Differential Privacy [and Analysis of Social Networks]

Kobbi Nissim

BGU/Harvard/BU

Charles River Workshop on Private Analysis of Social Networks
May 2014
Data Privacy - The Problem

- **Given:**
  - A dataset with sensitive information

- **How to:**
  - Compute and release functions of the dataset without compromising individual privacy
**DATA PRIVACY - THE PROBLEM**

- **Given:**
  - A dataset with sensitive information
- **How to:**
  - Compute and release functions of the dataset without compromising individual privacy

---

**Diagram:**

- **Individuals** sending data to **Server/agency** which computes and releases functions of the dataset.
- **Users** (Government, researchers, businesses (or) Malicious adversary) are the ones querying for answers.
Age of Miss America compared with Murders by steam, hot vapours and hot objects
DATA PRIVACY - THE PROBLEM

**Given:**
- A dataset with sensitive information

**How to:**
- Compute and release functions of the dataset without compromising individual privacy

---

![Diagram of data privacy problem]

- **Individuals**
  - $x_1$
  - $x_2$
  - $\vdots$
  - $x_n$

- **Server/agency**

- **Users**
  - Government, researchers, businesses (or)
  - Malicious adversary

- **Queries**
- **Answers**
**Data Privacy - The Problem**

- **Given:**
  - A dataset with sensitive information

- **How to:**
  - Compute and release functions of the dataset without compromising individual privacy

![Diagram of data privacy problem]

Database $X$: $x_1, x_2, x_3, \ldots, x_{n-1}, x_n$

Server/agency

Users:
- Government, researchers, businesses
- (or)
- Malicious adversary

Server/agency answers queries from Users.
**Data Privacy - The Problem**

- **Given:**
  - A dataset with sensitive information

- **How to:**
  - Compute and release functions of the dataset without compromising individual privacy

![Diagram](www.perey.com)
Yes, This Has Been Asked Before
YES, THIS HAS BEEN ASKED BEFORE

- Traditional approaches:
  - Anonymization, redaction, auditing, noise addition, synthetic data, ...
    - Still in use
    - Accumulating litany of attacks and failures
Yes, This Has Been Asked Before

- Traditional approaches:
  - Anonymization, redaction, auditing, noise addition, synthetic data, ...
    - Still in use
    - Accumulating litany of attacks and failures

- Lack of rigor leads to unforeseen breaks
YES, THIS HAS BEEN ASKED BEFORE

- Traditional approaches:
  - Anonymization, redaction, auditing, noise addition, synthetic data, ...
    - Still in use
    - Accumulating litany of attacks and failures

- Lack of rigor leads to unforeseen breaks
- Privacy protection is unlike other ‘incremental’ algorithmic endeavors
  - Information cannot be “de-leaked”, breaks are forever
Aggregate Computations and Privacy

- Aren't releases of "global" information safe?
  - Statistics, machine learning, ...
  - Don’t I “hide in the crowd”?
 Aren’t releases of “global” information safe?
  - Statistics, machine learning, …
  - Don’t I “hide in the crowd”?

“Global” goal can depend on a few specific values
  - Not uncommon, e.g., Support Vector Machines
Aggregate Computations and Privacy

- Aren’t releases of “global” information safe?
  - Statistics, machine learning, ...
  - Don’t I “hide in the crowd”?
- “Global” goal can depend on a few specific values
  - Not uncommon, e.g., Support Vector Machines
- Composition
  - Compute average salary before/after professor resigns
Aren’t releases of “global” information safe?
- Statistics, machine learning, ...
- Don’t I “hide in the crowd”?

“Global” goal can depend on a few specific values
- Not uncommon, e.g., Support Vector Machines

Composition
- Compute average salary before/after professor resigns

Statistics may together encode sensitive info
- Too many, “too accurate” stats ⇒ reconstruct the data
- Robust even to fairly significant noise
How to compute aggregates ...
DATA PRIVACY - THE PROBLEM
[REFORMULATED FOR TODAY’S PURPOSES]

How to compute aggregates ...

