Differential Privacy

Matt Kusner

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

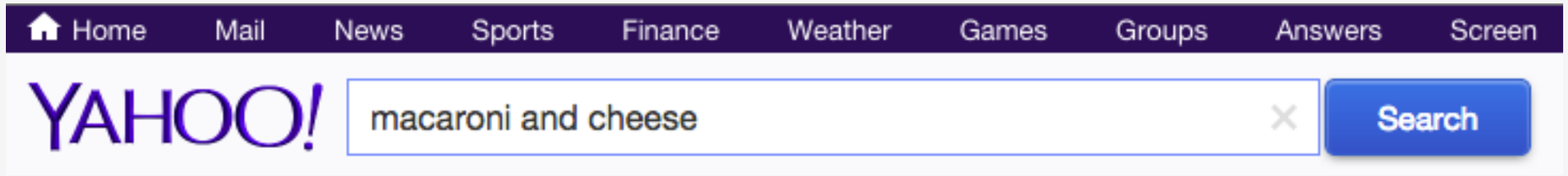
Privacy Mechanisms

- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

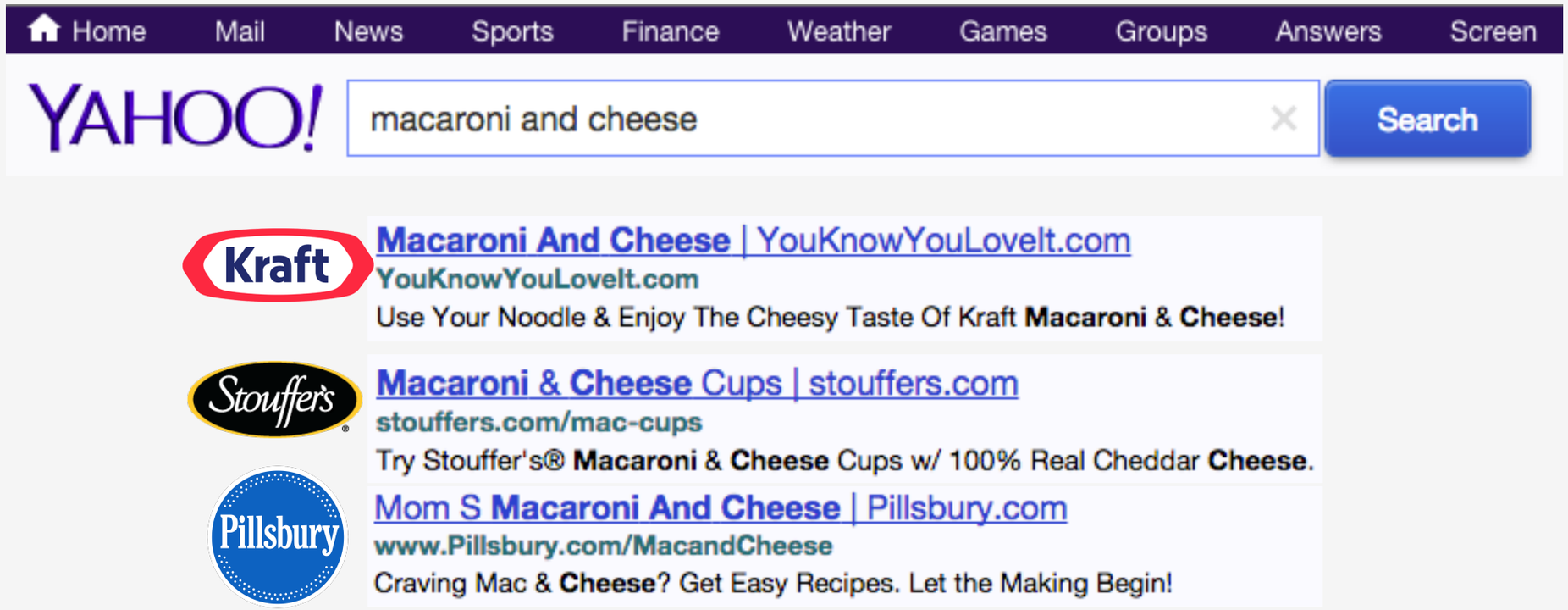
Just a Web Search?

somePerson@yahoo.com **searches**



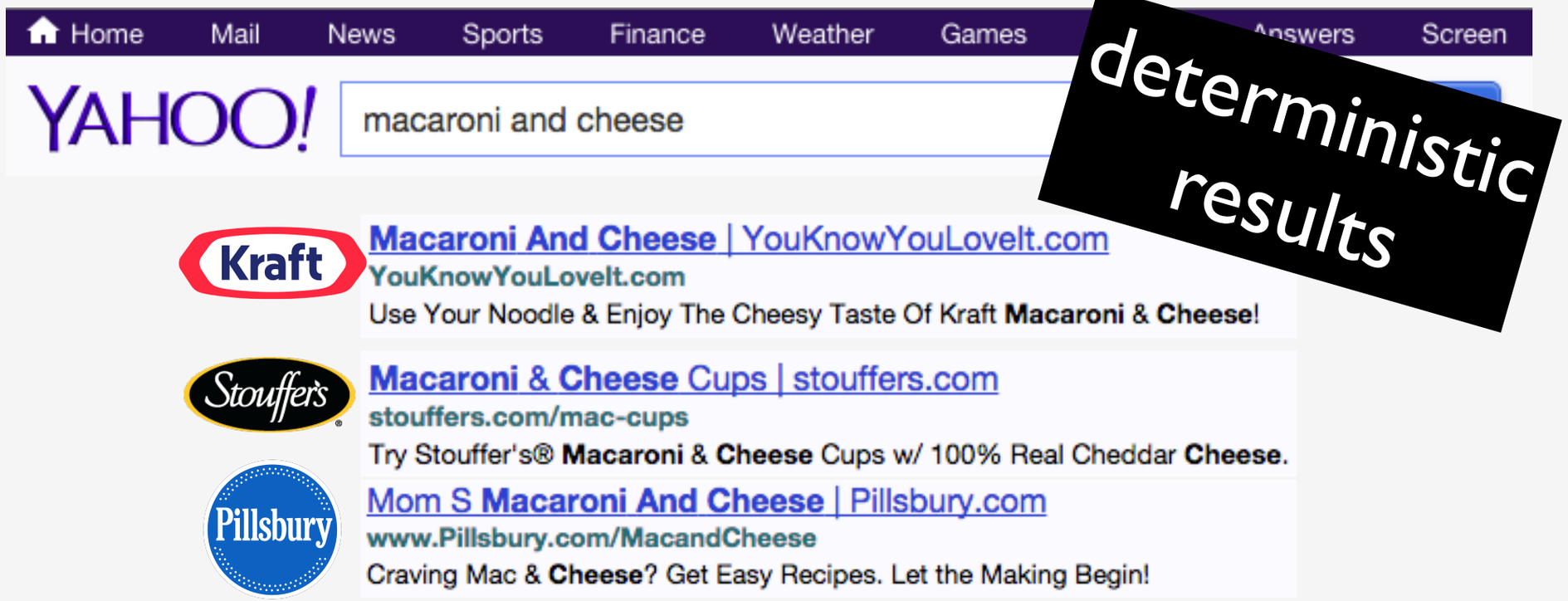
Just a Web Search?

somePerson@yahoo.com **searches**



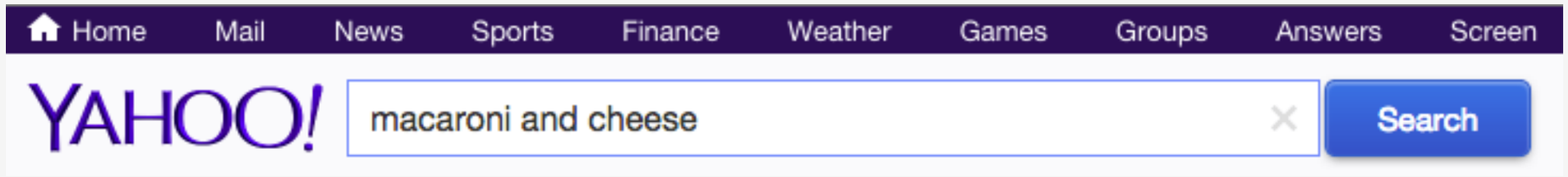
Just a Web Search?

somePerson@yahoo.com **searches**



Just a Web Search?

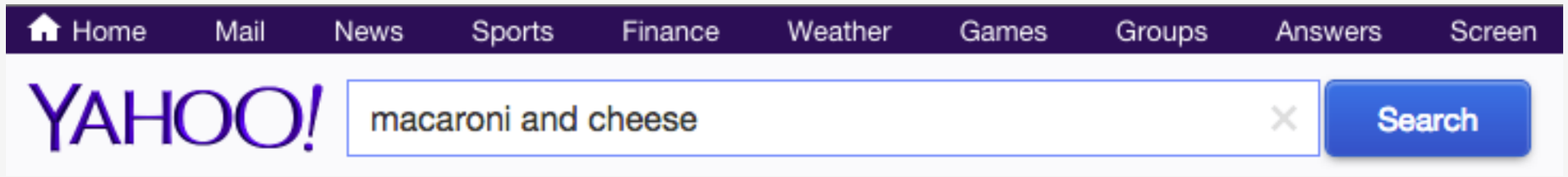
somePerson@yahoo.com **searches**



Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Just a Web Search?

somePerson@yahoo.com **searches**

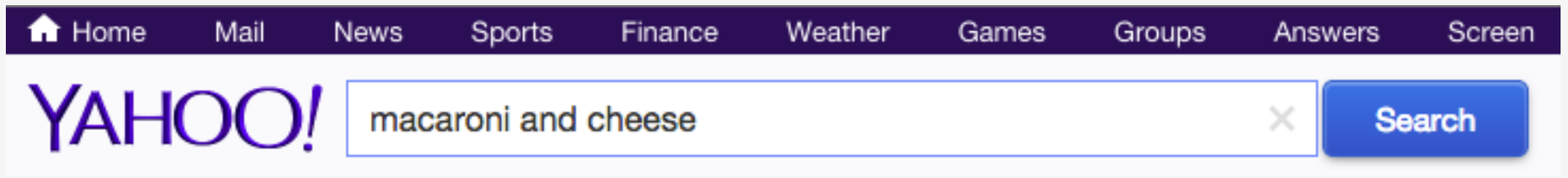


Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

somePerson@yahoo.com **clicks!**

Just a Web Search?

somePerson@yahoo.com **searches**



Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

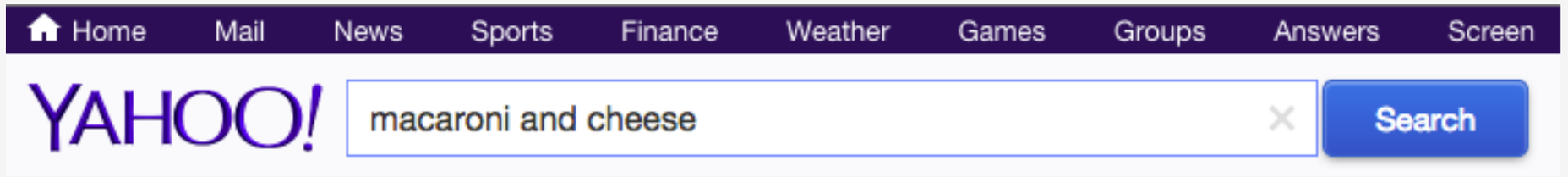
somePerson@yahoo.com **clicks!**

YAHOO!

update ad-recommendation algorithm using profile data on somePerson@yahoo.com

Just a Web Search?

somePerson@yahoo.com **searches**



Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

somePerson@yahoo.com **clicks!**

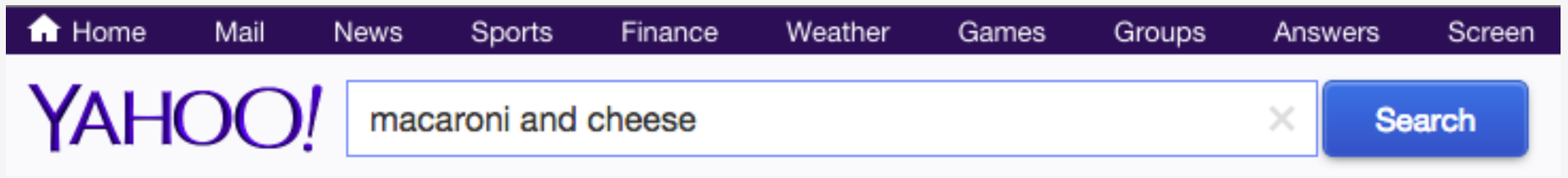
YAHOO!

