Statistically Valid Inferences from Privacy Protected Data

Gary King

Institute for Quantitative Social Science
Harvard University

University of Chicago, 11/8/2019

---

1Joint work 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! Time to go home.)

• 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! Time to go home.)
• 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! Time to go home.)

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

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?”
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! Time to go home.)
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! Time to go home.)
- 3 days later: “Could you do a study of the 2016 election?”
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! Time to go home.)
- 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

- 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! Time to go home.)
• 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)
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! Time to go home.)
• 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! Time to go home.)
• 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! Time to go home.)
- 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! Time to go home.)
• 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
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! Time to go home.)
• 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! Time to go home.)
- 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:
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! Time to go home.)
• 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! Time to go home.)
• 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
Data Sharing Regime $\leadsto$ 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 $\leadsto$ 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
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 $\Rightarrow$ 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 $\leadsto$ 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 $\implies$ 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)

- **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*

- **Data Access Regime**

\[\approx\] differential privacy (**seems to satisfy regulators et al.**)
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

- **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!

- **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

- **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,

- **Data Access Regime**
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
  - Increasing public concern with privacy
  - Scholars discovered: de-identification doesn’t work!
  - Nor does aggregation, query auditing,

- **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,

- **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 \(\rightsquigarrow\) 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.

- **Data Access Regime**

Solving Political Problems Technologically
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.!)  

- **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;
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 $\rightsquigarrow$ 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,
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

\[ \text{Goal: impossible to violate individual privacy; & possible to discover population level patterns} \]

\[ \approx \text{differential privacy (seems to satisfy regulators et al.)} \]

\[ \text{New Problem: Most DP algorithms are statistically invalid!} \]

\[ \text{unknown statistical properties (usually biased)} \]

\[ \text{no uncertainty estimates} \]
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 $\rightsquigarrow$ noisy answer, a limited number of times

- **Goal**:
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
Data Sharing Regime $\implies$ 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 $\implies$ noisy answer, a limited number of times
  - **Goal**: Impossible to violate individual privacy; & possible to discover population level patterns
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
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy
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
  - **Goal**: impossible to violate individual privacy; & possible to discover population level patterns
  - $\approx$ differential privacy (seems to satisfy regulators et al.)
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
  - **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 $\Leftrightarrow$ 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 $\Leftrightarrow$ 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 $\rightsquigarrow$ 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
  - **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

Differential Privacy & Inferential Validity

A General Purpose, Statistically Valid DP Algorithm

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Class</th>
<th>Quantity of Interest</th>
<th>Mean Income</th>
<th>Noise &amp; Censoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Andrey</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Georgie</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gary</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meg</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abhradeep</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ella</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anya</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greg</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary</td>
</tr>
<tr>
<td>Andrey</td>
</tr>
<tr>
<td>Georgie</td>
</tr>
<tr>
<td>Gary</td>
</tr>
<tr>
<td>Meg</td>
</tr>
<tr>
<td>Abhradeep</td>
</tr>
<tr>
<td>Ella</td>
</tr>
<tr>
<td>Anya</td>
</tr>
<tr>
<td>Greg</td>
</tr>
<tr>
<td>Max</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quantity of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean income:</td>
</tr>
<tr>
<td>$48</td>
</tr>
</tbody>
</table>
# Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary</td>
<td>✔</td>
</tr>
<tr>
<td>Andrey</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>Ella</td>
<td>✔</td>
</tr>
<tr>
<td>Anya</td>
<td>✔</td>
</tr>
<tr>
<td>Greg</td>
<td>✔</td>
</tr>
<tr>
<td>Max</td>
<td>✔</td>
</tr>
</tbody>
</table>

Mean income: $48
# Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary</td>
<td>✓</td>
<td>76</td>
</tr>
<tr>
<td>Andrey</td>
<td>✓</td>
<td>96</td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>122</td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
</tr>
<tr>
<td>Ella</td>
<td>✓</td>
<td>72</td>
</tr>
<tr>
<td>Anya</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>Greg</td>
<td>✓</td>
<td>95</td>
</tr>
<tr>
<td>Max</td>
<td>✓</td>
<td>134</td>
</tr>
</tbody>
</table>

Mean income: $48

Classical Inference $108

Quantity of Interest

Usually no direct relevance
## Theories of Inference: Statistics vs. CS

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary</td>
<td>✓</td>
<td>76</td>
</tr>
<tr>
<td>Andrey</td>
<td>✓</td>
<td>96</td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>122</td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
</tr>
<tr>
<td>Ella</td>
<td>✓</td>
<td>72</td>
</tr>
<tr>
<td>Anya</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>Greg</td>
<td>✓</td>
<td>95</td>
</tr>
<tr>
<td>Max</td>
<td>✓</td>
<td>134</td>
</tr>
</tbody>
</table>

