Statistically Valid Inferences from Privacy Protected Data

Gary King

Institute for Quantitative Social Science
Harvard University

Interagency Arctic Research Policy Committee, 11/19/2020

1Joint with Georgina Evans, Margaret Schwenzfeier, Abhradeep Thakurta.
2GaryKing.org/dp
Solving Political Problems Technologically

Differential Privacy & Inferential Validity

A General Purpose, Statistically Valid DP Algorithm

The Algorithm in Practice
Convincing Facebook to Make Data Available

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: “Could you do a study of the 2016 election?”
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)
  • No pre-publication approval (like NO employees ever)
• We iterate, and I propose a 2-part solution
  • Outside academics: send proposals, no company veto
  • Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges
• Problem solved, without balancing agreements, announcements, funding, 30+ people assigned at Facebook
• Just one issue: Facebook’s implementation plan was illegal!
• New Problem: Sharing data without it leaving Facebook
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: "Hey what do we do about this?"
• This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: "Could you do a study of the 2016 election?"
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)
  • No pre-publication approval (like NO employees ever)
• We iterate, and I propose a 2-part solution
  • Outside academics: send proposals, no company veto
  • Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges
• Problem solved, without balancing agreements, announcements, funding, 30+ people assigned at Facebook
• Just one issue: Facebook’s implementation plan was illegal!
• New Problem: Sharing data without it leaving Facebook
Convincing Facebook to Make Data Available
Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
Gary visits Facebook to persuade them to make data available.

In my hotel room packing, email arrives: “Hey what do we do about this?”

This was Cambridge Analytica. (The worst timed lobby effort in history!)

3 days later: “Could you do a study of the 2016 election?”

I’d love to, but I need 2 things & you’ll only give me 1:

- Complete access to data, people, etc. (like employees)
- No pre-publication approval (like NO employees ever)

We iterate, and I propose a 2-part solution:

- Outside academics: send proposals, no company veto
- Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges

Problem solved, without balancing agreements, announcements, funding, 30+ people assigned at Facebook.

Just one issue: Facebook’s implementation plan was illegal!

New Problem: Sharing data without it leaving Facebook.
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica.
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
Convincing Facebook to Make Data Available
Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
- 3 days later: “Could you do a study of the 2016 election?”

Problem solved, without balancing agreements, announcements, funding, 30+ people assigned at Facebook

New Problem: Sharing data without it leaving Facebook
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
- 3 days later: “Could you do a study of the 2016 election?”
- I’d love to, but I need 2 things & you’ll only give me 1:
Convincing Facebook to Make Data Available
Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: “Could you do a study of the 2016 election?”
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)

• 30+ people assigned at Facebook

Problem solved, without balancing agreements, announcements, funding; Facebook’s implementation plan was illegal!

New Problem: Sharing data without it leaving Facebook
Convincing Facebook to Make Data Available
Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: “Could you do a study of the 2016 election?”
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)
  • No pre-publication approval (like NO employees ever)
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: “Could you do a study of the 2016 election?”
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)
  • No pre-publication approval (like NO employees ever)
• We iterate, and I propose a 2-part solution
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
- 3 days later: “Could you do a study of the 2016 election?”
- I’d love to, but I need 2 things & you’ll only give me 1:
  - Complete access to data, people, etc. (like employees)
  - No pre-publication approval (like NO employees ever)
- We iterate, and I propose a 2-part solution
  - Outside academics: send proposals, no company veto
Convincing Facebook to Make Data Available
Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: “Could you do a study of the 2016 election?”
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)
  • No pre-publication approval (like NO employees ever)
• We iterate, and I propose a 2-part solution
  • Outside academics: send proposals, no company veto
  • Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges

Problem solved, without balancing; agreements, announcements, funding, 30+ people assigned at Facebook

Just one issue: Facebook’s implementation plan was illegal!

New Problem: Sharing data without it leaving Facebook

Solving Political Problems Technologically
Convincing Facebook to Make Data Available
Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
- 3 days later: “Could you do a study of the 2016 election?”
- I’d love to, but I need 2 things & you’ll only give me 1:
  - Complete access to data, people, etc. (like employees)
  - No pre-publication approval (like NO employees ever)
- We iterate, and I propose a 2-part solution
  - Outside academics: send proposals, no company veto
  - Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges
- Problem solved, without balancing agreements, announcements, funding, 30+ people assigned at Facebook
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
- 3 days later: “Could you do a study of the 2016 election?”
- I’d love to, but I need 2 things & you’ll only give me 1:
  - Complete access to data, people, etc. (like employees)
  - No pre-publication approval (like NO employees ever)
- We iterate, and I propose a 2-part solution
  - Outside academics: send proposals, no company veto
  - Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges
- Problem solved, without balancing \(\sim\) agreements, announcements, funding, 30+ people assigned at Facebook
- Just one issue:
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

- Gary visits Facebook to persuade them to make data available
- In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
- 3 days later: “Could you do a study of the 2016 election?”
- I’d love to, but I need 2 things & you’ll only give me 1:
  - Complete access to data, people, etc. (like employees)
  - No pre-publication approval (like NO employees ever)
- We iterate, and I propose a 2-part solution
  - Outside academics: send proposals, no company veto
  - Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges
- Problem solved, without balancing ~ agreements, announcements, funding, 30+ people assigned at Facebook
- Just one issue: Facebook’s implementation plan was illegal!
Convincing Facebook to Make Data Available