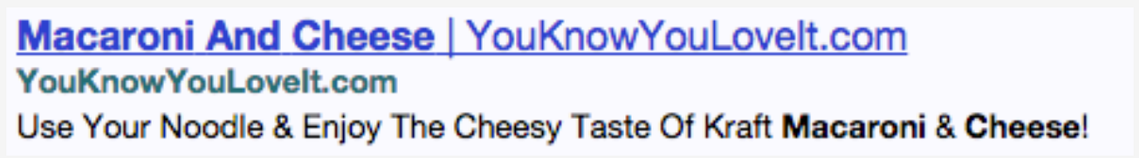
somePerson@yahoo.com

age: 55 | gender: M | SSN: 83...1

Just a Web Search?

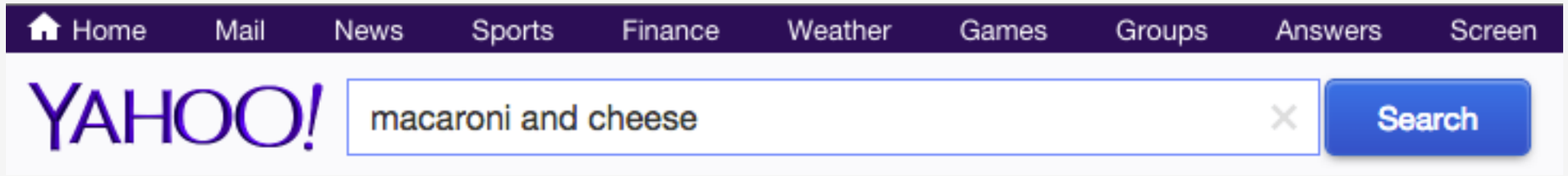
somePerson@yahoo.com **searches**



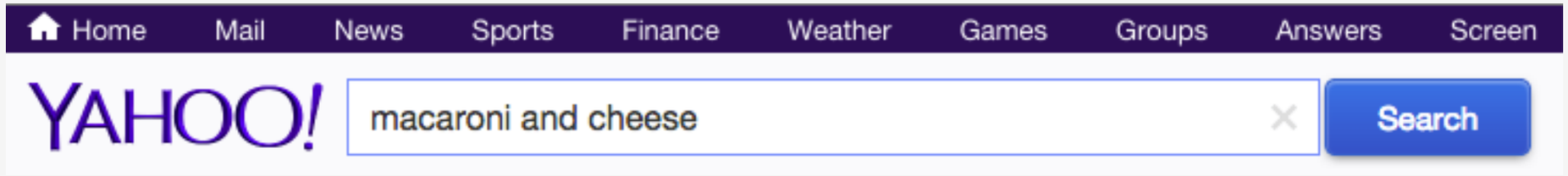


somePerson@yahoo.com **clicks!**

The Attack

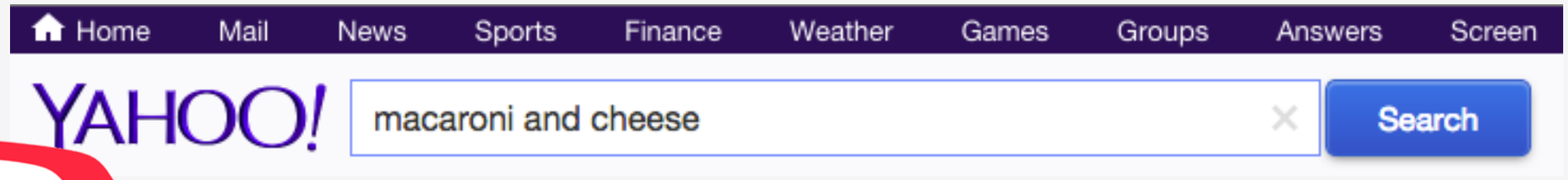

Home
Mail
News
Sports
Finance
Weather
Games
Groups
Answers
Screen
YAHOO!
macaroni and cheese
Search

The Attack



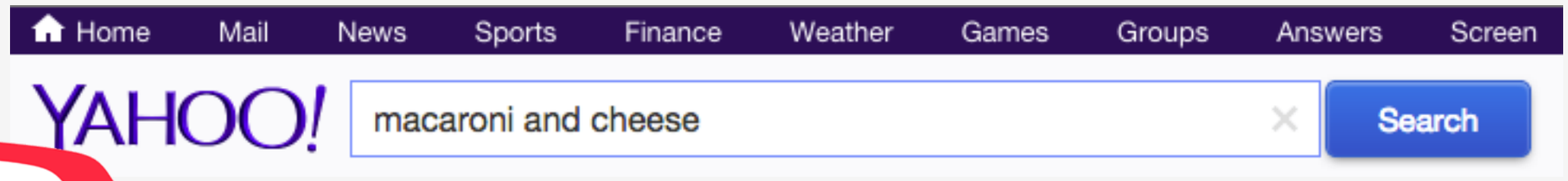
Is `somePerson@yahoo.com` >49?

The Attack



Is `somePerson@yahoo.com` >49?

The Attack



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

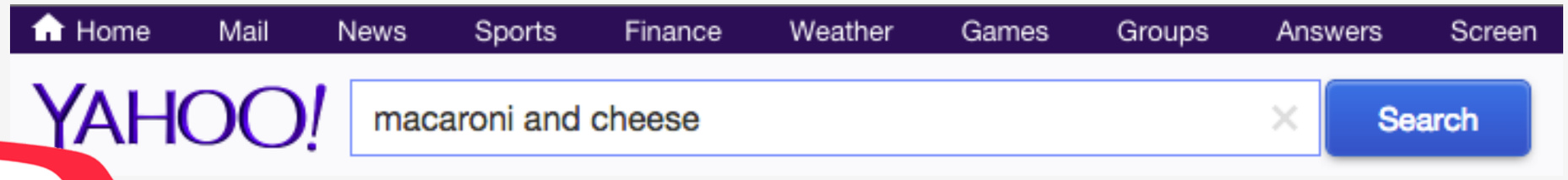
age: 50

account 2

`young@yahoo.com`

age: 49

The Attack



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

age: 50

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Macaroni & **Cheese** Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

account 2

`young@yahoo.com`

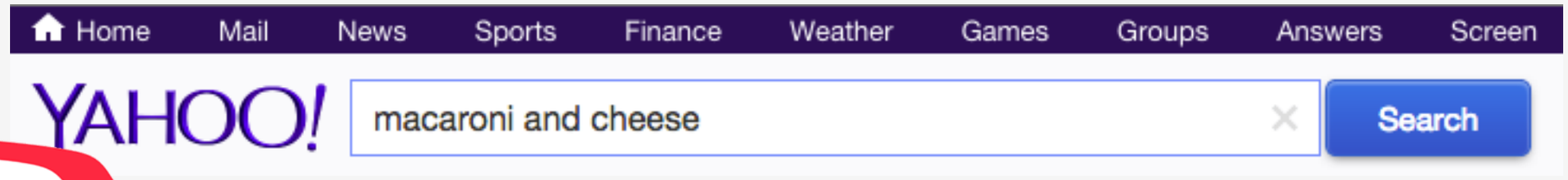
age: 49

Macaroni & **Cheese** Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

The Attack



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

age: 50

account 2

`young@yahoo.com`

age: 49

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

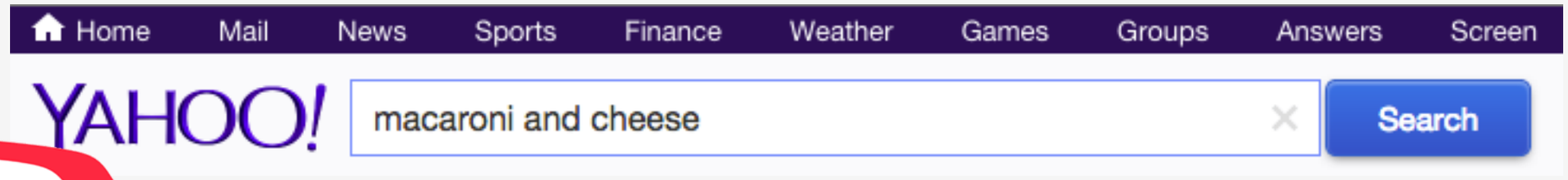
Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

The Attack



Is `somePerson@yahoo.com` >49?

account 1	account 2
`old@yahoo.com` age: 50	`young@yahoo.com` age: 49

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

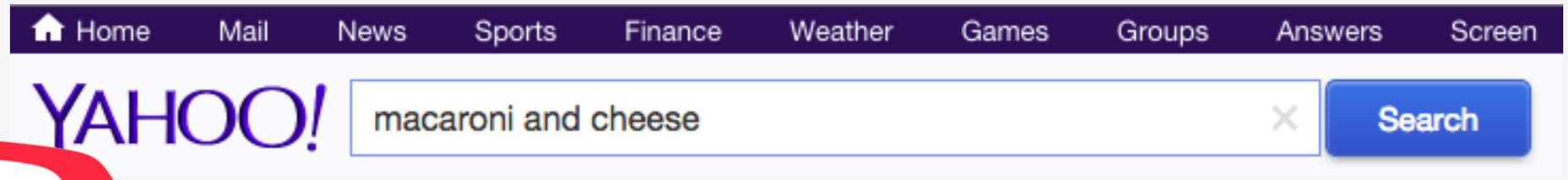
Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

The Attack



Is `somePerson@yahoo.com` >49?

Yes!

Data Leaks

Aol.

private search logs

650,000 users

NETFLIX

private movie ratings

33 million users

Data Leaks

Aol.

private search logs

650,000 users

NETFLIX

private movie ratings

33 million users

How to keep data private?