**Mean income:**
- Classical Inference: $48
- Privacy Protected Data: $108

**Quantity of Interest**

**Usually no direct relevance**
### 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>Mary</td>
<td>✓</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Andrey</td>
<td>✓</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>122</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>Ella</td>
<td>✓</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Anya</td>
<td>✓</td>
<td>132</td>
<td></td>
</tr>
<tr>
<td>Greg</td>
<td>✓</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>Max</td>
<td>✓</td>
<td>134</td>
<td></td>
</tr>
</tbody>
</table>

Mean income:

- Classical Inference: $48
- Usually no direct relevance
- $108

**Noise & Censoring**

- Quantity of Interest

---

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

<table>
<thead>
<tr>
<th>Population</th>
<th>Sample</th>
<th>Quantity of Interest</th>
<th>$ +Privacy</th>
<th>=dp$</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>✗</td>
<td></td>
<td>$48$</td>
<td></td>
</tr>
<tr>
<td>Mary</td>
<td>✓</td>
<td></td>
<td>76</td>
<td>85</td>
</tr>
<tr>
<td>Andrey</td>
<td>✓</td>
<td></td>
<td>96</td>
<td>103</td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td></td>
<td>145</td>
<td>75</td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td></td>
<td>122</td>
<td>113</td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td></td>
<td>86</td>
<td>125</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td></td>
<td>127</td>
<td>97</td>
</tr>
<tr>
<td>Ella</td>
<td>✓</td>
<td></td>
<td>72</td>
<td>101</td>
</tr>
<tr>
<td>Anya</td>
<td>✓</td>
<td></td>
<td>132</td>
<td>128</td>
</tr>
<tr>
<td>Greg</td>
<td>✓</td>
<td></td>
<td>95</td>
<td>83</td>
</tr>
<tr>
<td>Max</td>
<td>✓</td>
<td></td>
<td>134</td>
<td>201</td>
</tr>
</tbody>
</table>

**Mean income:**

- Classical Inference: $48$
- Query-Response: $108$
- Differential Privacy: $111$

### Notes:
- **Population:** Usually no direct relevance
- **Sample:** Usually no direct relevance
- **Noise & Censoring:** No direct relevance

---

Differential Privacy & Inferential Validity
### 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>Mary</td>
<td>✓</td>
<td>76</td>
<td></td>
<td>85</td>
</tr>
<tr>
<td>Andrey</td>
<td>✓</td>
<td>96</td>
<td></td>
<td>103</td>
</tr>
<tr>
<td>Georgie</td>
<td>✓</td>
<td>145</td>
<td></td>
<td>75</td>
</tr>
<tr>
<td>Gary</td>
<td>✓</td>
<td>122</td>
<td></td>
<td>113</td>
</tr>
<tr>
<td>Meg</td>
<td>✓</td>
<td>86</td>
<td></td>
<td>125</td>
</tr>
<tr>
<td>Abhradeep</td>
<td>✓</td>
<td>127</td>
<td></td>
<td>97</td>
</tr>
<tr>
<td>Ella</td>
<td>✓</td>
<td>72</td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>Anya</td>
<td>✓</td>
<td>132</td>
<td></td>
<td>128</td>
</tr>
<tr>
<td>Greg</td>
<td>✓</td>
<td>95</td>
<td></td>
<td>83</td>
</tr>
<tr>
<td>Max</td>
<td>✓</td>
<td>134</td>
<td></td>
<td>201</td>
</tr>
</tbody>
</table>

Mean income: $48 \rightarrow \text{Classical Inference} \rightarrow \$108 \rightarrow \text{Query-Response} \rightarrow \$111

Statistically Valid Inferences from Privacy Protected Data
Differential Privacy and its Inferential Challenges

- Estimators
  - Classical Statistics: Apply statistic $s(D)$ to dataset $D$
  - DP Mechanism: $M(s, D)$, with noise & censoring

- Essential components of ensuring privacy
- Fundamental problems for statistical inference

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

- Examples
  - All proven to protect the biggest possible outlier
    
    $M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N(0, 4\Lambda n \epsilon)$
  - 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
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**
  - 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 $D, D', m$
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**
  - 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**
  - 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
  - $M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N\left(0, \frac{4\Lambda}{n\epsilon}\right)$
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**
  - 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
  - $M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N\left(0, \frac{4\Lambda}{n\epsilon}\right)$
  - Or: mess with gradients, $X_i'X_i$, 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**
  - 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
  - $M(\text{mean}, D) = \frac{1}{n} \sum_{i=1}^{n} c(y_i, \Lambda) + N \left(0, \frac{4\Lambda}{n\epsilon} \right)$
  - Or: mess with gradients, $X_i'X_i$, data, QOIs, etc.