... while controlling the leakage of individual information
What is differential privacy
  - Differential privacy for graph data - edge/node privacy

Interpretations of the definition

Basic properties

Basic techniques
Differential Privacy

- Changes to my data (almost) unnoticeable in outcome
  - I can claim that my data is different from what it really is (deniability)
Differential Privacy

- Changes to my data (almost) unnoticeable in outcome
  - I can claim that my data is different from what it really is (deniability)

- Omission/inclusion of my data (almost) unnoticeable in outcome
  - As if I chose to opt out
Differential Privacy

- Changes to my data (almost) unnoticeable in outcome
  - I can claim that my data is different from what it really is (deniability)

- Omission/inclusion of my data (almost) unnoticeable in outcome
  - As if I chose to opt out

- My data?
  - Record containing my information in a database
DIFFERENTIAL PRIVACY

- Changes to my data (almost) unnoticeable in outcome
  - I can claim that my data is different from what it really is (deniability)

- Omission/inclusion of my data (almost) unnoticeable in outcome
  - As if I chose to opt out

- My data?
  - Record containing my information in a database
  - Graph data: edge/node
**Neighboring Inputs**

*What Should Be Protected?*

- Inputs are neighboring if they differ on the data of a single individual
  - **Record privacy:** Databases $X, X'$ neighboring if differ on one record
**Neighboring Inputs**

[What Should Be Protected?]

- Inputs are neighboring if they differ on the data of a single individual
  - **Record privacy:** Databases $X, X'$ neighboring if differ on one record
  - **Edge privacy:** graphs $G, G'$ neighboring if differ on one edge

Image credit: www.perey.com
**NEIGHBORING INPUTS**

[**WHAT SHOULD BE PROTECTED?**]

- Inputs are neighboring if they differ on the data of a single individual
  - **Record privacy**: Databases $X, X'$ neighboring if differ on one record
  - **Edge privacy**: graphs $G, G'$ neighboring if differ on one edge
  - **Node privacy**: graphs $G, G'$ neighboring if differ on one node and its adjacent edges

Image credit: www.perey.com
DIFFERENTIAL PRIVACY
[DMNS 06]
A is **differentially private if**

- for all neighboring G, G'
- given A’s outcome, privacy attacker cannot guess whether input was G or G'

![Diagram showing the process](image)
A is differentially private if

- for all neighboring $G, G'$
- for all subsets $S$ of outputs
  \[ \Pr[A(G) \in S] \approx \Pr[A(G') \in S] \]
**Differential Privacy**

[DMNS 06]

- $A$ is $\varepsilon$-differentially private if
  - for all neighboring $G, G'$
  - for all subsets $S$ of outputs
    \[
    \Pr[A(G) \in S] \leq e^\varepsilon \cdot \Pr[A(G') \in S]
    \]
**Differential Privacy**

**[DMNS 06]**

- $A$ is $\epsilon$-differentially private if
  - for all neighboring $G, G'$
  - for all subsets $S$ of outputs
    \[ \Pr[A(G) \in S] \leq e^\epsilon \cdot \Pr[A(G') \in S] \]

**Notes:**
- DP is a property of the algorithm $A$
  - No sense in saying that a particular output preserves privacy - relationship between input and output is what matters
Differential Privacy
[DMNS 06]

• A is $\varepsilon$-differentially private if
  o for all neighboring $G, G'$
  o for all subsets $S$ of outputs

$$\Pr[A(G) \in S] \leq e^\varepsilon \cdot \Pr[A(G') \in S]$$

Notes:
• DP is a property of the algorithm $A$
  o No sense in saying that a particular output preserves privacy - relationship between input and output is what matters
• The parameter $\varepsilon$ measures 'leakage' or 'harm' (more later).
  o Not negligible. Think $\varepsilon \approx \frac{1}{100}$ or $\varepsilon \approx \frac{1}{10}$ not $\varepsilon \approx 2^{-80}$
Differential Privacy
[DMNS 06]

- $A$ is $\varepsilon$-differentially private if
  - for all neighboring $G, G'$
  - for all subsets $S$ of outputs
    \[ \Pr[A(G) \in S] \leq e^{\varepsilon} \cdot \Pr[A(G') \in S] \]