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

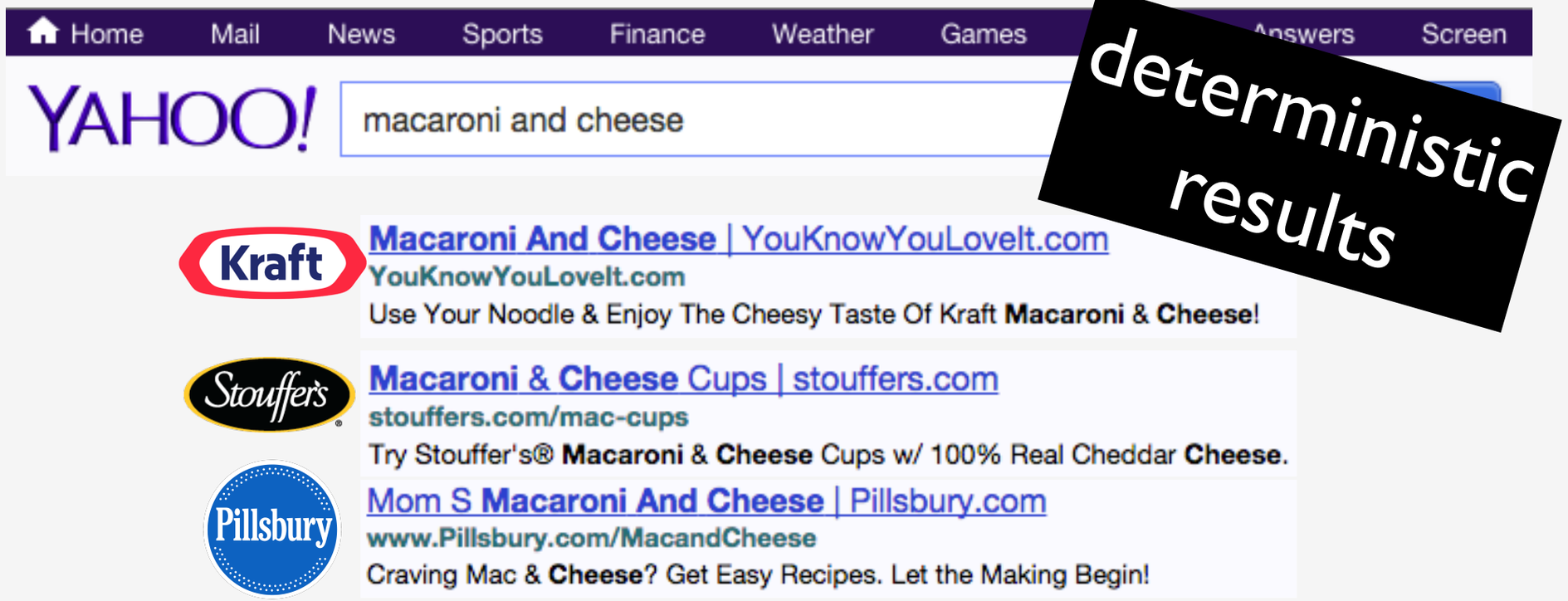
- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