- **Statistical properties:** usually biased, no uncertainty estimates
Properties of Differential Privacy

- Post-processing: if $M(s, D)$ is DP, so is $f[M(s, D)]$.

- Useful for bias corrections.

- Average privacy loss $\ll$ maximum privacy loss.

- Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID.

- Risk for small groups ($k$) drops linearly, $k\epsilon$.

- Composition: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP.

- Privacy Budget:
  - Can sum and limit 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 $f[M(s, D)]$
Properties of Differential Privacy

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

Average privacy loss $\ll$ maximum privacy loss

Privacy risk quantified ($\epsilon$), instead of 0/1 for re-ID

Risk for small groups ($k$) drops linearly, $k\epsilon$

Composition: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP

Privacy Budget

- Can sum and limit 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
- **Average 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
- **Average privacy loss** $\ll$ maximum privacy loss
- **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
- **Average privacy loss** $\ll$ **maximum privacy loss**
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
- **Risk for small groups** ($k$) drops linearly, $k\epsilon$
Properties of Differential Privacy

- **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Average privacy loss** $\ll$ **maximum privacy loss**
- **Privacy risk quantified** ($\epsilon$), instead of 0/1 for re-ID
- **Risk for small groups** ($k$) drops linearly, $k\epsilon$
- **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

• **Average privacy loss** \( \ll \) maximum privacy loss

• **Privacy risk quantified** \( (\epsilon) \), instead of 0/1 for re-ID

• **Risk for small groups** \( (k) \) drops linearly, \( k\epsilon \)

• **Composition:** \( \epsilon_1\)-DP and \( \epsilon_2\)-DP is \( (\epsilon_1 + \epsilon_2)\)-DP

• **Privacy Budget**
Properties of Differential Privacy

- **Post-processing**: if $M(s, D)$ is DP, so is $f[M(s, D)]$
  - Useful for bias corrections
- **Average privacy loss** $\ll$ **maximum privacy loss**
- **Privacy risk quantified** $(\epsilon)$, instead of 0/1 for re-ID
- **Risk for small groups** $(k)$ drops linearly, $k\epsilon$
- **Composition**: $\epsilon_1$-DP and $\epsilon_2$-DP is $(\epsilon_1 + \epsilon_2)$-DP
- **Privacy Budget**
  - Can sum and limit 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
- **Average privacy loss** \( \ll \) **maximum privacy loss**
- **Privacy risk quantified** (\( \epsilon \)), instead of 0/1 for re-ID
- **Risk for small groups** (\( k \)) drops linearly, \( k\epsilon \)
- **Composition:** \( \epsilon_1 \)-DP and \( \epsilon_2 \)-DP is \( (\epsilon_1 + \epsilon_2) \)-DP
- **Privacy Budget**
  - Can sum and limit risks across analyses & researchers
  - When the budget is used, **no new analyses can ever be run**
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or "multiple comparison" corrections

• With DP: tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
  • Higher probability of being fooled by data
  • Must plan data analyses carefully!

• Risks
  • No differential privacy: no data access or privacy at risk
  • No inferential validity: incorrect scientific conclusions, medical & policy advice; society and individuals at risk

⇝ We need both DP and inferential validity
DP: Completely Changes Statistical Best Practices

- Normally we try to avoid being fooled by:
  - Data problems
    - by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  - Researcher biases
    - avoiding p-hacking via preregistration or "multiple comparison" corrections
  - With DP:
    - p-hacking avoided almost automatically
    - Little opportunity to explore data, run diagnostics, etc.
    - Lower probability of serendipitous discovery
    - Higher probability of being fooled by data
  - Must plan data analyses carefully!