Notes:
- DP is a property of the algorithm $A$
  - No sense in saying that a particular output preserves privacy - relationship between input and output is what matters
- The parameter $\varepsilon$ measures ‘leakage’ or ‘harm’ (more later).
  - Not negligible. Think $\varepsilon \approx \frac{1}{100}$ or $\varepsilon \approx \frac{1}{10}$ not $\varepsilon \approx 2^{-80}$
- Choice of distance measure (max log ratio) not accidental
Basic Properties Of Differential Privacy

- Post processing:
  - If $A$ is $\epsilon$-dp then $B \circ A$ is $\epsilon$-dp for all $B$
Basic Properties Of Differential Privacy

Post processing:
- If $A$ is $\varepsilon$-dp then $B \circ A$ is $\varepsilon$-dp for all $B$.

Composition:
- $A_1, A_2$: $\varepsilon$-dp then $(A_1, A_2)$ is $2\varepsilon$-dp.
  - More efficient composition theorems exist w.r.t. a relaxation of differential privacy.
Basic Properties Of Differential Privacy

- **Post processing:**
  - If $A$ is $\varepsilon$-dp then $B \circ A$ is $\varepsilon$-dp for all $B$

- **Composition:**
  - $A_1, A_2$: $\varepsilon$-dp then $(A_1, A_2)$ is $2\varepsilon$-dp.
    - More efficient composition theorems exist w.r.t. a relaxation of differential privacy
    - $t$ executions of $\varepsilon$-dp private mechanisms are
      $$\approx \sqrt{t\varepsilon}$$-dp
**INTERPRETING DIFFERENTIAL PRIVACY**

- A naïve hope: Your beliefs about me are the same after you see the output as they were before.
INTERPRETING DIFFERENTIAL PRIVACY

- A naïve hope: Your beliefs about me are the same after you see the output as they were before.

- Suppose I smoke in public
  - A public health study could teach that I am at risk for cancer.
  - But it didn’t matter whether or not my data was part of it.
INTERPRETING DIFFERENTIAL PRIVACY

- A naïve hope: Your beliefs about me are the same after you see the output as they were before.

- Suppose I smoke in public
  - A public health study could teach that I am at risk for cancer.
  - But it didn’t matter whether or not my data was part of it.

- Theorem [Dwork Naor 06]: Learning things about individuals is unavoidable in the presence of arbitrary external information.
**Interpreting Differential Privacy**

- Compare \( x = (x_1, x_2, ..., x_i, ..., x_n) \) to \( x_{-i} = (x_1, x_2, ..., \perp, ..., x_n) \)

- \( A \) is \( \varepsilon \)-differentially private if for all vectors \( x \) and for all \( i \): \( A(x) \approx \varepsilon \ A(x_{-i}) \).
**INTERPRETING DIFFERENTIAL PRIVACY**

- **Compare** $x = (x_1, x_2, ..., x_i, ..., x_n)$
  to $x_{-i} = (x_1, x_2, ..., \bot, ..., x_n)$

- **$A$ is $\varepsilon$-differentially private if for all vectors $x$**
  and for all $i$: $A(x) \approx _\varepsilon A(x_{-i})$.

- **No matter what you know ahead of time, you learn (almost) the same things about me whether or not my data are used.**
**Interpreting Differential Privacy**

- **Compare** $x = (x_1, x_2, ..., x_i, ..., x_n)$ to $x_{-i} = (x_1, x_2, ..., \perp, ..., x_n)$

- **$A$ is $\varepsilon$-differentially private if for all vectors $x$ and for all $i$:** $A(x) \approx \varepsilon A(x_{-i})$.

- **For any non-negative function $p$ of the outcome,**
  \[ E[p(A(x))] \leq e^\varepsilon \cdot E[p(A(x'))] \]
INTERPRETING DIFFERENTIAL PRIVACY

- Compare $x = (x_1, x_2, ..., x_i, ..., x_n)$ to $x_{-i} = (x_1, x_2, ..., \bot, ..., x_n)$

- $A$ is $\varepsilon$-differentially private if for all vectors $x$ and for all $i$: $A(x) \approx _{\varepsilon} A(x_{-i})$.