Solving a Political Problem Technologically (via “constitutional design”)

• Gary visits Facebook to persuade them to make data available
• In my hotel room packing, email arrives: “Hey what do we do about this?” This was Cambridge Analytica. (The worst timed lobby effort in history!)
• 3 days later: “Could you do a study of the 2016 election?”
• I’d love to, but I need 2 things & you’ll only give me 1:
  • Complete access to data, people, etc. (like employees)
  • No pre-publication approval (like NO employees ever)
• We iterate, and I propose a 2-part solution
  • Outside academics: send proposals, no company veto
  • Trusted 3rd party: Commission at Social Science One signs NDAs, agree not to publish from the data, chooses datasets, makes final decisions; can report publicly if Facebook reneges
• Problem solved, without balancing ~ agreements, announcements, funding, 30+ people assigned at Facebook
• Just one issue: Facebook’s implementation plan was illegal!
• New Problem: Sharing data without it leaving Facebook

Solving Political Problems Technologically 3/15
Data Sharing Regime $\rightarrow$ Data Access Regime

- Data Sharing Regime: I give you data (maybe you sign DUA)

  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.

  - Trusting researchers fails spectacularly at times (C.A.!)
  - Even trusting a researcher known to be trustworthy can fail

Data Access Regime

- Trusted server holds data; researchers as adversaries, can run any method; noisy answer, a limited number of times

  - Goal: impossible to violate individual privacy; & possible to discover population-level patterns

  - $\approx$ differential privacy (seems to satisfy regulators et al.)

New Problem:

- Most DP algorithms are statistically invalid!
- Unknown statistical properties (usually biased)
- No uncertainty estimates

Solving Political Problems Technologically
Data Sharing Regime $\rightsquigarrow$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
    - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!
    - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method; noisy answer, a limited number of times
  - Goal: impossible to violate individual privacy; possible to discover population level patterns
    - $\approx$ differential privacy (seems to satisfy regulators et al.)

- New problem: Most DP algorithms are statistically invalid!
  - Unknown statistical properties (usually biased)
  - No uncertainty estimates
Data Sharing Regime $\rightsquigarrow$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)

  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn't work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!!)
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**

  - Trusted server holds data; researchers as adversaries, can run any method; noisy answer, a limited number of times

  - Goal: impossible to violate individual privacy; $\approx$ differential privacy (seems to satisfy regulators et al.)

  - New Problem: Most DP algorithms are statistically invalid!
  - Unknown statistical properties (usually biased)
  - No uncertainty estimates
Data Sharing Regime $\sim$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)

- **Data Access Regime**

  - Trusting researchers fails spectacularly at times (e.g., C.A.!) even when trusting a researcher known to be trustworthy.
  - Increasing public concern with privacy.
  - Scholars discovered: de-identification doesn't work! Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.

- **Goal**: impossible to violate individual privacy; possible to discover population level patterns.

  - $\approx$ differential privacy (seems to satisfy regulators et al.)

- **New Problem**: Most DP algorithms are statistically invalid!
  - unknown statistical properties (usually biased)
  - no uncertainty estimates.
Data Sharing Regime ⇝ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing

- **Data Access Regime**
Data Sharing Regime \(\leadsto\) Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but **failing**
  - Increasing public concern with privacy

- **Data Access Regime**
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!

- **Data Access Regime**
Data Sharing Regime $\xrightarrow{\sim}$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does

- **Data Access Regime**
Data Sharing Regime $\sim$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation,

- **Data Access Regime**
Data Sharing Regime \(\sim\) Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing,

- **Data Access Regime**
Data Sharing Regime $\sim$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms,

- **Data Access Regime**
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but *failing*
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements,

- **Data Access Regime**
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing,

- **Data Access Regime**
Data Sharing Regime $\rightsquigarrow$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

• **Data Sharing Regime**: I give you data (maybe you sign DUA)
  • Venerable, but failing
  • Increasing public concern with privacy
  • Scholars discovered: de-identification doesn’t work!
  • Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models,

• **Data Access Regime**
Data Sharing Regime \(\sim\) Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but **failing**
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.

- **Data Access Regime**
Data Sharing Regime $\rightsquigarrow$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A. !)

- **Data Access Regime**
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
Data Sharing Regime $\rightsquigarrow$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but **failing**
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!) 
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data;

≈ differential privacy (seems to satisfy regulators et al.)

New Problem:
Most DP algorithms are statistically invalid!
- unknown statistical properties (usually biased)
- no uncertainty estimates
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries
Data Sharing Regime $\mapsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but *failing*
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\mapsto$ noisy answer,
Data Sharing Regime $\rightsquigarrow$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\rightsquigarrow$ noisy answer, a limited number of times
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal:**
Data Sharing Regime $\sim$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but *failing*
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!) 
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\sim$ noisy answer, a limited number of times
  - **Goal**: impossible to violate individual privacy
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime:** I give you data (maybe you sign DUA)
  - Venerable, but *failing*
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal:** *impossible* to violate individual privacy; & *possible* to discover population level patterns
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy (seems to satisfy regulators et al.)
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!) 
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy (seems to satisfy regulators et al.)
  - **New Problem:**
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!!)
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy (seems to satisfy regulators et al.)
  - **New Problem**: Most DP algorithms are statistically invalid!
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime**: I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy (seems to satisfy regulators et al.)
  - **New Problem**: Most DP algorithms are statistically invalid!
    - *unknown* statistical properties (usually *biased*)
Data Sharing Regime $\leadsto$ Data Access Regime