Risks
- No differential privacy:
  - no data access or privacy at risk
- No inferential validity:
  - incorrect scientific conclusions, medical & policy advice; society and individuals at risk

We need both DP and inferential validity
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems
DP: Completely Changes Statistical Best Practices

- Normally we try to avoid being fooled by:
  - Data problems
  - Researcher biases

- Risks
  - No differential privacy: no data access or privacy at risk
  - No inferential validity: incorrect scientific conclusions, medical & policy advice; society and individuals at risk

⇝ We need both DP and inferential validity
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • **Data problems** — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • **Researcher biases**
  
  • **Data problems** — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • **Researcher biases**
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections
• With DP: tips the scales

Differential Privacy & Inferential Validity
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • **Data problems** — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • **Researcher biases** — avoiding p-hacking via preregistration or “multiple comparison” corrections

• **With DP:** tips the scales
  • p-hacking avoided almost automatically

---

Differential Privacy & Inferential Validity
DP: Completely Changes Statistical Best Practices

- Normally we try to avoid being fooled by:
  - **Data problems** — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  - **Researcher biases** — avoiding p-hacking via preregistration or “multiple comparison” corrections

- **With DP**: tips the scales
  - p-hacking avoided almost automatically
  - Little opportunity to explore data, run diagnostics, etc.
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections

• With DP: tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
DP: Completely Changes Statistical Best Practices

- **Normally we try to avoid being fooled by:**
  - **Data problems** — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  - **Researcher biases** — avoiding p-hacking via preregistration or “multiple comparison” corrections

- **With DP:** tips the scales
  - p-hacking avoided almost automatically
  - Little opportunity to explore data, run diagnostics, etc.
  - Lower probability of serendipitous discovery
  - Higher probability of being fooled by data
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • **Data problems** — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • **Researcher biases** — avoiding p-hacking via preregistration or “multiple comparison” corrections

• **With DP:** tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
  • Higher probability of being fooled by data
  • **Must plan data analyses carefully!**
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections

• With DP: tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
  • Higher probability of being fooled by data
  • Must plan data analyses carefully!

• Risks
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections

• With DP: tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
  • Higher probability of being fooled by data
  • Must plan data analyses carefully!

• Risks
  • No differential privacy: no data access or privacy at risk
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections

• With DP: tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
  • Higher probability of being fooled by data
  • Must plan data analyses carefully!

• Risks
  • No differential privacy: no data access or privacy at risk
  • No inferential validity: incorrect scientific conclusions, medical & policy advice; society and individuals at risk
DP: Completely Changes Statistical Best Practices

• Normally we try to avoid being fooled by:
  • Data problems — by running every possible diagnostic, data exploration and visualization, and conducting numerous statistical checks
  • Researcher biases — avoiding p-hacking via preregistration or “multiple comparison” corrections

• With DP: tips the scales
  • p-hacking avoided almost automatically
  • Little opportunity to explore data, run diagnostics, etc.
  • Lower probability of serendipitous discovery
  • Higher probability of being fooled by data
  • Must plan data analyses carefully!

• Risks
  • No differential privacy: no data access or privacy at risk
  • No inferential validity: incorrect scientific conclusions, medical & policy advice; society and individuals at risk
  • \( \rightsquigarrow \) We need both DP and inferential validity
Solving Political Problems Technologically

Differential Privacy & Inferential Validity

A General Purpose, Statistically Valid DP Algorithm

The Algorithm in Practice
A Differentially Private Estimator

Partition $D_1, D_2, D_3, D_4, D_5$ into disjoint sets

Bag of little bootstraps

Estimator $\hat{\theta}^p, b = s(D^p, \text{Multinom}(N, 1/n))$

Censor Average Noise $\hat{\theta}_{dp} = 1/P \sum_{p=1}^P c(\hat{\theta}^p, \Lambda) + N(0, 4\Lambda \epsilon P)$

Bias Correction & variance estimation
A Differentially Private Estimator

Private data
A Differentially Private Estimator

Private data

Partition

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

Private data
Partition
Bag of little bootstraps

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

Private data
Partition
Bag of little bootstraps
Estimator

\[ \hat{\theta}_p, b = s(D_p, \text{Multinom}(N, 1/n)) \]

Estimator

\[ \hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_3, \hat{\theta}_4, \hat{\theta}_5 \]

Bias Correction
(& variance estimation)

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 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)

\[ \hat{\theta}_{p,b} = s(D_p, \text{Multinom}(N, 1_n/n)) \]
A Differentially Private Estimator

Private data $D$

Partition $D_1, D_2, D_3, D_4, D_5$

Bag of little bootstraps

Estimator $\hat{\theta}_{p,b} = s(D_p, \text{Multinom}(N, 1_n/n))$

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)**

\[ \hat{\theta}_{p,b} = s(D_p, \text{Multinom}(N, 1_n/n)) \]

\[ \hat{\theta}_1 \quad \hat{\theta}_2 \quad \hat{\theta}_3 \quad \hat{\theta}_4 \quad \hat{\theta}_5 \]