- For any non-negative function $p$ of the outcome,
  \[ E[p(A(x))] \leq e^\varepsilon \cdot E[p(A(x'))] \]
  - Let $p$ = my insurance premium
  - My expected premium almost does not change whether I participate in $A$ or not!
THINGS TO NOTE ABOUT DIFFERENTIAL PRIVACY

- May not protect sensitive global information, e.g.
  - Clinical data: Smoking and cancer
  - Financial transactions: firm-level trading strategies
  - Genomic data: information about me may be revealed if enough of my family members participate
  - Social data: what if my presence affects everyone else?
**Things to Note About Differential Privacy**

- May not protect sensitive global information, *e.g.*
  - Clinical data: Smoking and cancer
  - Financial transactions: firm-level trading strategies
  - Genomic data: information about me may be revealed if enough of my family members participate
  - Social data: what if my presence affects everyone else?
  - Bug of feature?
THINGS TO NOTE ABOUT DIFFERENTIAL PRIVACY

- **May not protect sensitive global information, e.g.**
  - Clinical data: Smoking and cancer
  - Financial transactions: firm-level trading strategies
  - Genomic data: information about me may be revealed if enough of my family members participate
  - Social data: what if my presence affects everyone else?
  - **Bug of feature?**

- **Leakage accumulates with composition**
  - \( \varepsilon \) adds up with many releases
    - Very unlikely what is usual in crypto
    - Inevitable in some form (reconstruction attacks)
THINGS TO NOTE ABOUT DIFFERENTIAL PRIVACY

- May not protect sensitive global information, e.g.
  - Clinical data: Smoking and cancer
  - Financial transactions: firm-level trading strategies
  - Genomic data: information about me may be revealed if enough of my family members participate
  - Social data: what if my presence affects everyone else?
  - Bug of feature?

- Leakage accumulates with composition
  - $\epsilon$ adds up with many releases
    - Very unlike what is usual in crypto
    - Inevitable in some form (reconstruction attacks)
  - How to set $\epsilon$?
Variations on Differential Privacy

- Predecessors [DDN’03, EGS’03, DN’04, BDMN’05]

- $(\epsilon, \delta)$-differential privacy [DKMMN’05]
  - Require $\Pr[A(x) \in S] \leq e^\epsilon \Pr[A(x') \in S] + \delta$
  - Similar semantics to $(\epsilon,0)$-differential privacy when $\delta \ll 1/\text{poly}(n)$
  - Allows for improved utility

- Computational variants [MPRV09, MMPRTV’10].

- Distributional variants [RHMS’09, BBGLT’11, BGKS’13].
  - Assume something about adversary's prior distribution.
  - Deterministic releases.
  - Poor composition guarantees.

- Generalizations.
  - [BLR’08, GLP’11] simulation-based definitions.

- Crowd-blending privacy [GHLP’12].
EXAMPLE: COUNTING EDGES
[THE BASIC TECHNIQUE]

- $f(G) = \sum e_{ij}$ where $e_{ij} \in \{0,1\}$
Example: Counting Edges
[The Basic Technique]

- \( f(G) = \Sigma e_{ij} \) where \( e_{ij} \in \{0,1\} \)
- **Algorithm:** On input \( G \) return \( f(G) + Y \), where \( Y \sim Lap(\frac{1}{\varepsilon}) \)

- Laplace Distribution:
  - \( E[Y] = 0; \sigma[Y] = \sqrt{2}/\varepsilon \)

\[
h(y) = \frac{\varepsilon}{2} e^{-\varepsilon |y|}
\]
**Example: Counting Edges**

*The Basic Technique*

- $f(G) = \sum e_{ij}$ where $e_{ij} \in \{0,1\}$
- **Algorithm**: On input $G$ return $f(G) + Y$, where $Y \sim Lap\left(\frac{1}{\epsilon}\right)$

**Laplace Distribution:**
- $E[Y] = 0$; $\sigma[Y] = \sqrt{2}/\epsilon$
- Sliding property: $\frac{h(y)}{h(y+1)} \leq e^{\epsilon}$

$$h(y) = \frac{\epsilon}{2} e^{-\frac{\epsilon}{2} |y|}$$
**Example: Counting Edges**

