What Are the Chances?
Explaining the Epsilon Parameter in Differential Privacy

 Priyanka Nanayakkara  
Northwestern University

Mary Anne Smart  
University of California San Diego

Rachel Cummings*  
Columbia University

Gabriel Kaptchuk*  
Boston University

Elissa M. Redmiles*  
Max Planck Institute for Software Systems

* equal advising

Should I share my data?
Should I share my data?
Should I share my data?

Desfontaines, D (2023). A list of real-world uses of differential privacy
Diagram adapted from
Wood, Altman, Bembenek et al. (2020). Differential Privacy: A Primer for a Non-Technical Audience
Near, Darais, Boeckl (2020). Differential Privacy for Privacy-Preserving Data Analysis: An Introduction to our Blog Series

Dwork, McSherry, Nissim, Smith (2006). Calibrating noise to sensitivity in private data analysis
Diagram adapted from
Wood, Altman, Bembenek et al. (2020). Differential Privacy: A Primer for a Non-Technical Audience
Near, Darais, Boeckl (2020). Differential Privacy for Privacy-Preserving Data Analysis: An Introduction to our Blog Series

Dwork, McSherry, Nissim, Smith (2006). Calibrating noise to sensitivity in private data analysis
Epsilon Registry

Dwork, Kohli, Mulligan (2019). Differential privacy in practice: Expose your epsilons!
Epsilon Registry

Need \( \varepsilon \) explanations!

Dwork, Kohli, Mulligan (2019). Differential privacy in practice: Expose your epsilons!
To reduce the intrusion into personal privacy, the company says they will use a technique called differential privacy. Differential privacy injects statistical noise into collected data in a way that protects privacy without significantly changing conclusions.

Adapted from Cummings et al.’s “Techniques” description
To reduce the intrusion into personal privacy, the company says they will use a technique called differential privacy. Differential privacy injects statistical noise into collected data in a way that protects privacy without significantly changing conclusions.

Adapted from Cummings et al.’s “Techniques” description

No $\epsilon$ information!
Challenges to explaining $\varepsilon$
unit-less & contextless
probabilistic guarantees

Slovic (2000). The perception of risk
Explanation methods for $\varepsilon$ that increase

- objective risk comprehension
- subjective privacy understanding
- self-efficacy
  - confidence deciding
  - enough information
<table>
<thead>
<tr>
<th>Odds-Based (Text)</th>
<th>Odds-Based (Visual)</th>
<th>Example-Based</th>
</tr>
</thead>
</table>

Portable explanation methods for $\varepsilon$
If you do not participate, \( x \) out of 100 potential DP outputs will lead adversary \( A \) to believe you responded \( d_{true} \).

If you participate, \( y \) out of 100 potential DP outputs will lead adversary \( A \) to believe you responded \( d_{true} \).
If you do not participate, $x$ out of 100 potential DP outputs will lead adversary $A$ to believe you responded $d_{true}$.

If you participate, $y$ out of 100 potential DP outputs will lead adversary $A$ to believe you responded $d_{true}$. 
If you do not participate, $x$ out of 100 potential $DP$ outputs will lead adversary $A$ to believe you responded $d_{true}$.

If you participate, $y$ out of 100 potential $DP$ outputs will lead adversary $A$ to believe you responded $d_{true}$. 
Probabilities reflect immediate decisions

If you **do not participate**, \( x \) out of 100 potential **DP outputs** will lead adversary \( A \) to believe you responded \( d_{true} \).

If you **participate**, \( y \) out of 100 potential **DP outputs** will lead adversary \( A \) to believe you responded \( d_{true} \).
Framing probabilities as frequencies vs. percentages supports statistical reasoning & has been applied in privacy contexts.

If you do not participate, **x out of 100** potential \( DP \) outputs will lead adversary \( A \) to believe you responded \( d_{\text{true}} \).

If you participate, **y out of 100** potential \( DP \) outputs will lead adversary \( A \) to believe you responded \( d_{\text{true}} \).

Gigerenzer and Hoffrage (1995). How to improve Bayesian reasoning without instruction: Frequency formats
Slovic (2000). The perception of risk
Kaptchuk, Goldstein, Hargittai, Hofman, and Redmiles (2020). How good is good enough for COVID19 apps? ...
Franzen, Nuñez von Voigt, Sörries, Tschorsch, Müller-Birn (2022). “Am I private and if so, how many?” ...
If you **do not participate**, $x$ out of 100 potential DP outputs will lead adversary $A$ to believe you responded $d_{\text{true}}$.

If you **participate**, $y$ out of 100 potential DP outputs will lead adversary $A$ to believe you responded $d_{\text{true}}$.

Icon arrays assume $x = 39$ and $y = 61$ for illustration purposes.