\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N \left(0, \frac{4\Lambda}{\epsilon P} \right) \]
Bias Correction of: 

\[ \hat{\theta}^\text{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N \left( 0, \frac{4\Lambda}{\epsilon P} \right) \]
Bias Correction of: 

\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N(0, \frac{4\Lambda}{\epsilon P}) \]
Bias Correction of: \[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution

Uncensored distribution

\[ \hat{\theta}_p \sim N(\theta, \sigma^2) \]
Bias Correction of: \[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution

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

Uncensored distribution

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

\[ \int_{-\infty}^{-\Lambda} N(t | \theta, \sigma^2) dt \quad \int_{\Lambda}^{\infty} N(t | \theta, \sigma^2) dt \]
Bias Correction of: \[ \hat{\theta}_{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution
\[ \theta_C = -\alpha_1 \Lambda + (1 - \alpha_2 - \alpha_1)\theta_T + \alpha_2 \Lambda \]

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

\[ \int_{-\Lambda}^{\theta} N(t \mid \theta, \sigma^2) dt \]
\[ \int_{-\infty}^{0} N(t \mid \theta, \sigma^2) dt \]
\[ \int_{\theta}^{\Lambda} N(t \mid \theta, \sigma^2) dt \]
\[ \int_{\Lambda}^{\infty} N(t \mid \theta, \sigma^2) dt \]
Bias Correction of:  
\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution
\[ \theta_C = -\alpha_1 \Lambda + (1 - \alpha_2 - \alpha_1) \theta_T + \alpha_2 \Lambda \]

Estimate: \( \hat{\theta}^{dp} \)

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

\[ \int_{-\infty}^{-\Lambda} N(t \mid \theta, \sigma^2)dt \quad \int_{\Lambda}^{\infty} N(t \mid \theta, \sigma^2)dt \]
Bias Correction of: \[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution
\[ \theta_C = -\alpha_1 \Lambda + (1 - \alpha_2 - \alpha_1) \theta_T + \alpha_2 \Lambda \]

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

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

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

3 eqns, 4 unknowns \( \theta, \sigma^2, \alpha_1, \alpha_2 \)
Bias Correction of: \[ \hat{\theta}^\text{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\varepsilon P}\right) \]

Censored distribution
\[ \theta_C = -\alpha_1 \Lambda + (1 - \alpha_2 - \alpha_1) \theta_T + \alpha_2 \Lambda \]

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

Estimate: \( \hat{\theta}^\text{dp}, \hat{\alpha}_2^\text{dp} \)

3 eqns, 4 unknowns \( \theta, \sigma^2, \alpha_1, \alpha_2 \)
Bias Correction of: 
\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution
\[ \theta_C = -\alpha_1 \Lambda + (1 - \alpha_2 - \alpha_1)\theta_T + \alpha_2 \Lambda \]

Estimate: \( \hat{\theta}^{dp}, \hat{\alpha}_2^{dp} \)

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

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

3 eqns, 4 unknowns \( \theta, \sigma^2, \alpha_1, \alpha_2 \)
Bias Correction of: 

\[ \hat{\theta}^{dp} = \frac{1}{P} \sum_{p=1}^{P} c(\hat{\theta}_p, \Lambda) + N\left(0, \frac{4\Lambda}{\epsilon P}\right) \]

Censored distribution

\[ \theta_C = -\alpha_1 \Lambda + (1 - \alpha_2 - \alpha_1)\theta_T + \alpha_2 \Lambda \]

Estimate: \( \hat{\theta}^{dp}, \hat{\alpha}_2^{dp} \)

Uncensored distribution

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

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

3 eqns, 4 unknowns \( \theta, \sigma^2, \alpha_1, \alpha_2 \)

Solve for \( \theta \) (and \( \sigma^2, \alpha_1 \))
Variance Estimation

• DP Variance is unhelpful:
  $V(\hat{\theta}^{dp}) \neq V(\hat{\theta}^{dp})$

• Simulate estimates via standard procedures:
  $\hat{\theta}^{dp}(i), \hat{\alpha}^{dp2}(i) \sim N([\hat{\theta}^{dp} \hat{\alpha}^{dp2}], [\hat{V}(\hat{\theta}^{dp}) \hat{Cov}(\hat{\alpha}^{dp2}, \hat{\theta}^{dp}) \hat{Cov}(\hat{\alpha}^{dp2}, \hat{\theta}^{dp}) \hat{V}(\hat{\alpha}^{dp2})])$