**[The Basic Technique]**

- \( f(G) = \sum e_{ij} \) where \( e_{ij} \in \{0,1\} \)
- **Algorithm:** On input \( G \) return \( f(G) + Y \), where \( Y \sim \text{Lap}(\frac{1}{\varepsilon}) \)

**Laplace Distribution:**
- \( E[Y] = 0; \sigma[Y] = \sqrt{2}/\varepsilon \)
- **Sliding property:** \( \frac{h(y)}{h(y+1)} \leq e^\varepsilon \)

**For \( G, G' \) edge neighboring:**

\[
|f(G) - f(G')| = \left| \sum_{ij} e_{ij} - \sum_{ij} e'_{ij} \right| \leq 1
\]
Framework of Global Sensitivity [DMNS06]

- $GS_f = \max |f(G) - f(G')|_1$ taken over neighboring $G, G'$

- Theorem [DMNS06]:
  - $A(G) = f(G) + \text{Lap}^d \left( \frac{GS_f}{\epsilon} \right)$ is $\epsilon$-differentially private
**Framework of Global Sensitivity**

\[ GS_f = \max |f(G) - f(G')|_1 \text{ taken over neighboring } G, G' \]

\[ A(G) = f(G) + \text{Lap}^d \left( \frac{GS_f}{\epsilon} \right) \]

- Many natural functions have low global sensitivity
  - e.g., histogram, mean, covariance matrix, distance to a function, estimators with bounded “sensitivity curve”, strongly convex optimization problems.
FRAMEWORK OF GLOBAL SENSITIVITY

\[ GS_f = \max |f(G) - f(G')|_1 \text{ taken over neighboring } G, G' \]

\[ A(G) = f(G) + \text{Lap}^d \left( \frac{GS_f}{\epsilon} \right) \]

- Many natural functions have low global sensitivity
  - e.g., histogram, mean, covariance matrix, distance to a function, estimators with bounded “sensitivity curve”, strongly convex optimization problems.

- Laplace mechanism can be a programming interface [BDMN '05].
  - Implemented in several systems [McSherry '09, Roy et al. '10, Haeberlen et al. '11, Moharan et al. '12].
Edge vs. Node Privacy - Counting Edges

\[ GS_f = \max |f(G) - f(G')|_1 \text{ taken over neighboring } G, G' \]

\[ A(G) = f(G) + \text{Lap}^d\left(\frac{GS_f}{\epsilon}\right) \]

- Counting edges: \( f(G) = \sum e_{ij} \text{ where } e_{ij} \in \{0,1\} \)
- Edge privacy: \( GS_f = 1, \text{ noise } \sim \frac{1}{\epsilon} \)
- Node privacy: \( GS_f = n, \text{ noise } \sim \frac{n}{\epsilon} \)
**Edge vs. Node Privacy - Counting Edges**

\[ G_S f = \max |f(G) - f(G')|_1 \text{ taken over neighboring } G, G' \]

\[ A(G) = f(G) + \text{Lap}^d \left( \frac{G_S f}{\epsilon} \right) \]

- **Counting edges:** \( f(G) = \sum e_{ij} \) where \( e_{ij} \in \{0,1\} \)
- **Edge privacy:** \( G_S f = 1 \), noise \( \sim \frac{1}{\epsilon} \)
- **Node privacy:** \( G_S f = n \), noise \( \sim \frac{n}{\epsilon} \)

- **Degree distribution??**
**GLOBAL VS. LOCAL SENSITIVITY**

Database Space  

Range($f$)  

(Distribr/s on) Output Space
GLOBAL VS. LOCAL SENSITIVITY

Database Space  \( X \)  Range(\( f \))  (Distribs on) Output Space

\( f(X) \)  \( A(X) \)
GLOBAL VS. LOCAL SENSITIVITY

Database Space  Range(f)  (Distribbs on) Output Space

$X$  $f(X)$  $A(X)$
GLOBAL VS. LOCAL SENSITIVITY

Database Space → Range(f) → (Distribrbs on) Output Space

$X \rightarrow f(X) \rightarrow A(X)$
Global vs. Local Sensitivity

$LS_f (X) = \max_{X' \text{neighbor of } X} |f(X) - f(X')|_1$
**Global vs. Local Sensitivity**