Solving Another Political Problem Technologically (via CS & Statistics)

- **Data Sharing Regime:** I give you data (maybe you sign DUA)
  - Venerable, but failing
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing, data clean rooms, legal agreements, restricted viewing, paired programmer models, etc.
  - Trusting researchers fails spectacularly at times (C.A.!)  
  - Even trusting a researcher known to be trustworthy can fail

- **Data Access Regime**
  - Trusted server holds data; researchers as adversaries, can run any method $\leadsto$ noisy answer, a limited number of times
  - **Goal:** impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy (seems to satisfy regulators et al.)
  - **New Problem:** Most DP algorithms are statistically invalid!
    - *unknown* statistical properties (usually *biased*)
    - *no* uncertainty estimates

Solving Political Problems Technologically
Solving Political Problems Technologically

Differential Privacy & Inferential Validity

A General Purpose, Statistically Valid DP Algorithm

The Algorithm in Practice
### Theories of Inference: Statistics vs. CS

| Name    | Class | Quantity of Interest | Typical Practitioner | Privacy & CS | Inference
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lindsay</td>
<td>3</td>
<td>Noise &amp; Censoring</td>
<td>No direct relevance</td>
<td>Mean income</td>
<td>Classical</td>
</tr>
<tr>
<td>Salil</td>
<td>3</td>
<td></td>
<td>No direct relevance</td>
<td></td>
<td>Query-Response</td>
</tr>
<tr>
<td>Georgie</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gary</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meg</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abhradeep</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Joshua</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annie</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ellen</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Differential Privacy & Inferential Validity
Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lindsay</td>
</tr>
<tr>
<td>Salil</td>
</tr>
<tr>
<td>Georgie</td>
</tr>
<tr>
<td>Gary</td>
</tr>
<tr>
<td>Meg</td>
</tr>
<tr>
<td>Abhradeep</td>
</tr>
<tr>
<td>Joshua</td>
</tr>
<tr>
<td>Annie</td>
</tr>
<tr>
<td>Bob</td>
</tr>
<tr>
<td>Ellen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mean income:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$48</td>
</tr>
</tbody>
</table>

Quantity of Interest
# Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>🛠️</td>
<td>⬗️</td>
</tr>
<tr>
<td>Lindsay</td>
<td>✔️</td>
</tr>
<tr>
<td>Salil</td>
<td>✔️</td>
</tr>
<tr>
<td>Georgie</td>
<td>✔️</td>
</tr>
<tr>
<td>Gary</td>
<td>✔️</td>
</tr>
<tr>
<td>Meg</td>
<td>✔️</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✔️</td>
</tr>
<tr>
<td>Joshua</td>
<td>✔️</td>
</tr>
<tr>
<td>Annie</td>
<td>✔️</td>
</tr>
<tr>
<td>Bob</td>
<td>✔️</td>
</tr>
<tr>
<td>Ellen</td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Mean income:** $48

**Quantity of Interest**

Differential Privacy & Inferential Validity
Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>Lindsay</td>
<td>✓</td>
<td>122</td>
</tr>
<tr>
<td>Salil</td>
<td>✓</td>
<td>76</td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>96</td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
</tr>
<tr>
<td>Joshua</td>
<td>✓</td>
<td>72</td>
</tr>
<tr>
<td>Annie</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>Bob</td>
<td>✓</td>
<td>95</td>
</tr>
<tr>
<td>Ellen</td>
<td>✓</td>
<td>134</td>
</tr>
</tbody>
</table>

Mean income:

- Classical Inference: $48
- Usually no direct relevance: $108
### Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lindsay</td>
<td>✓</td>
<td>122</td>
</tr>
<tr>
<td>Salil</td>
<td>✓</td>
<td>76</td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>96</td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
</tr>
<tr>
<td>Joshua</td>
<td>✓</td>
<td>72</td>
</tr>
<tr>
<td>Annie</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>Bob</td>
<td>✓</td>
<td>95</td>
</tr>
<tr>
<td>Ellen</td>
<td>✓</td>
<td>134</td>
</tr>
</tbody>
</table>

**Quantity of Interest**

- Classical Inference
- Usually no direct relevance

**Mean income:**

- $48
- $108
Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>$</th>
<th>+Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lindsay</td>
<td>✓</td>
<td>122</td>
<td>?</td>
</tr>
<tr>
<td>Salil</td>
<td>✓</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>Joshua</td>
<td>✓</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Annie</td>
<td>✓</td>
<td>132</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>✓</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>Ellen</td>
<td>✓</td>
<td>134</td>
<td></td>
</tr>
</tbody>
</table>

Mean income: $48 → Classical Inference $108

Quantity of Interest

Usually no direct relevance

Noise & Censoring
Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>Mean Income</th>
<th>+Privacy</th>
<th>=dp$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lindsay</td>
<td>✓</td>
<td>122</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Salil</td>
<td>✓</td>
<td>76</td>
<td>103</td>
<td></td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>96</td>
<td>113</td>
<td></td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>Joshua</td>
<td>✓</td>
<td>72</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>Annie</td>
<td>✓</td>
<td>132</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>✓</td>
<td>95</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>Ellen</td>
<td>✓</td>
<td>134</td>
<td>201</td>
<td></td>
</tr>
</tbody>
</table>

