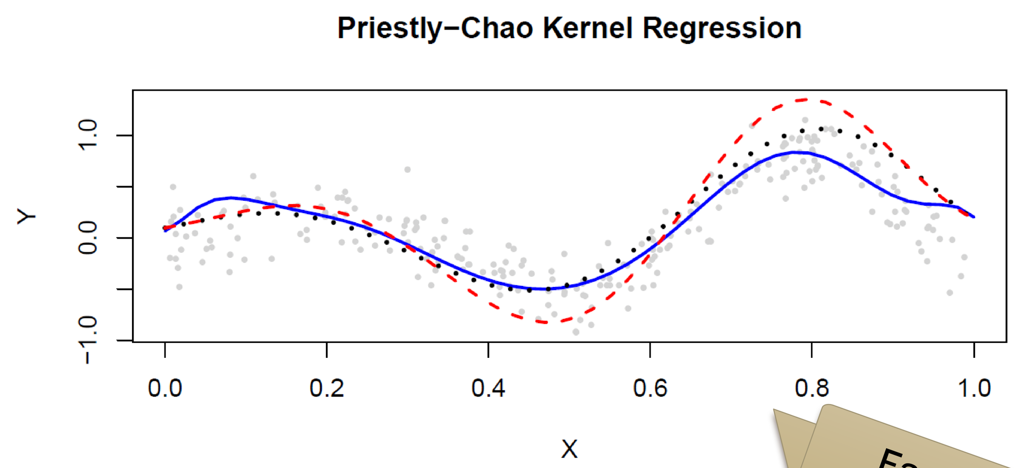

SVM sensitivity: global vs sampled

## Open-Source Package

diffpriv




- Open-source R package on GitHub
- 'Official' on CRAN with rigorous submission process checks
- Implements generic mechanisms for DP, sampler for automatic RDP
- roxygen2 docs
- Tutorial vignettes (→ JMLR MLOSS)
- 98% code coverage with `testthat`
- Travis CI continuous integration




Easy install

```
install.packages("diffpriv")

library(diffpriv)
m <- DPMechBernstein(
  target=pck_regression, latticeK=K, dims=1)
m <- sensitivitySampler(m, oracle=P, gamma=0.05)
R <- releaseResponse(m, DPParams(epsilon=1), D)
```

Acknowledgements: Australian Research Council (DE160100584), DFG Research Training Group GRK 1817/1