If you **do not participate**, below are examples of potential DP outputs adversary $A$ might receive:

<table>
<thead>
<tr>
<th>Potential Output</th>
<th>$x_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Output</td>
<td>$x_2$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$x_3$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$x_4$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$x_5$</td>
</tr>
</tbody>
</table>

If you **participate**, below are examples of potential DP outputs adversary $A$ might receive:

<table>
<thead>
<tr>
<th>Potential Output</th>
<th>$y_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Output</td>
<td>$y_2$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$y_3$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$y_4$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$y_5$</td>
</tr>
</tbody>
</table>
If you **do not participate**, below are examples of potential DP outputs adversary $A$ might receive:

<table>
<thead>
<tr>
<th>Potential Output</th>
<th>$x_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Output</td>
<td>$x_2$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$x_3$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$x_4$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$x_5$</td>
</tr>
</tbody>
</table>

Are these similar to...

If you **participate**, below are examples of potential DP outputs adversary $A$ might receive:

<table>
<thead>
<tr>
<th>Potential Output</th>
<th>$y_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Output</td>
<td>$y_2$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$y_3$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$y_4$</td>
</tr>
<tr>
<td>Potential Output</td>
<td>$y_5$</td>
</tr>
</tbody>
</table>

these?
Evaluation Criteria

- objective risk comprehension
- subjective privacy understanding
- self-efficacy
  - confidence deciding
  - enough information
Evaluation Criteria

- objective risk comprehension
- subjective privacy understanding
- self-efficacy
  - confidence deciding
  - enough information
- willingness to share data
Between-subjects vignette survey study \((n = 963)\)

Workplace scenario with a data-sharing decision

Hainmueller, Hangartner, Yamamoto (2015). Validating vignette and conjoint survey experiments against real-world behavior
Between-subjects **vignette survey study** (n = 963)

Workplace scenario with a **data-sharing decision**

*mandatory vs. optional*
Scenario
Explanation
Sharing Decision
Evaluation Questions
Num. Skills & Demographics

Survey Flow

$\varepsilon \in \{0.1, 0.5, 2, 4\}$

Odds-Based (Visual)
Odds-Based (Text)
Example-Based

Example-Based

Odds-Based (Text)

Odds-Based (Visual)

$\varepsilon \in \{0.1, 0.5, 2, 4\}$
Xiong, Wang, Li, Jha (2020). Towards effective differential privacy communication for users’ data sharing decision and comprehension.
Would you share your data?
Yes/No

Briefly explain your reasoning.

Survey Flow

Scenario  →  Explanation  →  Sharing Decision  →  Evaluation Questions  →  Num. Skills & Demographics
Objective risk comprehension T/F

Subjective privacy understanding Likert-style

Self-efficacy Likert-style
Results

Compared to our Example-Based Method, Odds-Based Text and Odds-Based Visual improved:

Objective risk comprehension \((O.R. = 4.7; 7.6)\)

Subjective privacy understanding \((O.R. = 1.7; 1.5)\)

Self-efficacy (enough info) \((O.R. = 1.7; 1.6)\)
Results

Over 2x as likely to answer an additional objective risk comprehension question correctly with Odds-Based Visual vs. Deterministic Control

Negative effect of our Example-Based Method (O.R. = 0.32)

No significant effect of Odds-Based Text
Results

Compared to the Xiong et al. Control, Odds-Based Text and Odds-Based Visual improved self-efficacy (enough info) \((O.R. = 1.8; 1.7)\)

No significant effect of our Example-Based Method
Results: Willingness to Share Data

Compared to the Xiong et al. Control,

over 2x, nearly 2x, over 4x as likely to share data when given Odds-Based Text,
Odds-Based Visual,
& Example-Based respectively
Results: Willingness to Share Data

Compared to the Xiong et al. Control,

over 2x, nearly 2x, over 4x as likely to share data when given Odds-Based Text, Odds-Based Visual, & Example-Based respectively

Decreased willingness to share as privacy strength decreases
Takeaways

→ Odds-based methods are promising for explaining $\varepsilon$ to end users
→ Explanations should include $\varepsilon$ information, since it supports self-efficacy
→ People’s willingness to share data is sensitive to changes in $\varepsilon$
→ Explanation methods can support auditing & public deliberation over differential privacy deployments
Takeaways

→ Odds-based methods are promising for explaining $\varepsilon$ to end users
→ Explanations should include $\varepsilon$ information, since it supports self-efficacy
→ People’s willingness to share data is sensitive to changes in $\varepsilon$
→ Explanation methods can support auditing & public deliberation over differential privacy deployments

Future

→ Explain impacts of $\varepsilon$ on accuracy & utility
→ Port our methods into real-world settings & create developer tools
→ Odds-based methods are promising for explaining $\varepsilon$ to end users
→ Explanations should include $\varepsilon$ information, since it supports self-efficacy
→ People’s willingness to share data is sensitive to changes in $\varepsilon$
→ Explanation methods can support auditing & public deliberation over differential privacy deployments

**Future**

→ Explain impacts of $\varepsilon$ on accuracy & utility

→ Port our methods into real-world settings & create developer tools

---

**Thank you!**

**Priyanka Nanayakkara** (priyankan@u.northwestern.edu | @priyakalot | @priyakalot@hci.social)

Coauthors: Mary Anne Smart, Rachel Cummings, Gabriel Kaptchuk, Elissa M. Redmiles