Mean income: $48, $108, $111

Classical Inference: Usually no direct relevance
Query-Response: Usually no direct relevance
Noise & Censoring: No direct relevance
## Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>$</th>
<th>$+Privacy</th>
<th>=dp$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lindsay</td>
<td>✓</td>
<td>122</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Salil</td>
<td>✓</td>
<td>76</td>
<td>103</td>
<td></td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>96</td>
<td>113</td>
<td></td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>Joshua</td>
<td>✓</td>
<td>72</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>Annie</td>
<td>✓</td>
<td>132</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>✓</td>
<td>95</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>Ellen</td>
<td>✓</td>
<td>134</td>
<td>201</td>
<td></td>
</tr>
</tbody>
</table>

Mean income:
- Classical Inference: $48
- Query-Response: $108
- $111

Statistically Valid Inferences from Privacy Protected Data
Estimators

Classical Statistics: Apply statistic $s$ to dataset $D$, $s(D)$

DP Mechanism: $M(s, D)$, with noise & censoring

Essential components of ensuring privacy

Fundamental problems for statistical inference

The DP Standard (simplifying)

Including ($D$) or excluding ($D'$) you doesn't change conclusions

Pr[$M(s, D) = m]$ Pr[$M(s, D') = m] \in 1 \pm \epsilon$

Examples all proven to protect the biggest possible outlier

$M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N(0, 8 \Lambda n \epsilon) (\Lambda, n, \epsilon$ known)

Or: mess with gradients, $X'_i X_i$, data, QOIs, etc.

Statistical properties: usually biased, no uncertainty estimates
Differential Privacy and its Inferential Challenges

• Estimators
Differential Privacy and its Inferential Challenges

- **Estimators**
  - **Classical Statistics:** Apply statistic $s$ to dataset $D$, $s(D)$
Differential Privacy and its Inferential Challenges

- **Estimators**
  - Classical Statistics: Apply statistic $s$ to dataset $D$, $s(D)$
  - DP Mechanism: $M(s, D)$, with noise & censoring
Differential Privacy and its Inferential Challenges

• **Estimators**
  
  • **Classical Statistics:** Apply statistic $s$ to dataset $D$, $s(D)$
  • **DP Mechanism:** $M(s, D)$, with noise & censoring
    
    • Essential components of ensuring privacy
Differential Privacy and its Inferential Challenges

- **Estimators**
  - **Classical Statistics**: Apply statistic $s$ to dataset $D$, $s(D)$
  - **DP Mechanism**: $M(s, D)$, with noise & censoring
    - Essential components of ensuring privacy
    - Fundamental problems for statistical inference
Differential Privacy and its Inferential Challenges

• **Estimators**
  • **Classical Statistics:** Apply statistic $s$ to dataset $D$, $s(D)$
  • **DP Mechanism:** $M(s, D)$, with noise & censoring
    • Essential components of ensuring privacy
    • Fundamental problems for statistical inference

• **The DP Standard (simplifying)**
Differential Privacy and its Inferential Challenges

- **Estimators**
  - **Classical Statistics:** Apply statistic $s$ to dataset $D$, $s(D)$
  - **DP Mechanism:** $M(s, D)$, with noise & censoring
    - Essential components of ensuring privacy
    - Fundamental problems for statistical inference

- **The DP Standard (simplifying)**
  - Including ($D$) or excluding ($D'$) you doesn’t change conclusions
    
    \[
    \Pr[M(s, D) = m] \in 1 \pm \epsilon \\
    \Pr[M(s, D') = m] 
    \]

    for all $D, D', m$
Differential Privacy and its Inferential Challenges

• **Estimators**
  - **Classical Statistics:** Apply statistic $s$ to dataset $D$, $s(D)$
  - **DP Mechanism:** $M(s, D)$, with noise & censoring
    - Essential components of ensuring privacy
    - Fundamental problems for statistical inference

• **The DP Standard (simplifying)**
  - Including ($D$) or excluding ($D'$) you doesn’t change conclusions
    
    \[
    \frac{\Pr[M(s, D) = m]}{\Pr[M(s, D') = m]} \in 1 \pm \epsilon
    \]
    
    for all $D, D', m$

• **Examples** all proven to protect the biggest possible outlier
Differential Privacy and its Inferential Challenges

• **Estimators**
  - **Classical Statistics:** Apply statistic $s$ to dataset $D$, $s(D)$
  - **DP Mechanism:** $M(s, D)$, with noise & censoring
    - Essential components of ensuring privacy
    - Fundamental problems for statistical inference

• **The DP Standard (simplifying)**
  - Including $(D)$ or excluding $(D')$ you doesn’t change conclusions
    \[
    \frac{\Pr[M(s, D) = m]}{\Pr[M(s, D') = m]} \in 1 \pm \epsilon
    \]
    for all $D, D', m$

• **Examples** all proven to protect the biggest possible outlier
  - $M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N\left(0, \frac{8\Lambda}{n\epsilon}\right)$
    (\(\Lambda, n, \epsilon\) known)
Differential Privacy and its Inferential Challenges

• Estimators
  • Classical Statistics: Apply statistic $s$ to dataset $D$, $s(D)$
  • DP Mechanism: $M(s, D)$, with noise & censoring
    • Essential components of ensuring privacy
    • Fundamental problems for statistical inference

• The DP Standard (simplifying)
  • Including ($D$) or excluding ($D'$) you doesn’t change conclusions
    \[
    \frac{\Pr[M(s, D) = m]}{\Pr[M(s, D') = m]} \in 1 \pm \epsilon
    \]
    for all $D, D', m$