• Functions of disclosed params

• Bias correct simulated params:
  $\{\tilde{\theta}^{dp}(i), \hat{\alpha}^{dp1}(i), \hat{\sigma}^{dp2}(i)\} = \text{BiasCorrect}[\hat{\theta}^{dp}(i), \hat{\alpha}^{dp2}(i)]$

• Standard error, SE($\tilde{\theta}^{dp}$):
  Standard deviation of $\tilde{\theta}^{dp}(i)$ over $i$
Variance Estimation

- **DP Variance is unhelpful:** \( V(\hat{\theta})^{dp} \neq V(\hat{\theta}^{dp}) \)
Variance Estimation

- **DP Variance is unhelpful:** $V(\hat{\theta}^{dp}) \neq V(\hat{\theta}^{dp})$
- **Simulate estimates via standard (Clarify) procedures:**

$$\hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i) \sim N\left(\begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}_2^{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}_2^{dp}) \end{bmatrix}\right)$$
Variance Estimation

- DP Variance is unhelpful: $V(\hat{\theta})^{dp} \neq V(\hat{\theta}^{dp})$
- Simulate estimates via standard (Clarify) procedures:

$$\hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i) \sim N\left(\begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}_2^{dp} \end{bmatrix}, \begin{bmatrix} V(\hat{\theta}^{dp}) & \widehat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) \\ \widehat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}_2^{dp}) \end{bmatrix} \right)$$

Functions of disclosed params

Bias correct simulated params:

$$\{\tilde{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i)\} = \text{BiasCorrect}[\hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i)]$$

- Standard error, $SE(\tilde{\theta}^{dp})$:
  - Standard deviation of $\tilde{\theta}^{dp}(i)$ over $i$
Variance Estimation

• DP Variance is unhelpful: \( V(\hat{\theta})^{dp} \neq V(\hat{\theta}^{dp}) \)

• Simulate estimates via standard (Clarify) procedures:

\[
\hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i) \sim N\left( \begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}_2^{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}_2^{dp}) \end{bmatrix} \right)
\]

Functions of disclosed params

• Bias correct simulated params:

\[
\{\tilde{\theta}^{dp}(i), \tilde{\alpha}_1^{dp}(i), \tilde{\sigma}_{dp}^2(i)\} = \text{BiasCorrect}\left[\hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i)\right]
\]
Variance Estimation

- **DP Variance is unhelpful:** $V(\hat{\theta}^\text{dp}) \neq V(\hat{\theta}^\text{dp})$
- **Simulate estimates** via standard (Clarify) procedures:

  $$\hat{\theta}^\text{dp}(i), \hat{\alpha}_2^\text{dp}(i) \sim N\left(\begin{bmatrix} \hat{\theta}^\text{dp} \\ \hat{\alpha}_2^\text{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^\text{dp}) & \hat{\text{Cov}}(\hat{\alpha}_2^\text{dp}, \hat{\theta}^\text{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}_2^\text{dp}, \hat{\theta}^\text{dp}) & \hat{V}(\hat{\alpha}_2^\text{dp}) \end{bmatrix}\right)$$

- **Bias correct simulated params:**

  $$\{\tilde{\theta}^\text{dp}(i), \tilde{\alpha}_1^\text{dp}(i), \tilde{\sigma}_2^\text{dp}(i)\} = \text{BiasCorrect}\left[\hat{\theta}^\text{dp}(i), \hat{\alpha}_2^\text{dp}(i)\right]$$

- **Standard error, SE(\tilde{\theta}^\text{dp}):** Standard deviation of $\tilde{\theta}^\text{dp}(i)$ over $i$
Variance Estimation

- **DP Variance is unhelpful:** \( V(\hat{\theta}^{dp}) \neq V(\hat{\theta}^{dp}) \)
- **Simulate estimates** via standard (Clarify) procedures:

\[
\begin{align*}
\hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i) &\sim N \left( \begin{bmatrix} \hat{\theta}^{dp} \\ \hat{\alpha}_2^{dp} \end{bmatrix}, \begin{bmatrix} \hat{V}(\hat{\theta}^{dp}) & \hat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) \\ \hat{\text{Cov}}(\hat{\alpha}_2^{dp}, \hat{\theta}^{dp}) & \hat{V}(\hat{\alpha}_2^{dp}) \end{bmatrix} \right) \\
\end{align*}
\]