Privacy via Randomization

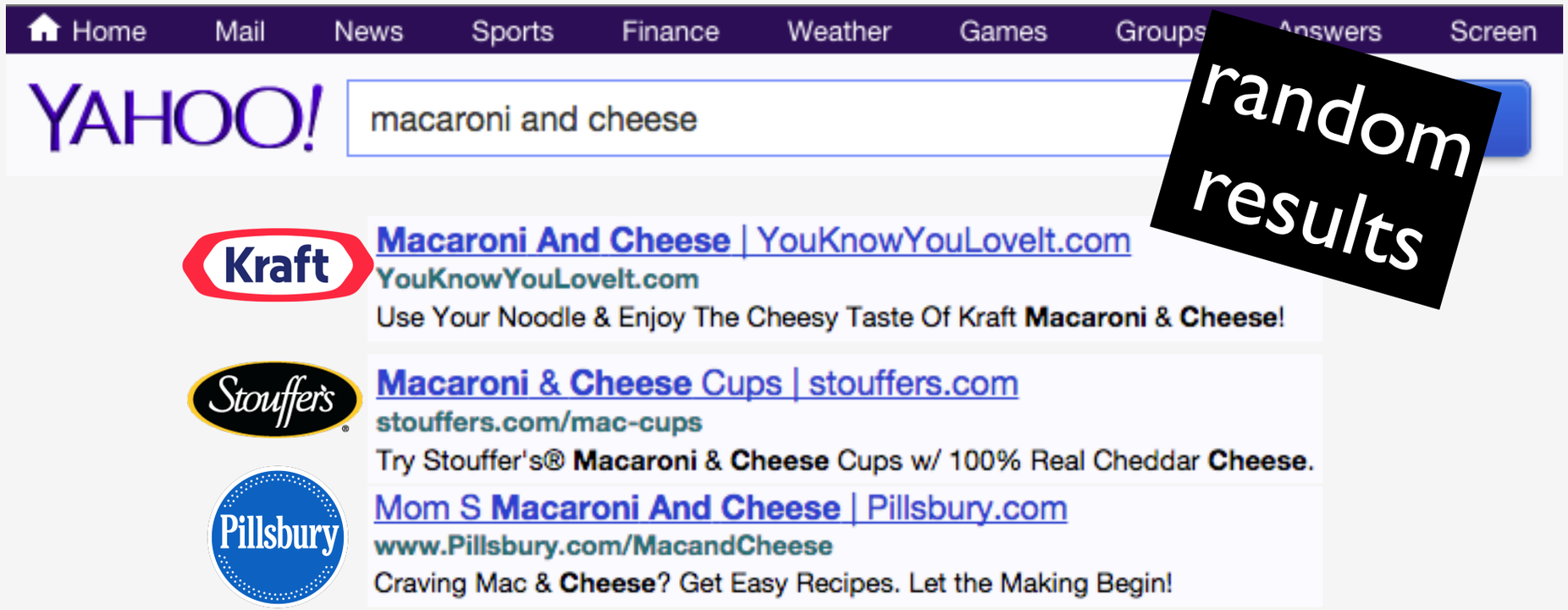
Privacy via Randomization

somePerson@yahoo.com **searches**



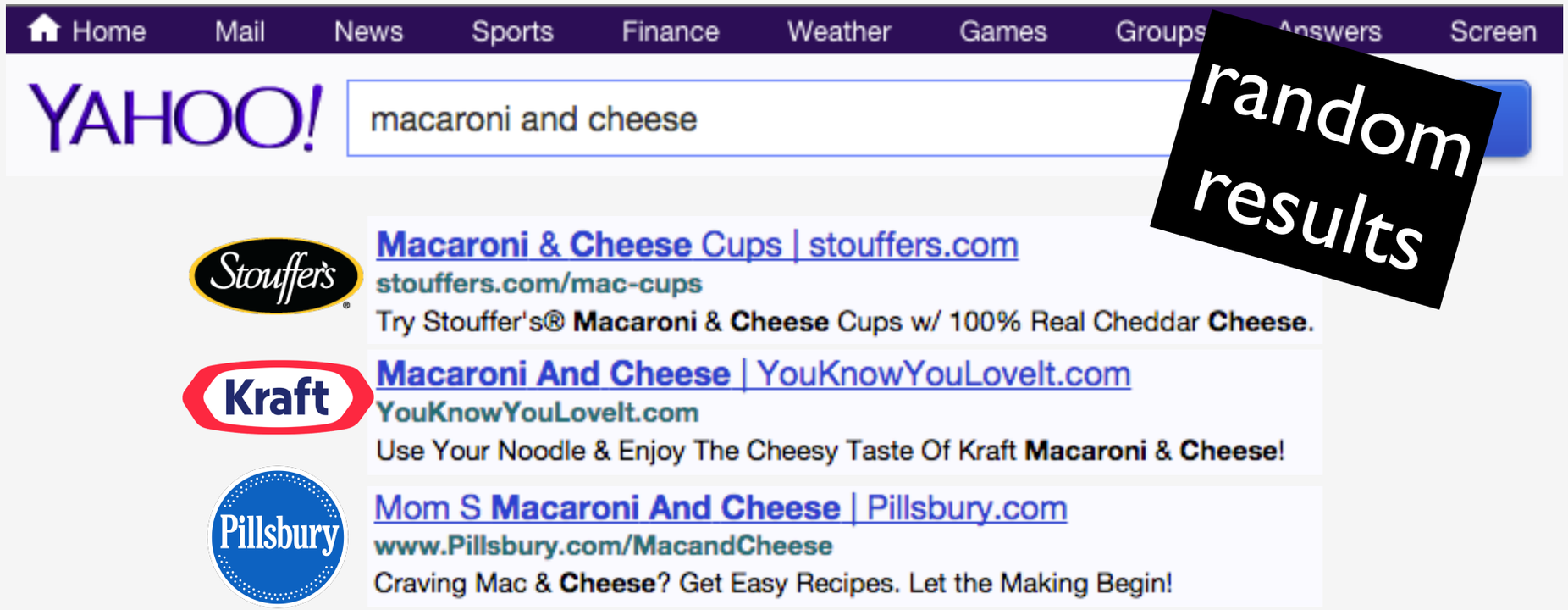
Privacy via Randomization

somePerson@yahoo.com **searches**



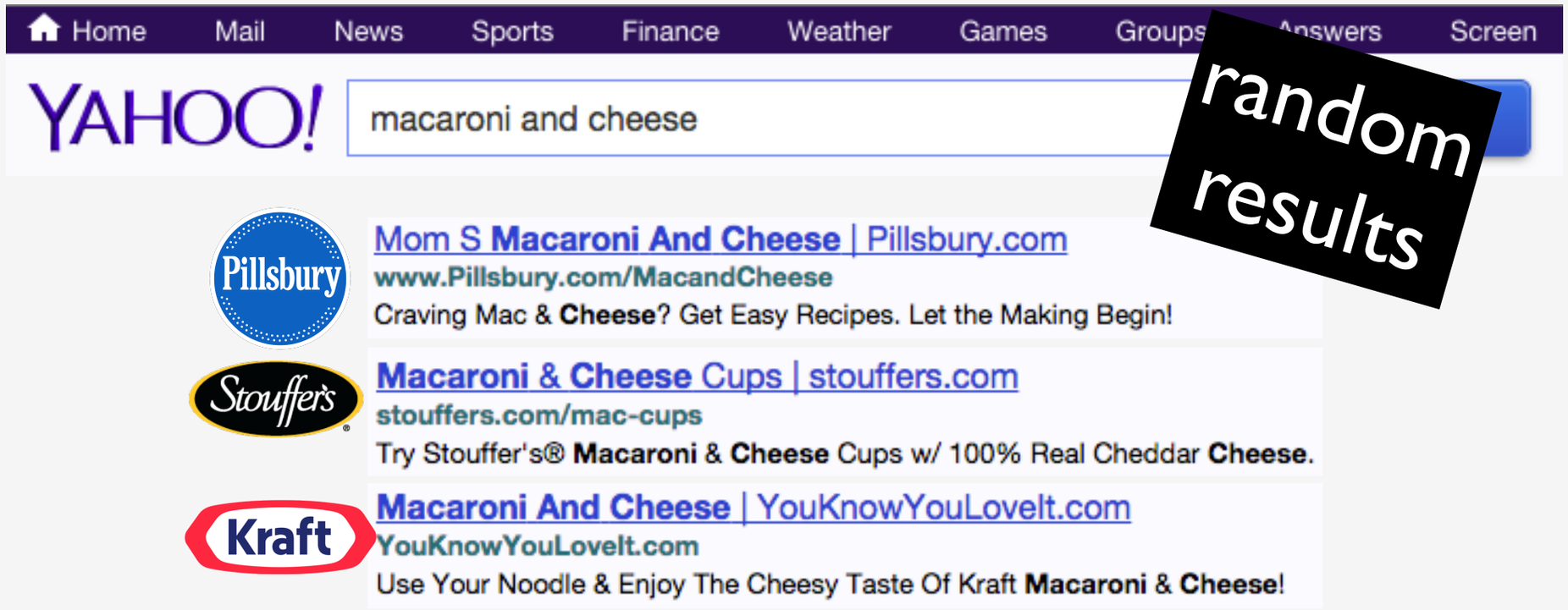
Privacy via Randomization

somePerson@yahoo.com **searches**



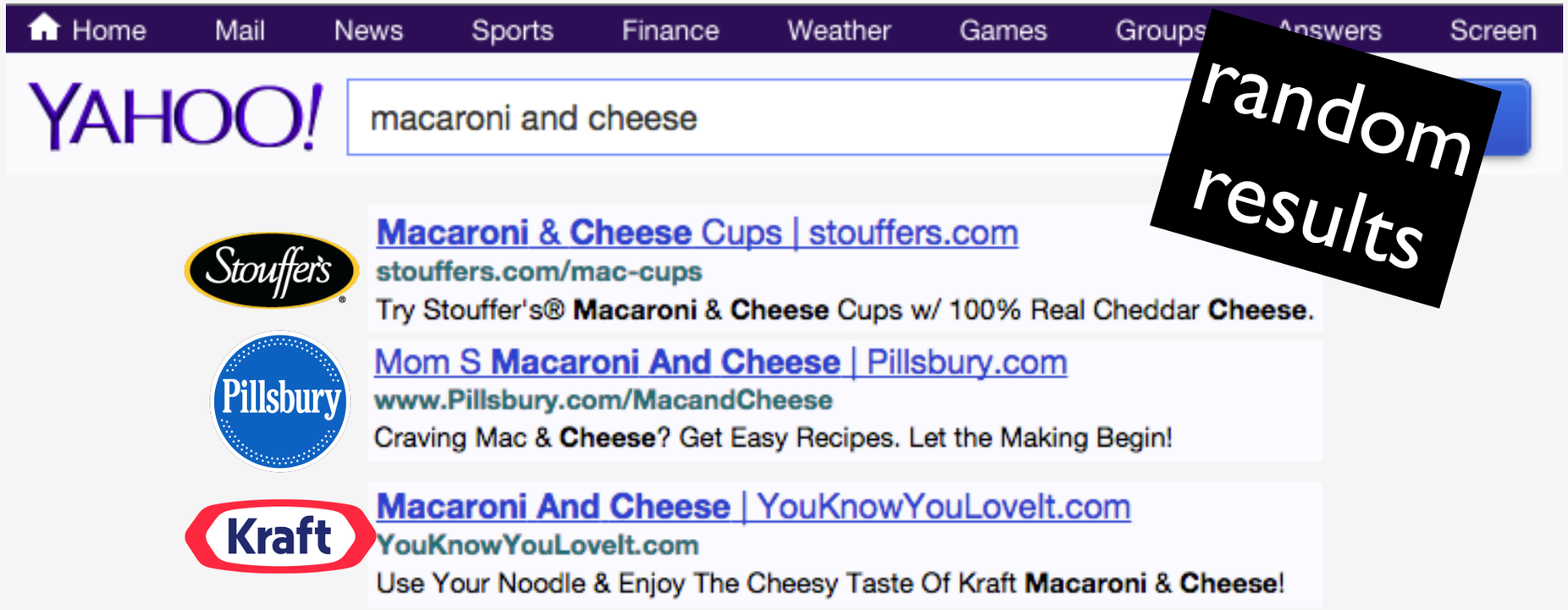
Privacy via Randomization

somePerson@yahoo.com **searches**

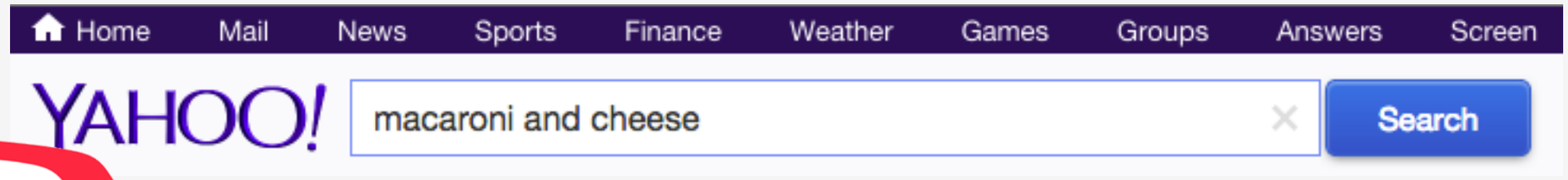


Privacy via Randomization

somePerson@yahoo.com **searches**



Privacy via Randomization



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

age: 50

account 2

`young@yahoo.com`

age: 49

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

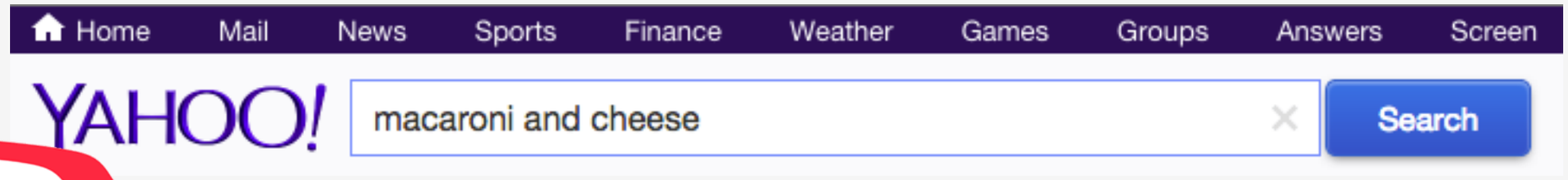
Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
uKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Macaroni & Cheese Cups | stouffers.com
touffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
ww.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Privacy via Randomization



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

age: 50

account 2

`young@yahoo.com`

age: 49

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

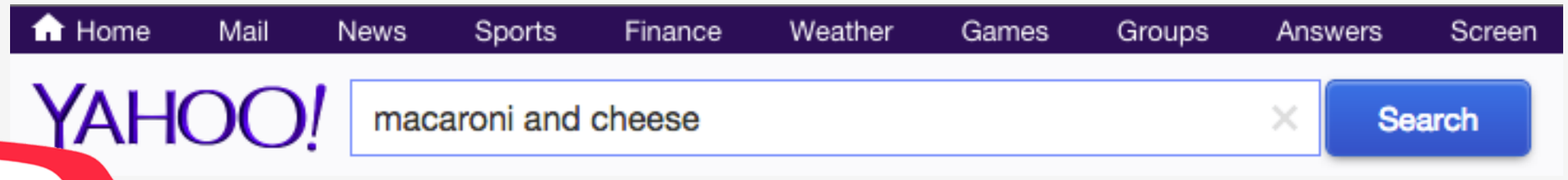
Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Privacy via Randomization



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

age: 50

account 2

`young@yahoo.com`

age: 49

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

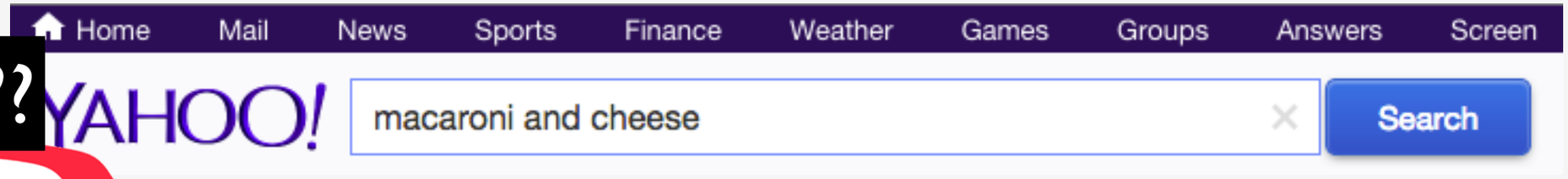
Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni & Cheese Cups | stouffers.com
touffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
uKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Privacy via Randomization



Is `somePerson@yahoo.com` >49?

account 1

`old@yahoo.com`

age: 50

account 2

`young@yahoo.com`

age: 49

Macaroni And Cheese | YouKnowYouLoveIt.com
YouKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Macaroni & Cheese Cups | stouffers.com
stouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
www.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni & Cheese Cups | stouffers.com
ouffers.com/mac-cups
Try Stouffer's® **Macaroni** & **Cheese** Cups w/ 100% Real Cheddar **Cheese**.

Mom S **Macaroni And Cheese** | Pillsbury.com
ww.Pillsbury.com/MacandCheese
Craving Mac & **Cheese**? Get Easy Recipes. Let the Making Begin!

Macaroni And Cheese | YouKnowYouLoveIt.com
uKnowYouLoveIt.com
Use Your Noodle & Enjoy The Cheesy Taste Of Kraft **Macaroni** & **Cheese**!

Privacy via Randomization

Implies a **trade-off**

Privacy  Accuracy

increased randomness

decreased randomness

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

Differential Privacy [Dwork et al., 2006]

Differential Privacy [Dwork et al., 2006]

A formalization of "privacy through randomness"

Differential Privacy

[Dwork et al., 2006]

A formalization of "privacy through randomness"

data

age: 20	gender: M	SSN: 42...2
age: 91	gender: M	SSN: 21...0
age: 82	gender: F	SSN: 46...7
age: 39	gender: F	SSN: 91...3
⋮	⋮	⋮

Differential Privacy

[Dwork et al., 2006]

A formalization of "privacy through randomness"

algorithm

$\mathcal{A}$

data

age: 20	gender: M	SSN: 42...2
age: 91	gender: M	SSN: 21...0
age: 82	gender: F	SSN: 46...7
age: 39	gender: F	SSN: 91...3
•	•	•
•	•	•
•	•	•

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data output

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \vdots & \vdots & \vdots \\ \hline \end{array}\right) = \mathbf{x}$$

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data $\mathcal{D}$ output

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \vdots & \vdots & \vdots \\ \hline \end{array}\right) = \mathbf{x}$$

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \vdots & \vdots & \vdots \\ \hline \text{age: 55} & \text{gender: M} & \text{SSN: 83...1} \\ \hline \end{array}\right)$$

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm $\mathcal{A}$ data $\mathcal{D}'$

age: 20	gender: M	SSN: 42...2
age: 91	gender: M	SSN: 21...0
age: 82	gender: F	SSN: 46...7
age: 39	gender: F	SSN: 91...3
⋮	⋮	⋮
age: 55	gender: M	SSN: 83...1

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data $\mathcal{D}'$ output

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \vdots & \vdots & \vdots \\ \hline \text{age: 55} & \text{gender: M} & \text{SSN: 83...1} \\ \hline \end{array}\right) = \mathbf{x}'$$

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data $\mathcal{D}'$ output

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \vdots & \vdots & \vdots \\ \hline \text{age: 55} & \text{gender: M} & \text{SSN: 83...1} \\ \hline \end{array}\right) = \mathbf{x}'$$

informally: $\mathbf{x} \approx \mathbf{x}'$

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data $\mathcal{D}'$ output

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \\ \hline \text{age: 55} & \text{gender: M} & \text{SSN: 83...1} \\ \hline \end{array}\right) = \mathbf{x}'$$

Definition. *A randomized algorithm $\mathcal{A}$ is* ϵ***-differentially private*** *if for all $\mathbf{x} \subseteq Range(\mathcal{A})$ and for neighboring datasets $\mathcal{D}, \mathcal{D}'$ we have that,*

$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

[Dwork et al., 2006]