• Examples all proven to protect the biggest possible outlier
  • $M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N\left(0, \frac{8\Lambda}{n\epsilon}\right)$ (\(\Lambda, n, \epsilon\) known)
  • Or: mess with gradients, $X'_iX_i$, data, QOIs, etc.
Differential Privacy and its Inferential Challenges

- Estimators
  - Classical Statistics: Apply statistic $s$ to dataset $D$, $s(D)$
  - DP Mechanism: $M(s, D)$, with noise & censoring
    - Essential components of ensuring privacy
    - Fundamental problems for statistical inference

- The DP Standard (simplifying)
  - Including $(D)$ or excluding $(D')$ you doesn’t change conclusions

$$\frac{\Pr[M(s, D) = m]}{\Pr[M(s, D') = m]} \in 1 \pm \epsilon$$

for all $D, D', m$

- Examples all proven to protect the biggest possible outlier
  - $M(\text{mean, } D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N\left(0, \frac{8\Lambda}{n\epsilon}\right)$  \hspace{1cm} (\Lambda, n, \epsilon \text{ known})
  - Or: mess with gradients, $X_i'X_i$, data, QOIs, etc.

- Statistical properties: usually biased, no uncertainty estimates
Solving Political Problems Technologically

Differential Privacy & Inferential Validity

A General Purpose, Statistically Valid DP Algorithm

The Algorithm in Practice
A Differentially Private Estimator

Private data \( \mathcal{D} \)

Partition \( \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_5 \)

Bag of little bootstraps

Estimator \( \hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_3, \hat{\theta}_4, \hat{\theta}_5 \)

Censor

Average Noise \( \hat{\theta}_{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N(0, 8\Lambda_P \varepsilon) \)

Bias Correction & variance estimation

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data

Partition

\[ \hat{\theta} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N(0, 8\Lambda P \epsilon) \]
A Differentially Private Estimator

- Private data
- Partition
- Bag of little bootstraps

\[ \hat{\theta}_\text{dp} = \frac{1}{\sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda_p)} + N(0, 8\Lambda_P \epsilon) \]
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data

Partition

Bag of little bootstraps

Estimator

Censor

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator
Censor
Average

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator
Censor
Average
Noise

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator
Censor
Average
Noise
Bias Correction

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data

Partition

Bag of little bootstraps

Estimator

Censor

Average

Noise

Bias Correction (& variance estimation)

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator
Censor
Average
Noise
Bias Correction (& variance estimation)

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator
Censor
Average
Noise
Bias Correction
(& variance estimation)
A Differentially Private Estimator

Private data
Partition
Bag of little bootstraps
Estimator
Censor
Average
Noise
Bias Correction (& variance estimation)
A Differentially Private Estimator

Private data

Partition

Bag of little bootstraps

Estimator

Censor

Average

Noise

Bias Correction
(& variance estimation)

A General Purpose, Statistically Valid DP Algorithm
A Differentially Private Estimator

Private data

Partition

Bag of little bootstraps

Estimator

Censor

Average

Noise

Bias Correction

\[
\hat{\theta}_{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N \left(0, \frac{8\Lambda}{P\epsilon}\right)
\]

A General Purpose, Statistically Valid DP Algorithm
Bias Correction of:  

\[ \hat{\theta}_{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \]  

(\Lambda, P, \epsilon \text{ known})
Bias Correction of: \[ \hat{\theta}_{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \] (\(\Lambda, P, \epsilon\) known)
Bias Correction of:

\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \quad (\Lambda, P, \epsilon \text{ known}) \]

\[ \hat{\theta}_p \sim N(\theta, \sigma^2) \]

Uncensored

Censored distribution

\[ \alpha = \int_{\Lambda}^{\infty} N(t | \theta, \sigma^2) dt \]

\[ \alpha \theta_c = (1 - \alpha) \theta_T + \alpha \Lambda \]

Equations: 2

Unknowns: \( \theta, \sigma^2, \alpha, \theta_c \)

Disclose: \( \hat{\theta}^{dp}, \hat{\alpha}^{dp} \)
Bias Correction of: 

\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \]  

(\Lambda, P, \epsilon \text{ known})

Uncensored: 

\[ \hat{\theta}_p \sim N(\theta, \sigma^2) \]

Censored distribution:

\[ \alpha = \int_{\Lambda}^{\infty} N(t | \theta, \sigma^2) dt \]

\[ \alpha = \int_{\Lambda}^{\infty} N(t | \theta, \sigma^2) dt \]

\[ \theta_c \quad \theta \quad \Lambda \]

Goal:

A General Purpose, Statistically Valid DP Algorithm
Bias Correction of: 

\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \]  

(\Lambda, P, \epsilon \text{ known})

\[ \hat{\theta}_p \sim N(\theta, \sigma^2) \]

Uncensored

\[ \hat{\theta}^{dp} \]

Censored distribution

\[ \alpha = \int_{\Lambda}^{\infty} N(t | \theta, \sigma^2) dt \]

\[ \theta_c = (1 - \alpha)\theta_T + \alpha\Lambda \]

Goal
Bias Correction of: \[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \] \hspace{1cm} (\Lambda, P, \epsilon \text{ known})
Bias Correction of: 
\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \] (\(\Lambda, P, \epsilon\) known)

Uncensored 
\[ \hat{\theta}_p \sim N(\theta, \sigma^2) \]