- **Bias correct simulated params:**

\[
\begin{align*}
\{\tilde{\theta}^{dp}(i), \tilde{\alpha}_1^{dp}(i), \tilde{\sigma}_2^{dp}(i)\} &\equiv \text{BiasCorrect} \left[ \hat{\theta}^{dp}(i), \hat{\alpha}_2^{dp}(i) \right] \\
\end{align*}
\]

- **Standard error, SE(\(\tilde{\theta}^{dp}\)):** Standard deviation of \(\tilde{\theta}^{dp}(i)\) over \(i\)
- **Bias correction (usually) reduces bias and variance:**

\[
V(\tilde{\theta}^{dp}) < V(\hat{\theta}^{dp})
\]
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
Theory and Practice

- Reducing DP's Societal Risks.
  - Report: Effective reduction in \( N = 1 - \frac{\hat{\sigma}_{dp}^2}{SE(\hat{\theta}_{dp})} \)

- Choosing \( \epsilon \) (like a power calculation):
  \[ \frac{SE(\hat{\theta}_{dp})^2}{\epsilon^2} < \frac{V(\hat{\theta}_{dp}) + (4\Lambda \epsilon^2)}{} \]

- Choosing \( \Lambda \):
  - Without bias correction: choose more censoring or more noise!
  - With bias correction: keep \( \max(\alpha_1, \alpha_2) < 0.6 \)

- Privacy Policies:
  - Science informs, but does not determine, policy
  - Few if any implementations exactly meet DP standards
  - Most use larger \( \epsilon \) and no budget, but with other protections
  - It's safer: de-identification + noise and censoring

The Algorithm in Practice
Theory and Practice

- **Reducing DP’s Societal Risks.** Report:

\[
\text{Effective reduction in } N = 1 - \frac{\hat{\sigma}_{dp}^2}{P \cdot SE(\tilde{\theta}_{dp})}
\]
Theory and Practice

• Reducing DP’s Societal Risks. Report:

\[
\text{Effective reduction in } N = 1 - \frac{\hat{\sigma}^2_{dp}/P}{\text{SE}(\tilde{\theta}_{dp})}
\]

• Choosing \( \epsilon \) (like a power calculation):

\[
\text{SE}(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2
\]

Privacy Policies:

• Science informs, but does not determine, policy
• Few if any implementations exactly meet DP standards
• Most use larger \( \epsilon \) and no budget, but with other protections
• It’s safer: de-identification + noise and censoring
Theory and Practice

- **Reducing DP’s Societal Risks. Report:**

  
  \[
  \text{Effective reduction in } N = 1 - \frac{\hat{\sigma}^2_{dp}/P}{\text{SE}(\tilde{\theta}^dp)}
  \]

- **Choosing } \epsilon (like a power calculation):**

  \[
  \text{SE}(\tilde{\theta}^dp)^2 < V(\hat{\theta}^dp) + \left(\frac{4\Lambda}{\epsilon P}\right)^2
  \]

- **Choosing } \Lambda
Theory and Practice

• Reducing DP’s Societal Risks. Report:

\[
effective \ reduction \ in \ N = 1 - \frac{\hat{\sigma}^2_{dp}/P}{SE(\tilde{\theta}_{dp})}
\]

• Choosing \( \epsilon \) (like a power calculation):

\[
SE(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2
\]

• Choosing \( \Lambda \)
  • Without bias correction: choose more censoring or more noise!
Theory and Practice

- **Reducing DP’s Societal Risks.** Report:

  \[
  \text{Effective reduction in } N = 1 - \frac{\sigma_{dp}^2/P}{SE(\tilde{\theta}_{dp})}
  \]

- **Choosing } \epsilon (like a power calculation):

  \[
  \text{SE}(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2
  \]

- **Choosing } \Lambda
  - Without bias correction: choose more censoring or more noise!
  - With bias correction: Keep max(\(\alpha_1, \alpha_2\)) < 0.6

The Algorithm in Practice
Theory and Practice

• Reducing DP’s Societal Risks. Report:

\[
\text{Effective reduction in } N = 1 - \frac{\hat{\sigma}_{dp}^2 / P}{SE(\tilde{\theta}_{dp})}
\]

• Choosing \( \epsilon \) (like a power calculation):

\[
SE(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left( \frac{4\Lambda}{\epsilon P} \right)^2
\]

• Choosing \( \Lambda \)
  • Without bias correction: choose more censoring or more noise!
  • With bias correction: Keep \( \max(\alpha_1, \alpha_2) < 0.6 \)