Differential Privacy

A formalization of "privacy through randomness"

algorithm data $\mathcal{D}'$ output

$$\mathcal{A}\left(\begin{array}{|c|c|c|}\hline \text{age: 20} & \text{gender: M} & \text{SSN: 42...2} \\ \hline \text{age: 91} & \text{gender: M} & \text{SSN: 21...0} \\ \hline \text{age: 82} & \text{gender: F} & \text{SSN: 46...7} \\ \hline \text{age: 39} & \text{gender: F} & \text{SSN: 91...3} \\ \hline \vdots & \vdots & \vdots \\ \hline \text{age: 55} & \text{gender: M} & \text{SSN: 83...1} \\ \hline \end{array}\right) = \mathbf{x}'$$

Definition. *A randomized algorithm $\mathcal{A}$ is* ϵ***-differentially private*** *if for all $\mathbf{x} \subseteq Range(\mathcal{A})$ and for neighboring datasets $\mathcal{D}, \mathcal{D}'$ we have that,*

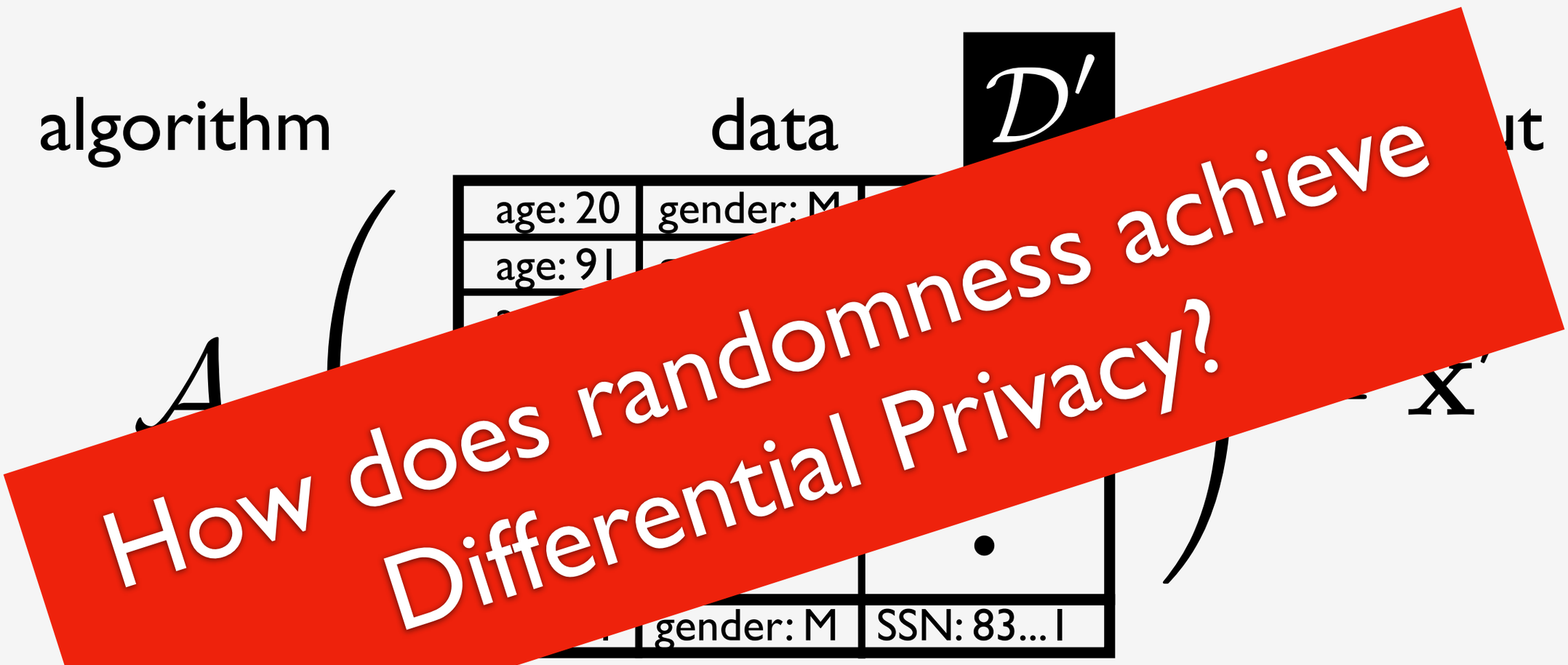
$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

$\mathcal{D}, \mathcal{D}'$ differ in one row

Differential Privacy

[Dwork et al., 2006]

A formalization of "privacy through randomness"



How does randomness achieve Differential Privacy?

De *randomized algorithm* $\mathcal{A}$ *is* ϵ***-differentially private*** *if for all* $\mathbf{x} \subseteq$ *Range*$(\mathcal{A})$ *and for neighboring datasets* $\mathcal{D}, \mathcal{D}'$ *we have that,*

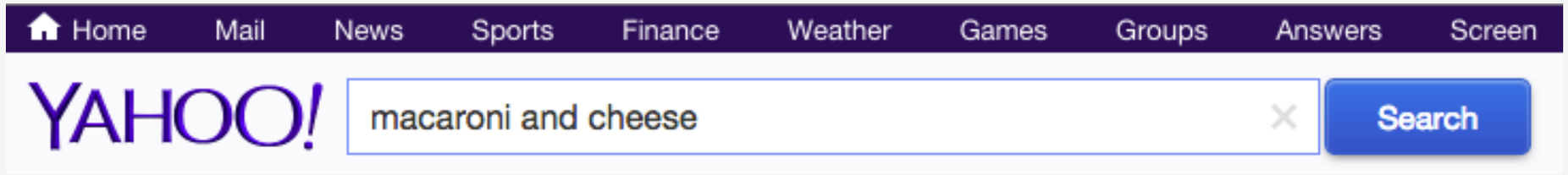
$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

$\mathcal{D}, \mathcal{D}'$ differ in one row

Randomized Response

[Warner, 1965]

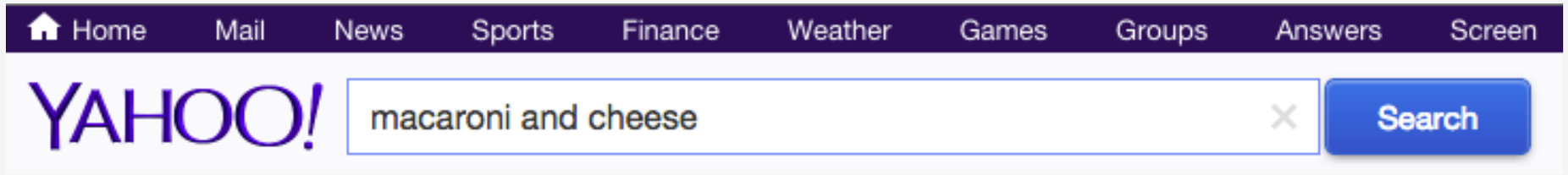
somePerson@yahoo.com **searches**



Randomized Response

[Warner, 1965]

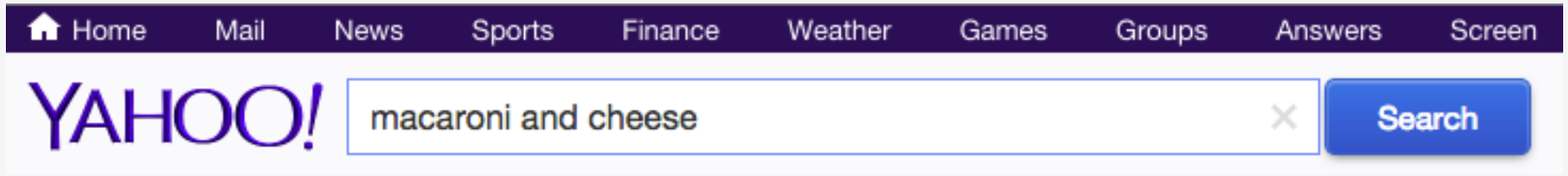
somePerson@yahoo.com **searches**



Randomized Response

[Warner, 1965]

somePerson@yahoo.com **searches**



tails

true prediction

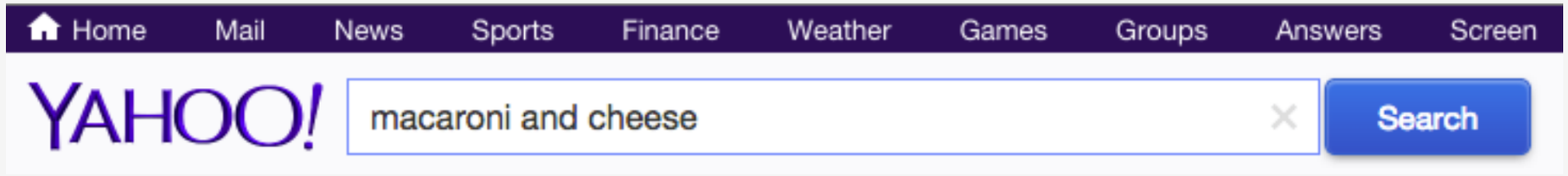
old@yahoo.com

age: 50	gender: M	SSN: 83...1

Randomized Response

[Warner, 1965]

somePerson@yahoo.com **searches**



tails 

heads 

true prediction

old@yahoo.com

age: 50	gender: M	SSN: 83...1

Kraft

randomised prediction

tails 

Kraft

heads 

Stouffer's

Randomized Response [Warner, 1965]

Claim:

Randomized response is (log 3)-differentially private

Randomized Response [Warner, 1965]

Claim:

Randomized response is (log 3)-differentially private

Proof:

Randomized Response [Warner, 1965]

Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]} \leq e^{\epsilon}$$

$\mathcal{D}, \mathcal{D}'$ differ in one row

Randomized Response [Warner, 1965]

Claim:

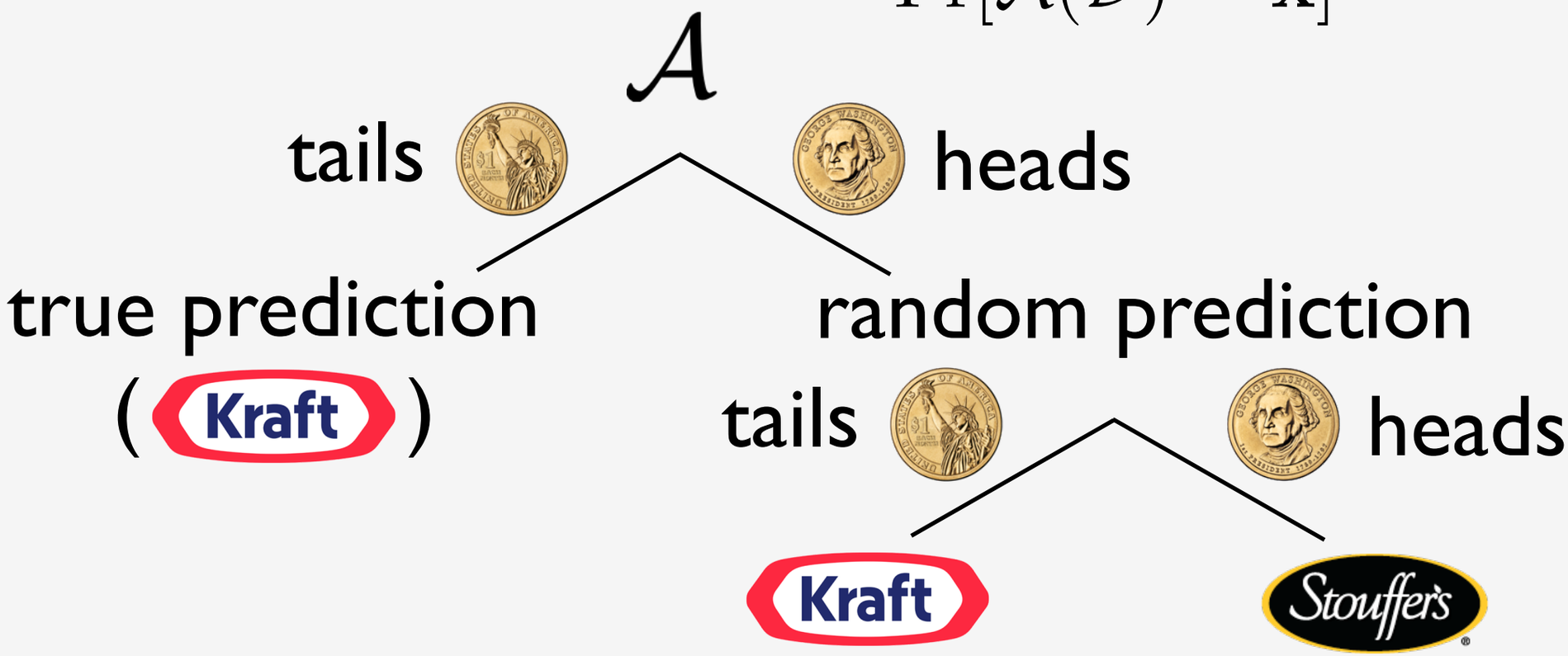
Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]} \leq e^{\epsilon}$$