Censored distribution 
\[ \alpha = \int_{\Lambda}^{\infty} N(t | \theta, \sigma^2) dt \]

\[ \theta_c = (1 - \alpha)\theta_T + \alpha\Lambda \]

Equations: 2
Unknowns: \(\theta, \sigma^2, \alpha, \theta_c\)
Bias Correction of:  
\[ \hat{\theta}^\text{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \quad (\Lambda, P, \epsilon \text{ known}) \]

\[ \hat{\theta}_p \sim N(\theta, \sigma^2) \]

Uncensored

\[ \theta_c = (1 - \alpha)\theta_T + \alpha\Lambda \]

Goal

Censored distribution

\[ \alpha = \int_{\Lambda}^{\infty} N(t \mid \theta, \sigma^2) \, dt \]

Equations: 2

Unknowns: \( \theta, \sigma^2, \alpha, \Lambda \)

Disclose: \( \hat{\theta}^\text{dp} \)
Bias Correction of:  
\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{8\Lambda}{P\epsilon}\right) \]  
\( (\Lambda, P, \epsilon \text{ known}) \)

Equations: 2  
Unknowns: \( \theta, \sigma^2, \Lambda, X_c \)
Variance Estimation

Simulate estimates via standard (Clarify) procedures:

\[ \hat{\theta}_{dp}, \hat{\alpha}_{dp} \sim N(\begin{bmatrix} \hat{\theta}_{dp} \\ \hat{\alpha}_{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}_{dp}) & \hat{\text{Cov}}(\hat{\alpha}_{dp}, \hat{\theta}_{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}_{dp}, \hat{\theta}_{dp}) & \hat{V}(\hat{\alpha}_{dp}) \end{bmatrix}) \]

Functions of disclosed params

Bias correct simulated params:

\[ \{\tilde{\theta}_{dp}, \hat{\sigma}^2_{dp}\} = \text{BiasCorrect}[\hat{\theta}_{dp}, \hat{\alpha}_{dp}] \]

Standard error:

Standard deviation of \( \tilde{\theta}_{dp} \) over simulations

Bias correction:

reduces bias and variance
Variance Estimation

- **Simulate estimates** via standard (Clarify) procedures:

\[ \hat{\theta}^{dp}, \hat{\alpha}^{dp} \sim N \left( \begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}^{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}^{dp}) \end{bmatrix} \right) \]
Variance Estimation

- **Simulate estimates** via standard (Clarify) procedures:

\[
\hat{\theta}^{dp}, \hat{\alpha}^{dp} \sim N\left(\begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}^{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}^{dp}) \end{bmatrix}\right)
\]

Functions of disclosed params

Bias correct simulated params:

\[
\{\tilde{\theta}^{dp}, \hat{\sigma}_2^{dp}\} = \text{BiasCorrect}\left[\hat{\theta}^{dp}, \hat{\alpha}^{dp}\right]
\]
Variance Estimation

- **Simulate estimates** via standard (Clarify) procedures:

\[
\hat{\theta}^{dp}, \hat{\alpha}^{dp} \sim N\left( \begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}^{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}^{dp}) \end{bmatrix} \right)
\]

- **Bias correct simulated params**:

\[
\{\tilde{\theta}^{dp}, \tilde{\sigma}^{2}_{dp}\} = \text{BiasCorrect}\left[ \hat{\theta}^{dp}, \hat{\alpha}^{dp} \right]
\]
Variance Estimation

- **Simulate estimates** via standard (Clarify) procedures:

  \[
  \hat{\theta}_{dp}, \hat{\alpha}_{dp} \sim N\left(\begin{bmatrix} \hat{\theta}_{dp} \\ \hat{\alpha}_{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}_{dp}) & \hat{\text{Cov}}(\hat{\alpha}_{dp}, \hat{\theta}_{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}_{dp}, \hat{\theta}_{dp}) & \hat{V}(\hat{\alpha}_{dp}) \end{bmatrix}\right)
  \]

  Functions of disclosed params

- **Bias correct simulated params:**

  \[
  \{\tilde{\theta}_{dp}, \tilde{\sigma}_{dp}^2\} = \text{BiasCorrect}\left[\hat{\theta}_{dp}, \hat{\alpha}_{dp}\right]
  \]

- **Standard error:** Standard deviation of \(\tilde{\theta}_{dp}\) over simulations
Variance Estimation

• Simulate estimates via standard (Clarify) procedures:

\[
\begin{bmatrix}
\hat{\theta}^{dp} \\
\hat{\alpha}^{dp}
\end{bmatrix} \sim N\left(\begin{bmatrix}
\hat{\theta}^{dp} \\
\hat{\alpha}^{dp}
\end{bmatrix}, \begin{bmatrix}
\hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) \\
\hat{\text{Cov}}(\hat{\alpha}^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}^{dp})
\end{bmatrix}\right)
\]

Functions of disclosed params

• Bias correct simulated params:

\[
\{\hat{\theta}^{dp}, \hat{\sigma}^{2}_{dp}\} = \text{BiasCorrect}\left[\hat{\theta}^{dp}, \hat{\alpha}^{dp}\right]
\]

• Standard error: Standard deviation of \(\hat{\theta}^{dp}\) over simulations
• Bias correction: reduces bias and variance
Solving Political Problems Technologically

Differential Privacy & Inferential Validity

A General Purpose, Statistically Valid DP Algorithm

The Algorithm in Practice
Simulations: Finite Sample Evaluation
Simulations: Finite Sample Evaluation