Database Space | Range(\(f\)) | (Distrib on) Output Space

\[ \frac{L S_f (X)}{X} = \max_{X \text{ neighbor of } X} |f(X) - f(X')|_1 \]

\[ GS_f = \max_X LS_f (X) \]
**Global vs. Local Sensitivity**

- $LS_f(X) = \max_{x' \text{ neighbor of } x} |f(X) - f(X')|_1$
- $GS_f = \max_X LS_f(X)$
- [NRS'07,DL'09] Techniques with error $\approx$ local sensitivity
**Exponential Sampling [MT07]**

- $x_i = \{\text{books read by } i \text{ this year}\}$, $Y = \{\text{book names}\}$
- “Score” of $y \in Y$: $q(y, x) = \#\{i: y \in x_i\}$
- **Goal**: output book read by most
**Exponential Sampling [MT07]**

- \( x_i = \{\text{books read by } i \text{ this year}\}, \ Y = \{\text{book names}\} \)
- “Score” of \( y \in Y \): \( q(y, x) = \#\{i: y \in x_i\} \)
- **Goal**: output book read by most

- **Mechanism**: given \( x \), output book name \( y \) with probability prop to \( \exp\left(\frac{\xi}{2} \cdot q(y, x)\right) \)
**Exponential Sampling [MT07]**

- $x_i = \{\text{books read by } i \text{ this year}\}$, $Y = \{\text{book names}\}$
- "Score" of $y \in Y$: $q(y, x) = \#\{i: y \in x_i\}$
- **Goal**: output book read by most

- **Mechanism**: given $x$, output book name $y$ with probability prop to $\exp\left(\frac{\varepsilon}{2} \cdot q(y, x)\right)$

- **Claim**: Mechanism is $\varepsilon$-differentially private
**Exponential Sampling [MT07]**

- $x_i = \{\text{books read by } i \text{ this year}\}$, $Y = \{\text{book names}\}$
- “Score” of $y \in Y$: $q(y, x) = \# \{i: y \in x_i\}$
- **Goal**: output book read by most

- **Mechanism**: given $x$, output book name $y$ with probability prop to $\exp\left(\frac{\epsilon}{2} \cdot q(y, x)\right)$

- **Claim**: Mechanism is $\epsilon$-differentially private

- **Claim**: If most popular website has score $T = \max_{y \in Y} q(y, x)$, then $E[q(y_0, x)] \geq t - O\left(\frac{\log|Y|}{\epsilon}\right)$
APPLICATIONS OF EXPONENTIAL SAMPLING

• Very general and widely used
  ○ Often a ‘first attempt’ at a differentially private task.

• Used explicitly for
  ○ Learning discrete classifiers, Synthetic data generation, Convex Optimization, Genome-wide association studies, High-dimensional sparse regression, ...

• But, generally inefficient [DNRRV,...]
Differential Privacy in “Practice”

• Currently, differential private algorithms hard to use.
  o Noise.
  o No off-the-shelf software.
  o Each application requires fresh thinking.

• Several systems to make use easier.
  o [McSherry’09] PINQ: variation on LINQ with differential privacy enforced by query mechanism.
  o [Haeberlen et al. ’11] Programming language with privacy enforced by type system.
  o [Roy et al. ’10, Moharan et al. ’12] Systems for restricted classes of queries, focus on usability with legacy code.

• Hard to get right!
  o [Mironov ’12] Leakage via numerical errors.
Settings where Differential Privacy was Applied [Partial List]

- Machine learning
- Statistics
- Continual observation and pan privacy
  - When input is supplied gradually
  - When the state of the algorithm can be subpoenaed
- Distributed settings
  - Surprising relationships with computational differential privacy
- Mechanism design
- Privacy for the analyzer
- Graph data
CONCLUSIONS

• Heuristic treatment of privacy leads to failures
  o Weaknesses: Auxiliary information, (self) composition, leakage in decisions, ...
• Differential Privacy: privacy defined in terms of my effect on output
  o Meaningful despite arbitrary external information.
  o I should participate if I get benefit.
• Computations with rigorous privacy guarantees.
  o Basic Tools.
  o More advanced examples.
• Connections to many areas: Security and crypto, Machine learning, Statistics, Economics.