$\mathcal{D}, \mathcal{D}'$ differ in one row



Randomized Response [Warner, 1965]

Claim:

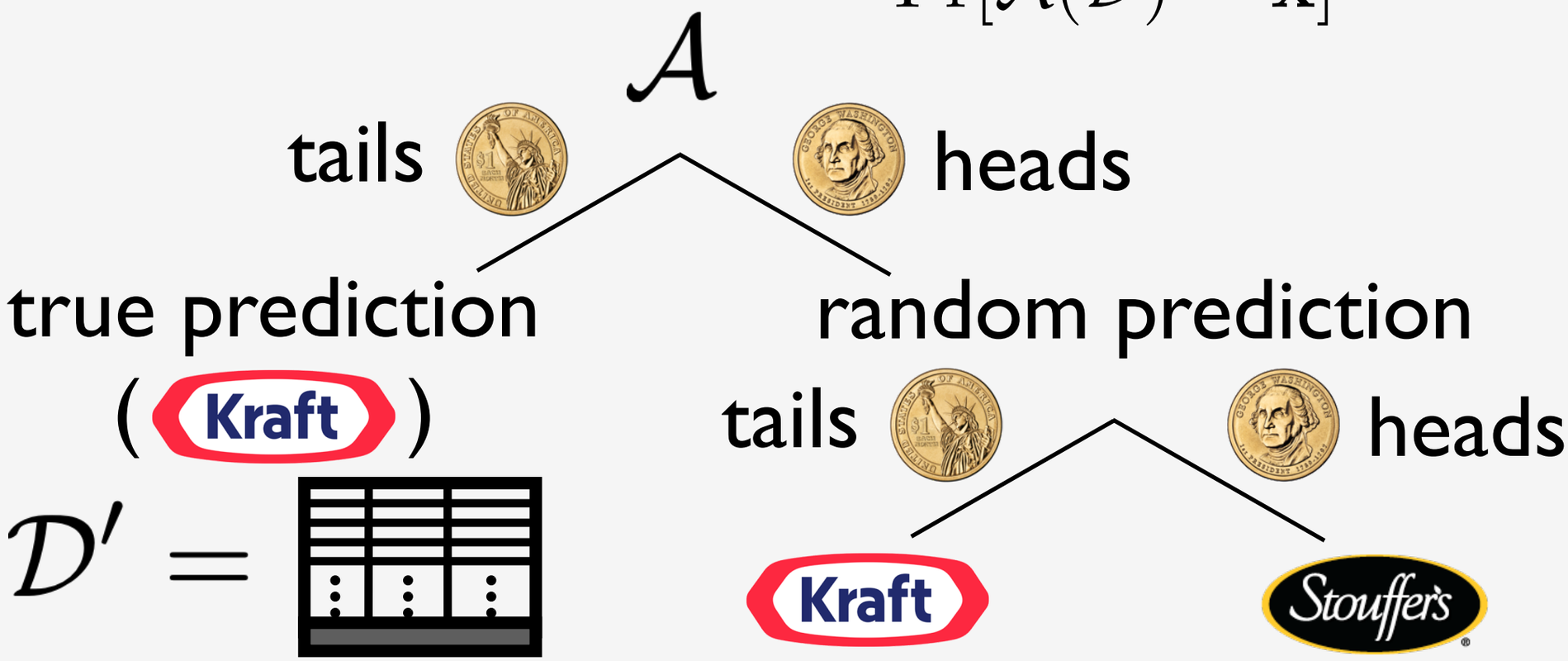
Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]} \leq e^{\epsilon}$$

$\mathcal{D}, \mathcal{D}'$ differ in one row



Randomized Response

[Warner, 1965]

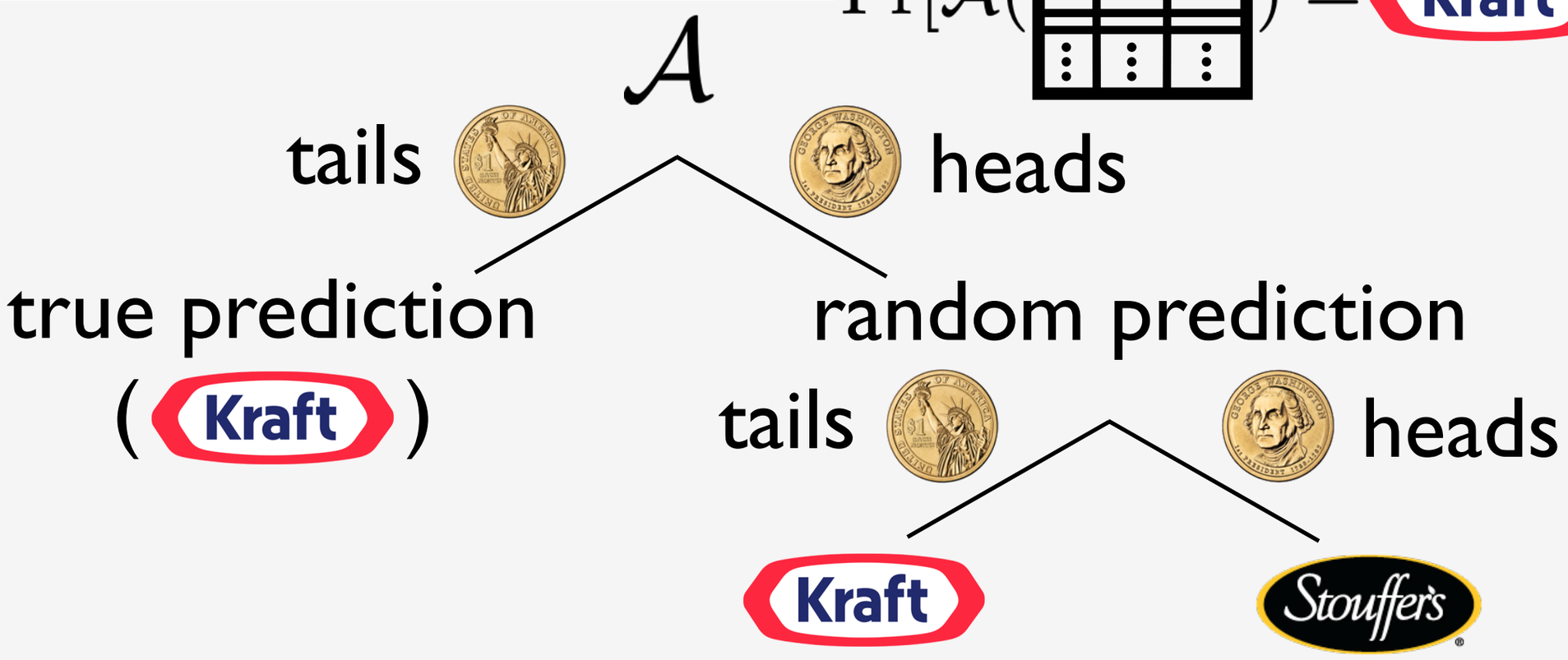
Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\text{[table]}) = \text{Kraft}]}{\Pr[\mathcal{A}(\text{[table]}) = \text{Kraft}]} \leq e^{\epsilon}$$



Randomized Response [Warner, 1965]

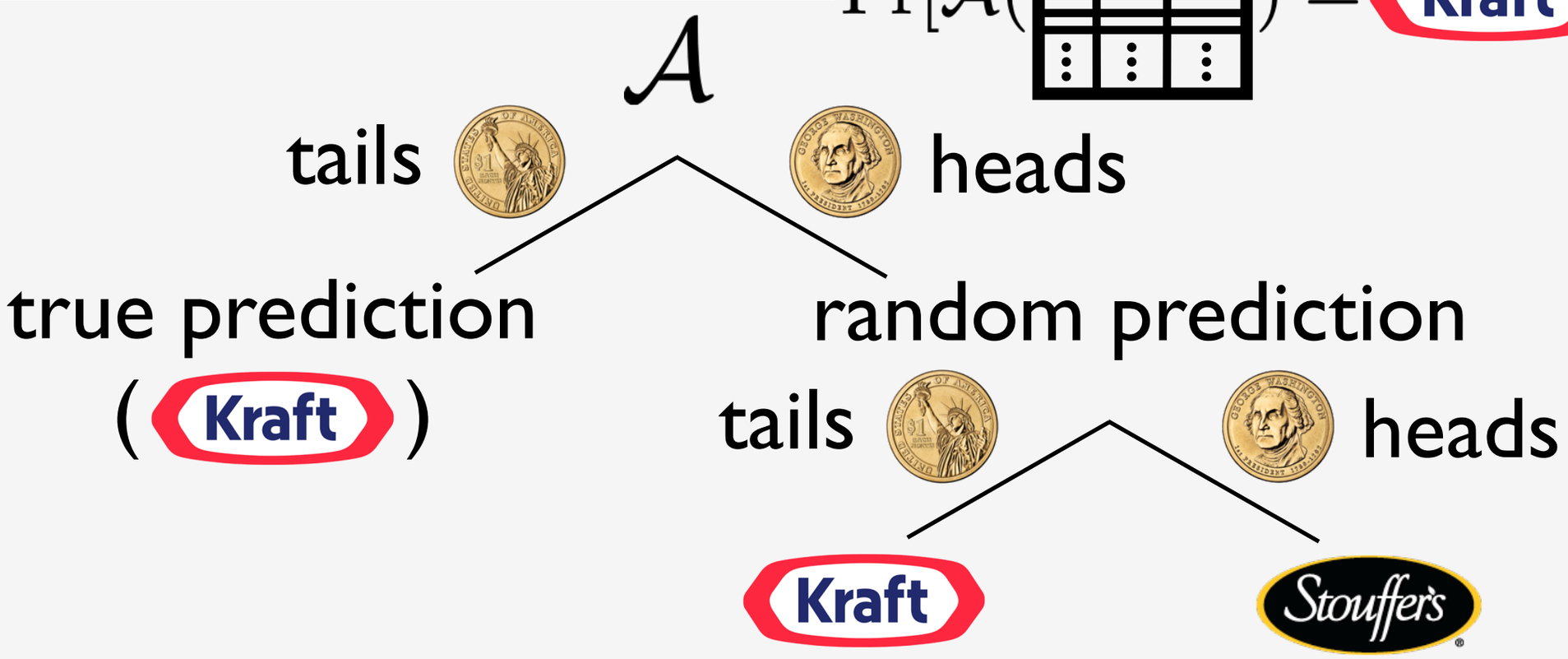
Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\text{[table]}) = \text{Kraft}]}{\Pr[\mathcal{A}(\text{[table]}) = \text{Kraft}]} \leq e^{\epsilon}$$