The Algorithm in Practice
Simulations: Finite Sample Evaluation

The Algorithm in Practice
Simulations: Finite Sample Evaluation

The Algorithm in Practice
Simulations: Finite Sample Evaluation

The Algorithm in Practice
Simulations: Finite Sample Evaluation

The Algorithm in Practice
Concluding Remarks

Data sharing; data access

• DP protects individual privacy
• Enables inference to private database, not population
• Usually biased, no uncertainty estimates

• Inferential validity
  • A scientific statement: not necessarily correct, but must have:
    • known statistical properties
    • valid uncertainty estimates

• Proposed algorithm
  • Generic: almost any statistical method or quantity of interest
  • Statistically unbiased,
  • lower variance
  • Valid uncertainty estimates
  • Computationally efficient
  • Solves political problems technologically

Implementations:
• Facebook, Microsoft+Harvard/IQSS, OpenDP
Concluding Remarks

- Data sharing \(\sim\) data access
Concluding Remarks

- Data sharing $\sim$ data access
  - DP protects individual privacy
Concluding Remarks

- **Data sharing ~ data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
Concluding Remarks

• Data sharing $\sim$ data access
  • DP protects individual privacy
  • Enables inference to private database, not population
  • Usually biased, no uncertainty estimates
Concluding Remarks

- **Data sharing \(\leadsto\) data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions
Concluding Remarks

- Data sharing $\leadsto$ data access
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- Inferential validity
Concluding Remarks

• Data sharing $\sim$ data access
  • DP protects individual privacy
  • Enables inference to private database, not population
  • Usually biased, no uncertainty estimates
  • Fails to protect society from fallacious scientific conclusions

• Inferential validity
  • A scientific statement: not necessarily correct, but must have:
Concluding Remarks

- **Data sharing ~ data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates
Concluding Remarks

- **Data sharing \( \sim \) data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

- **Proposed algorithm**
Concluding Remarks

• **Data sharing ~ data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

• **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

• **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
Concluding Remarks

- **Data sharing $\sim$ data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically **unbiased**, lower variance

The Algorithm in Practice
Concluding Remarks

- **Data sharing** → data access
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
  - known statistical properties & valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically unbiased, lower variance
  - Valid uncertainty estimates
Concluding Remarks

- **Data sharing ↔ data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically unbiased, lower variance
  - Valid uncertainty estimates
  - Computationally efficient
Concluding Remarks

- Data sharing $\sim$ data access
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- Inferential validity
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

- Proposed algorithm
  - Generic: almost any statistical method or quantity of interest
  - Statistically unbiased, lower variance
  - Valid uncertainty estimates
  - Computationally efficient
  - Solves political problems technologically
Concluding Remarks

- **Data sharing** $\leadsto$ data access
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

- **Proposed algorithm**
  - **Generic:** almost any statistical method or quantity of interest
  - Statistically unbiased, lower variance
  - Valid uncertainty estimates
  - Computationally efficient
  - Solves political problems technologically
  - Implementations in progress:
Concluding Remarks

- **Data sharing → data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no uncertainty estimates
  - Fails to protect society from fallacious scientific conclusions

- **Inferential validity**
  - A scientific statement: not necessarily correct, but must have:
    - known statistical properties & valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically unbiased, lower variance
  - Valid uncertainty estimates
  - Computationally efficient
  - Solves political problems technologically
  - **Implementations in progress**:
    - Facebook, Microsoft+Harvard/IQSS, OpenDP
For more information

Georgina-Evans.com

GaryKing.org

MegSchwenzfeier.com

bit.ly/AbhradeepThakurta

Paper, software, slides, video: GaryKing.org/dp
Appendix
Properties of Differential Privacy

- Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$.
- Useful for bias corrections.
- Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID.
- Helpful mathematically; insufficient in applications.
- Real privacy loss $\ll$ maximum privacy loss.
- OK for worst case scenario; unhelpful in practice.

- Privacy Budget
- Composition: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
- Can limit maximum risks across analyses & researchers.
- When the budget is used, no new analyses can ever be run.
- Completely changes statistical best practices.

Without DP, we balance worries:

- P-hacking, pre-registration (e.g., clinical trials, Mars lander).
- Threats to inference; diagnostics, exploration, serendipity (e.g., observational data).

With DP: XXXXX P-hacking, surveys treated like the Mars lander.
Properties of Differential Privacy

- Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$
Properties of Differential Privacy

- **Post-processing**: if \( M(s, D) \) is DP, so is \( f[M(s, D)] \)
  - Useful for bias corrections
Properties of Differential Privacy

- **Post-processing**: If $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
Properties of Differential Privacy

• Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  • Useful for bias corrections
• Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID
  • Helpful mathematically; insufficient in applications
Properties of Differential Privacy

• **Post-processing:** if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections

• **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications

• **Real privacy loss** $\ll$ maximum privacy loss
Properties of Differential Privacy

• **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections

• **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications

• **Real privacy loss** $\ll$ maximum privacy loss
  - OK for worst case scenerio; unhelpful in practice

• **Privacy Budget**
  - **Composition**: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
  - Completely changes statistical best practices

• **Without DP**,
  - We balance worries:
    - P-hacking; pre-registration (e.g., clinical trials, Mars lander)
    - Threats to inference; diagnostics, exploration, serendipity (e.g., observational data)