• Privacy Policies:
Theory and Practice

• Reducing DP’s Societal Risks. Report:

\[
\text{Effective reduction in } N = 1 - \frac{\hat{\sigma}_{dp}^2}{P \cdot \text{SE}(\tilde{\theta}_{dp})}
\]

• Choosing \( \epsilon \) (like a power calculation):

\[
\text{SE}(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2
\]

• Choosing \( \Lambda \)
  • Without bias correction: choose more censoring or more noise!
  • With bias correction: Keep \( \max(\alpha_1, \alpha_2) < 0.6 \)

• Privacy Policies:
  • Science informs, but does not determine, policy
Theory and Practice

- Reducing DP’s Societal Risks. Report:

  Effective reduction in $N = 1 - \frac{\hat{\sigma}_{dp}^2 / P}{SE(\tilde{\theta}_{dp})}$

- Choosing $\epsilon$ (like a power calculation):

  $SE(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2$

- Choosing $\Lambda$
  - Without bias correction: choose more censoring or more noise!
  - With bias correction: Keep $\max(\alpha_1, \alpha_2) < 0.6$

- Privacy Policies:
  - Science informs, but does not determine, policy
  - Few if any implementations exactly meet DP standards
Theory and Practice

- Reducing DP’s Societal Risks. Report:

  $$\text{Effective reduction in } N = 1 - \frac{\hat{\sigma}_{dp}^2/P}{SE(\tilde{\theta}_{dp})}$$

- Choosing $\epsilon$ (like a power calculation):

  $$SE(\tilde{\theta}_{dp})^2 < V(\hat{\theta}_{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2$$

- Choosing $\Lambda$
  - Without bias correction: choose more censoring or more noise!
  - With bias correction: Keep $\max(\alpha_1, \alpha_2) < 0.6$

- Privacy Policies:
  - Science informs, but does not determine, policy
  - Few if any implementations exactly meet DP standards
  - Most use larger $\epsilon$ and no budget, but with other protections
Theory and Practice

• **Reducing DP’s Societal Risks.** Report:

\[
\text{Effective reduction in } N = 1 - \frac{\hat{\sigma}_{dp}^2 / P}{\text{SE}(\tilde{\theta}^{dp})}
\]

• Choosing \( \epsilon \) (like a power calculation):

\[
\text{SE}(\tilde{\theta}^{dp})^2 < V(\hat{\theta}^{dp}) + \left(\frac{4\Lambda}{\epsilon P}\right)^2
\]

• Choosing \( \Lambda \)
  • Without bias correction: choose more censoring or more noise!
  • With bias correction: Keep \( \max(\alpha_1, \alpha_2) < 0.6 \)

• **Privacy Policies:**
  • Science informs, but does not determine, policy
  • Few if any implementations exactly meet DP standards
  • Most use larger \( \epsilon \) and no budget, but with other protections
  • It’s safer: de-identification + noise and censoring
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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty

Utility requires known statistical properties and valid uncertainty estimates

Proposed algorithm

Generic:

- Almost any statistical method or quantity of interest
- Statistically unbiased (if estimator is), lower variance
- Valid uncertainty estimates
- Computationally efficient

The Algorithm in Practice
Concluding Remarks

• Data sharing \(\leadsto\) data access
Concluding Remarks

• Data sharing $\rightarrow$ 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 ⇛ data access**
  - DP protects individual privacy
  - Enables inference to private database, not population
  - Usually biased, no 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

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**
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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  - Utility requires known statistical properties and valid uncertainty estimates
Concluding Remarks

• Data sharing $\implies$ 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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  • Utility requires known statistical properties and 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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  - Utility requires known statistical properties and valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  - Utility requires known statistical properties and valid uncertainty estimates

• **Proposed algorithm**
  - **Generic:** almost any statistical method or quantity of interest
  - Statistically **unbiased** (if estimator is), **lower variance**
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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  - Utility requires known statistical properties and valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically **unbiased** (if estimator is), **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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  - Utility requires known statistical properties and valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically unbiased (if estimator is), **lower variance**
  - Valid uncertainty estimates
  - Computationally efficient
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 is not one that is correct; it is one that comes with an appropriate degree of uncertainty
  - Utility requires known statistical properties and valid uncertainty estimates

- **Proposed algorithm**
  - **Generic**: almost any statistical method or quantity of interest
  - Statistically unbiased (if estimator is), lower variance
  - Valid uncertainty estimates
  - Computationally efficient
  - Easy to implement
For more information

Georgina-Evans.com

GaryKing.org

MegSchwenzfeier.com

bit.ly/AbhradeepThakurta

Paper, software, slides: GaryKing.org/dp