Randomized Response [Warner, 1965]

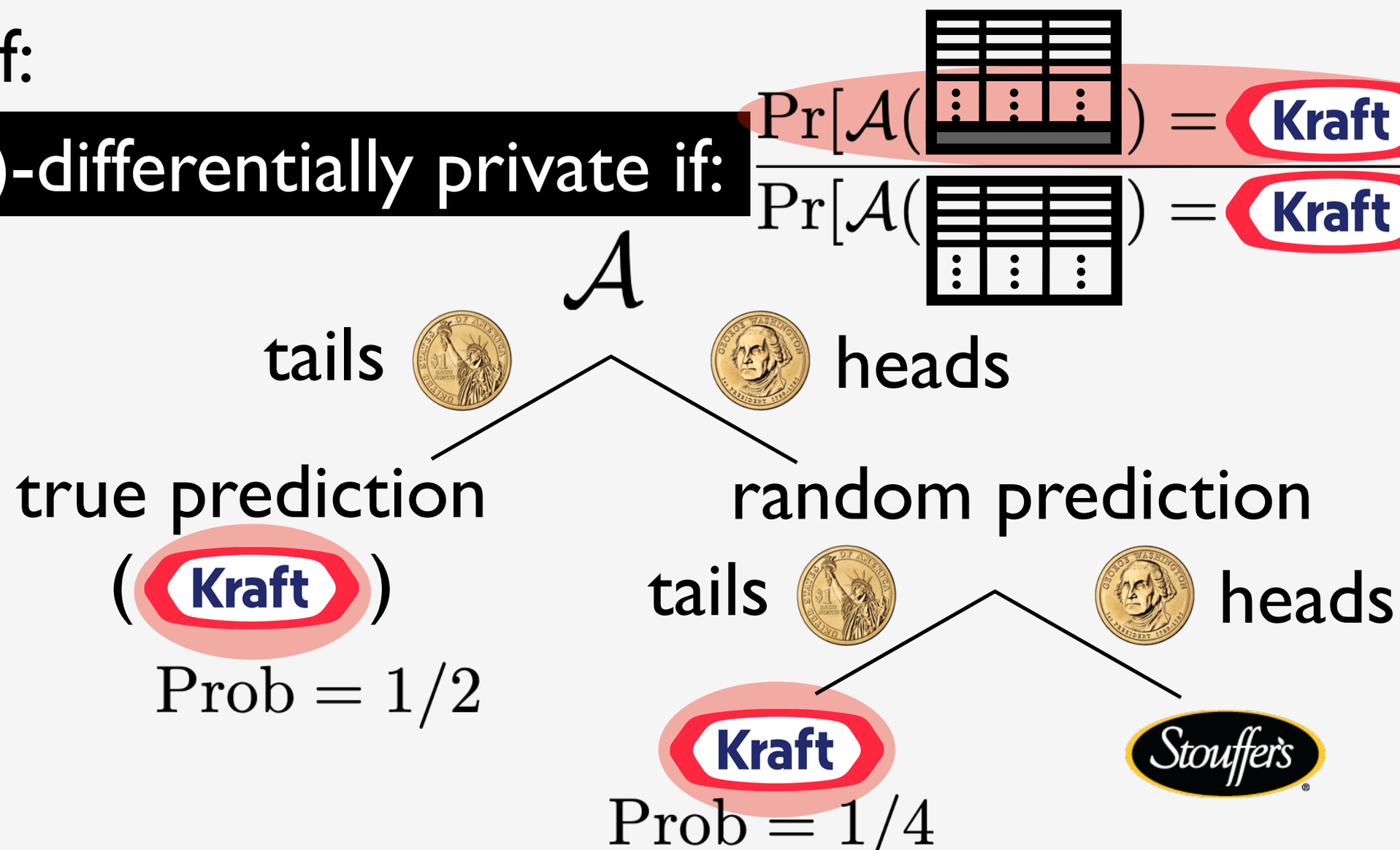
Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\text{table}) = \text{Kraft}]}{\Pr[\mathcal{A}(\text{table}) = \text{Kraft}]} \leq e^{\epsilon}$$



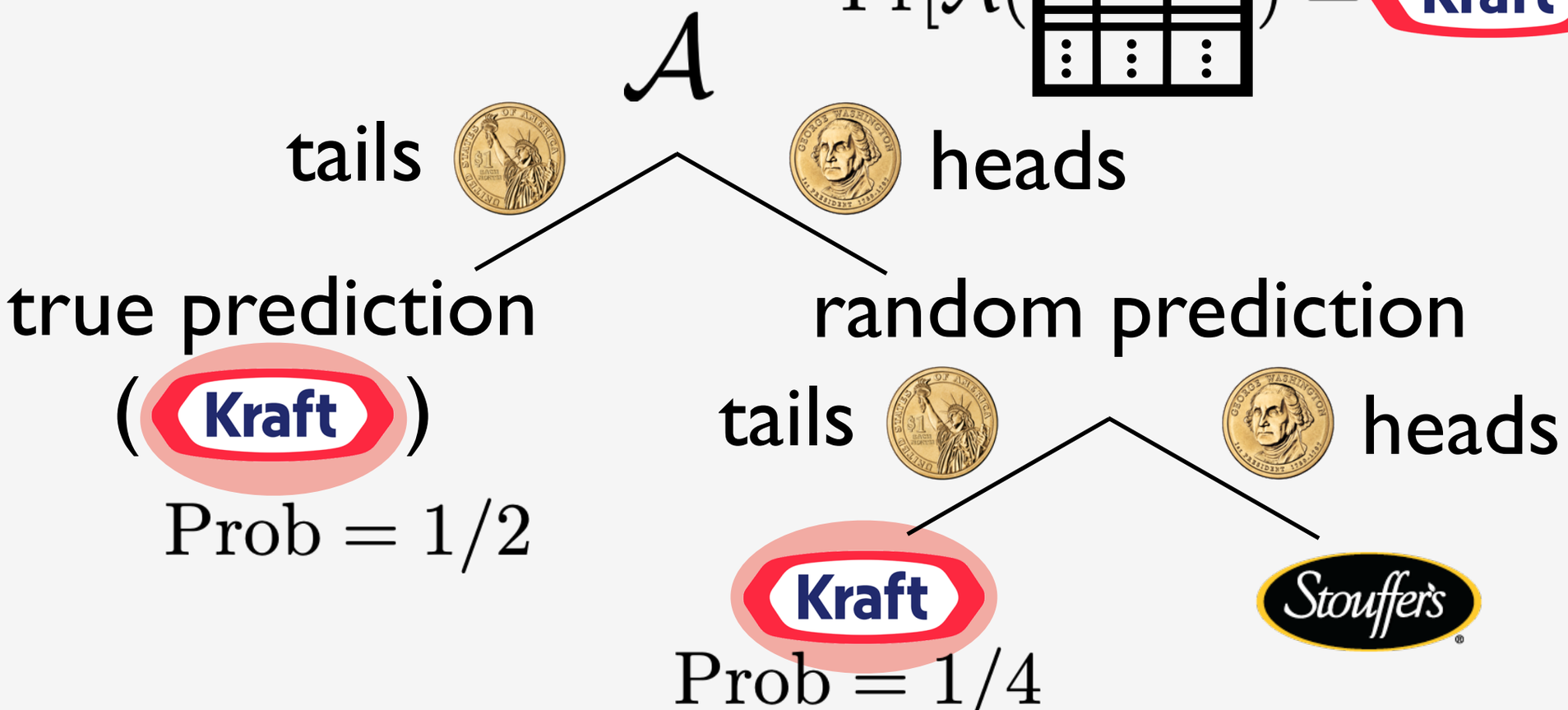
Randomized Response [Warner, 1965]

Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if: $\dfrac{3/4}{\Pr[\mathcal{A}(\text{table}) = \text{Kraft}]} \leq e^{\epsilon}$



Randomized Response [Warner, 1965]

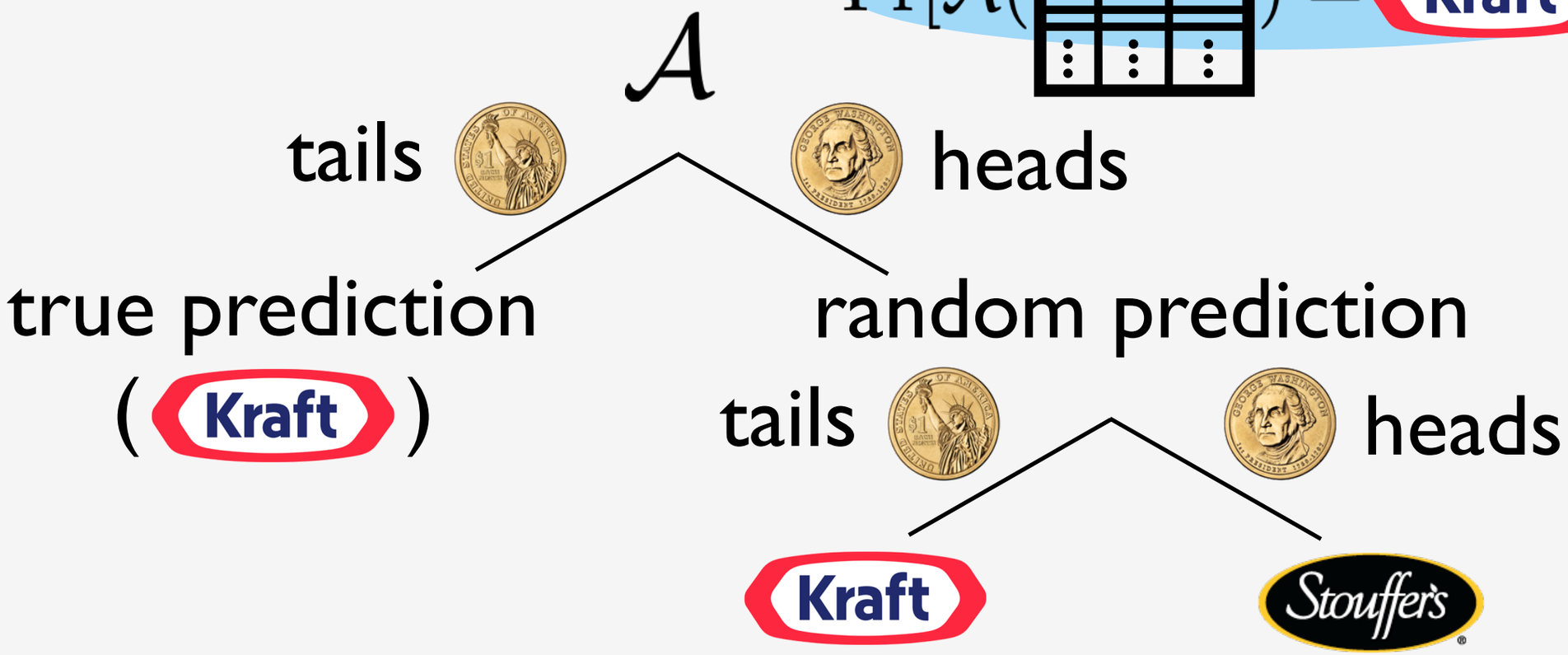
Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{3/4}{\Pr[\mathcal{A}(\text{table}) = \text{Kraft}]} \leq e^{\epsilon}$$