• **With DP**:
  - XXXXX
Properties of Differential Privacy

• Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  • Useful for bias corrections
• Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID
  • Helpful mathematically; insufficient in applications
• Real privacy loss $\ll$ maximum privacy loss
  • OK for worst case scenario; unhelpful in practice
• Privacy Budget
Properties of Differential Privacy

- Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- Real privacy loss $\ll$ maximum privacy loss
  - OK for worst case scenario; unhelpful in practice
- Privacy Budget
  - Composition: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
Properties of Differential Privacy

• Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  • Useful for bias corrections
• Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID
  • Helpful mathematically; insufficient in applications
• Real privacy loss $\ll$ maximum privacy loss
  • OK for worst case scenario; unhelpful in practice
• Privacy Budget
  • Composition: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  • Can limit maximum risks across analyses & researchers
Properties of Differential Privacy

- **Post-processing:** if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss** $\ll$ maximum privacy loss
  - OK for worst case scenario; unhelpful in practice
- **Privacy Budget**
  - **Composition:** $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
Properties of Differential Privacy

• **Post-processing:** if $M(s, D)$ is DP, so is $f[M(s, D)]$
  • Useful for bias corrections

• **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  • Helpful mathematically; insufficient in applications

• **Real privacy loss** $\ll$ maximum privacy loss
  • OK for worst case scenario; unhelpful in practice

• **Privacy Budget**
  • **Composition:** $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  • Can limit maximum risks across analyses & researchers
  • When the budget is used, no new analyses can ever be run

• **Completely changes statistical best practices**
Properties of Differential Privacy

- **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss** $\ll$ maximum privacy loss
  - OK for worst case scenario; unhelpful in practice
- **Privacy Budget**
  - **Composition**: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
- **Completely changes statistical best practices**
  - **Without DP**, we balance worries:
Properties of Differential Privacy

• **Post-processing:** if $M(s, D)$ is DP, so is $f[M(s, D)]$
  • Useful for bias corrections

• **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  • Helpful mathematically; insufficient in applications

• **Real privacy loss** $\ll$ maximum privacy loss
  • OK for worst case scenario; unhelpful in practice

• **Privacy Budget**
  • **Composition:** $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  • Can limit maximum risks across analyses & researchers
  • When the budget is used, no new analyses can ever be run

• **Completely changes statistical best practices**
  • **Without DP,** we balance worries:
    • $P$-hacking
Properties of Differential Privacy

- **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss $\ll$ maximum privacy loss**
  - OK for worst case scenerio; unhelpful in practice
- **Privacy Budget**
  - **Composition**: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
- **Completely changes statistical best practices**
  - **Without DP**, we balance worries:
    - P-hacking
    - Threats to inference
Properties of Differential Privacy

- **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss $\ll$ maximum privacy loss**
  - OK for worst case scenario; unhelpful in practice
- **Privacy Budget**
  - **Composition**: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
- **Completely changes statistical best practices**
  - **Without DP**, we balance worries:
    - $P$-hacking $\leadsto$ pre-registration (e.g., clinical trials, Mars lander)
    - Threats to inference
Properties of Differential Privacy

- **Post-processing:** if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss** $\ll$ maximum privacy loss
  - OK for worst case scenario; unhelpful in practice
- **Privacy Budget**
  - **Composition:** $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
- **Completely changes statistical best practices**
  - **Without DP,** we balance worries:
    - **P-hacking** $\sim$ pre-registration (e.g., clinical trials, Mars lander)
    - **Threats to inference** $\sim$ diagnostics, exploration, serendipity (e.g., observational data)
Properties of Differential Privacy

- **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss** $\ll$ maximum privacy loss
  - OK for worst case scenario; unhelpful in practice
- **Privacy Budget**
  - **Composition**: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
- **Completely changes statistical best practices**
  - **Without DP**, we balance worries:
    - **P-hacking** $\rightsquigarrow$ pre-registration (e.g., clinical trials, Mars lander)
    - **Threats to inference** $\rightsquigarrow$ diagnostics, exploration, serendipity (e.g., observational data)
  - **With DP:**
Properties of Differential Privacy

• Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  • Useful for bias corrections

• Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID
  • Helpful mathematically; insufficient in applications

• Real privacy loss $\ll$ maximum privacy loss
  • OK for worst case scenario; unhelpful in practice

• Privacy Budget
  • Composition: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  • Can limit maximum risks across analyses & researchers
  • When the budget is used, no new analyses can ever be run

• Completely changes statistical best practices
  • Without DP, we balance worries:
    • P-hacking $\leadsto$ pre-registration (e.g., clinical trials, Mars lander)
    • Threats to inference $\leadsto$ diagnostics, exploration, serendipity (e.g., observational data)
  • With DP: P-hacking,
Properties of Differential Privacy

- **Post-processing:** if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
  - Helpful mathematically; insufficient in applications
- **Real privacy loss $\ll$ maximum privacy loss**
  - OK for worst case scenario; unhelpful in practice
- **Privacy Budget**
  - **Composition:** $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
  - Can limit maximum risks across analyses & researchers
  - When the budget is used, no new analyses can ever be run
- **Completely changes statistical best practices**
  - **Without DP,** we balance worries:
    - **P-hacking $\sim$** pre-registration (e.g., clinical trials, Mars lander)
    - **Threats to inference $\sim$** diagnostics, exploration, serendipity (e.g., observational data)
  - **With DP:** P-hacking, surveys treated like the Mars lander