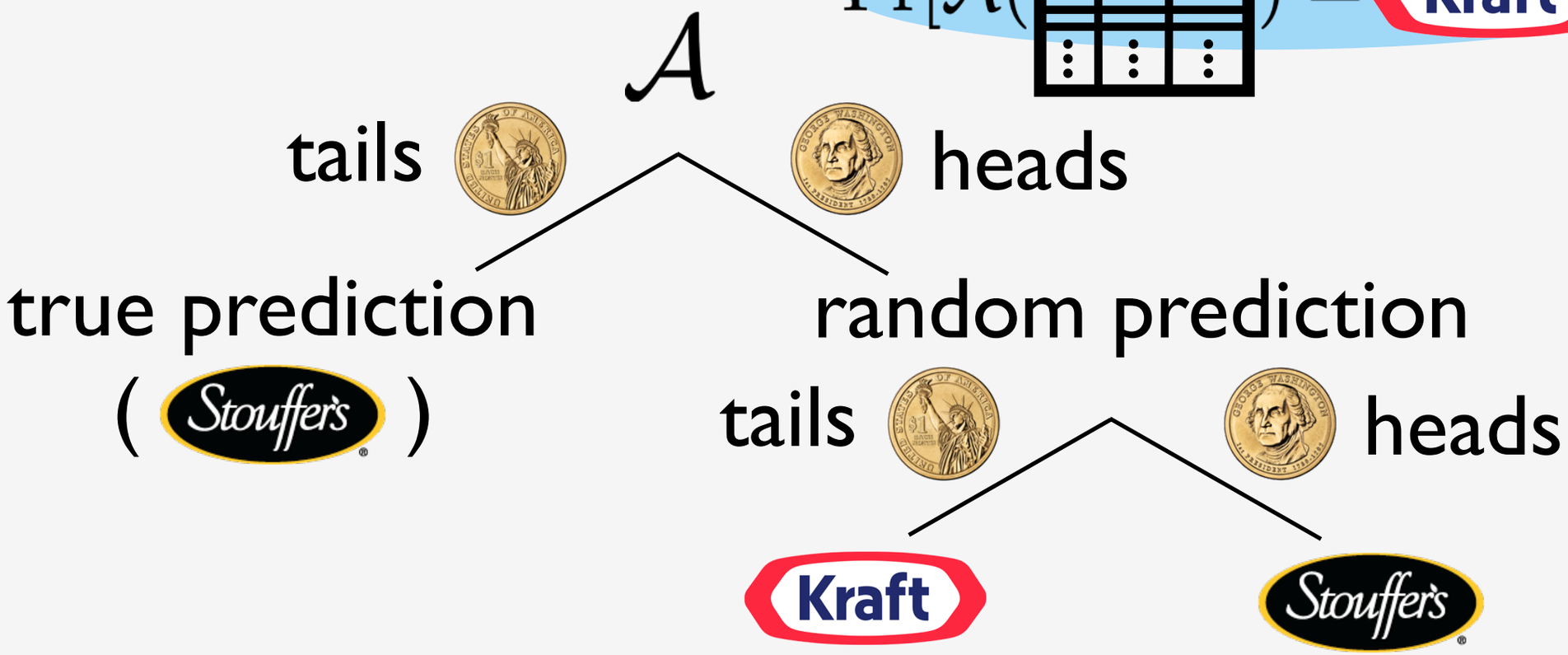
Randomized Response [Warner, 1965]

Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if: $\frac{3/4}{\Pr[\mathcal{A}(\text{table}) = \text{Kraft}]} \leq e^{\epsilon}$



Randomized Response [Warner, 1965]

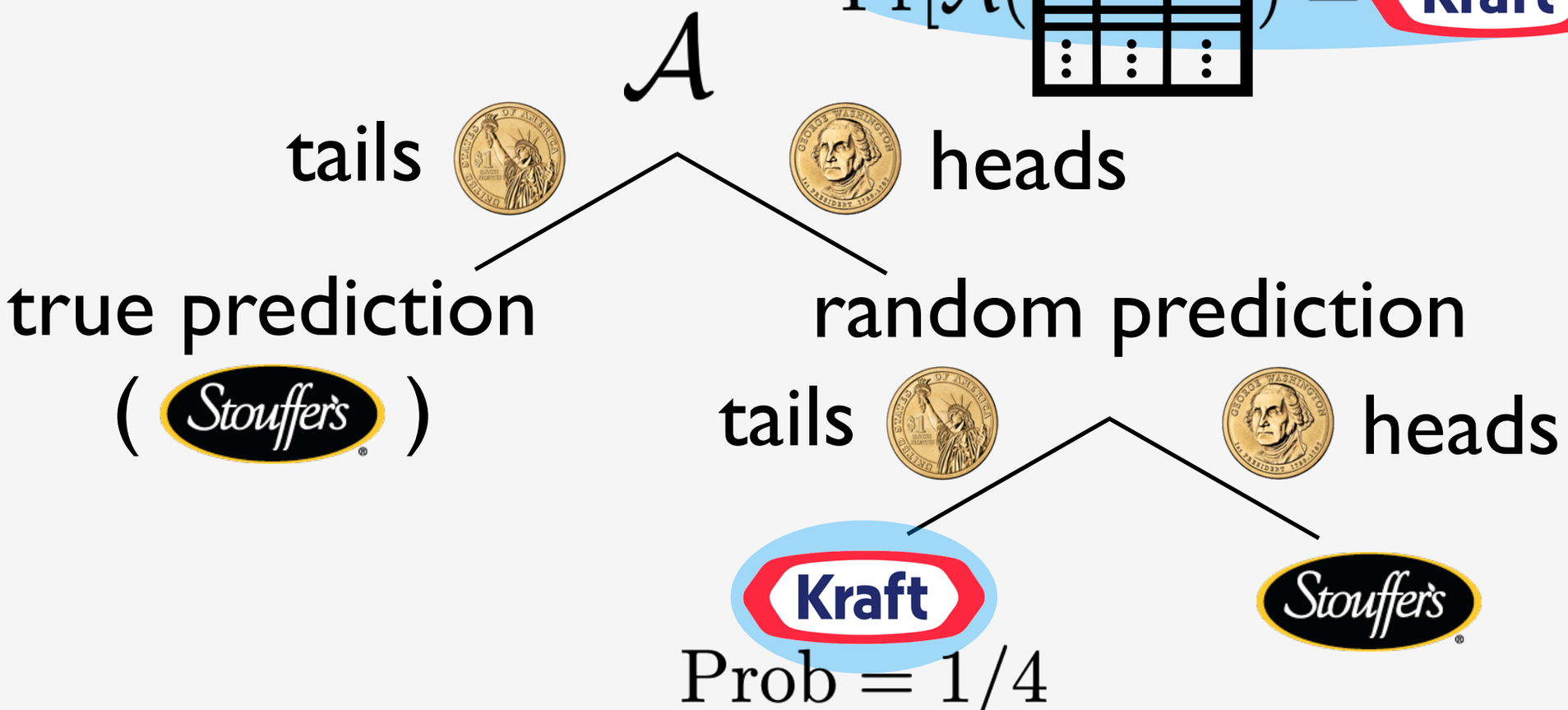
Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{3/4}{\Pr[\mathcal{A}(\text{table}) = \text{Kraft}]} \leq e^{\epsilon}$$



Randomized Response [Warner, 1965]

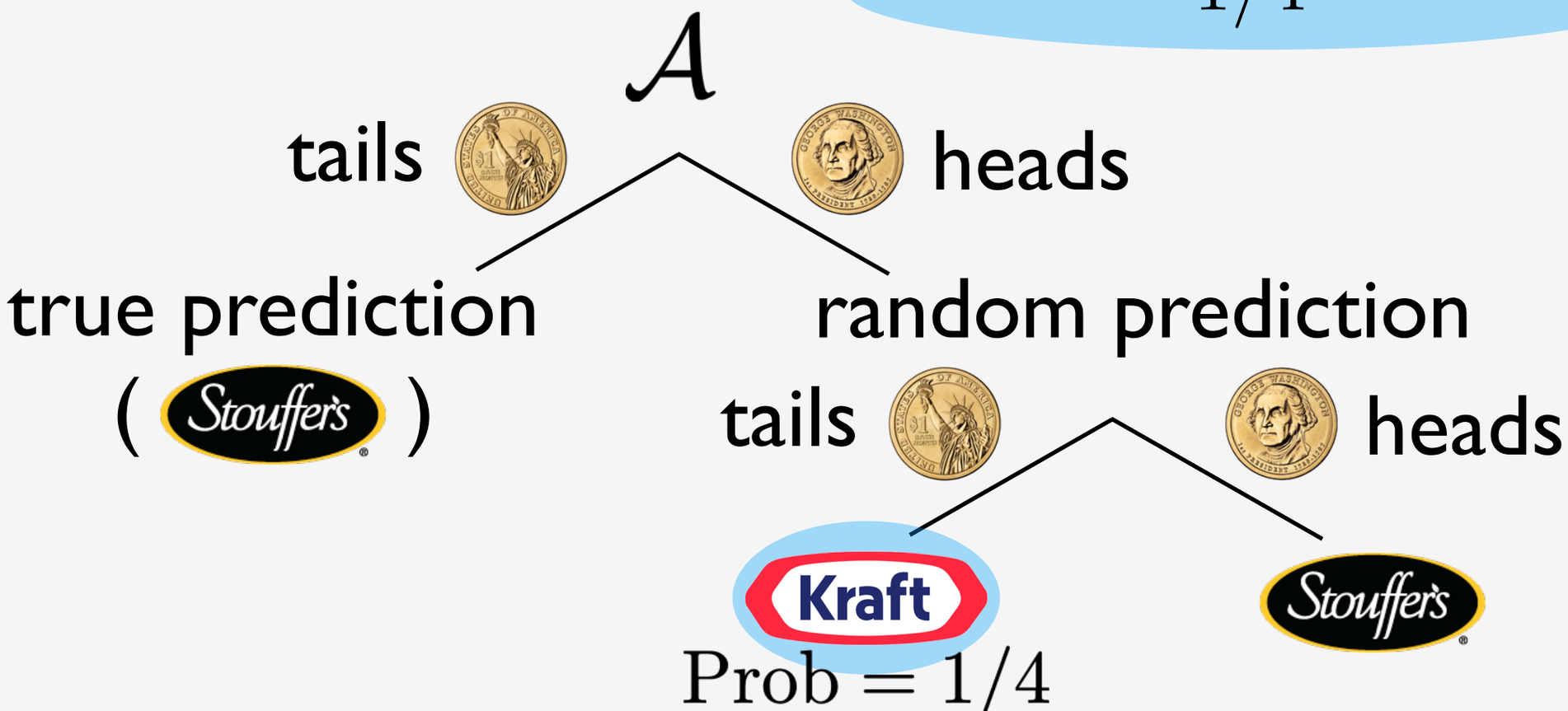
Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{3/4}{1/4} \leq e^{\epsilon}$$



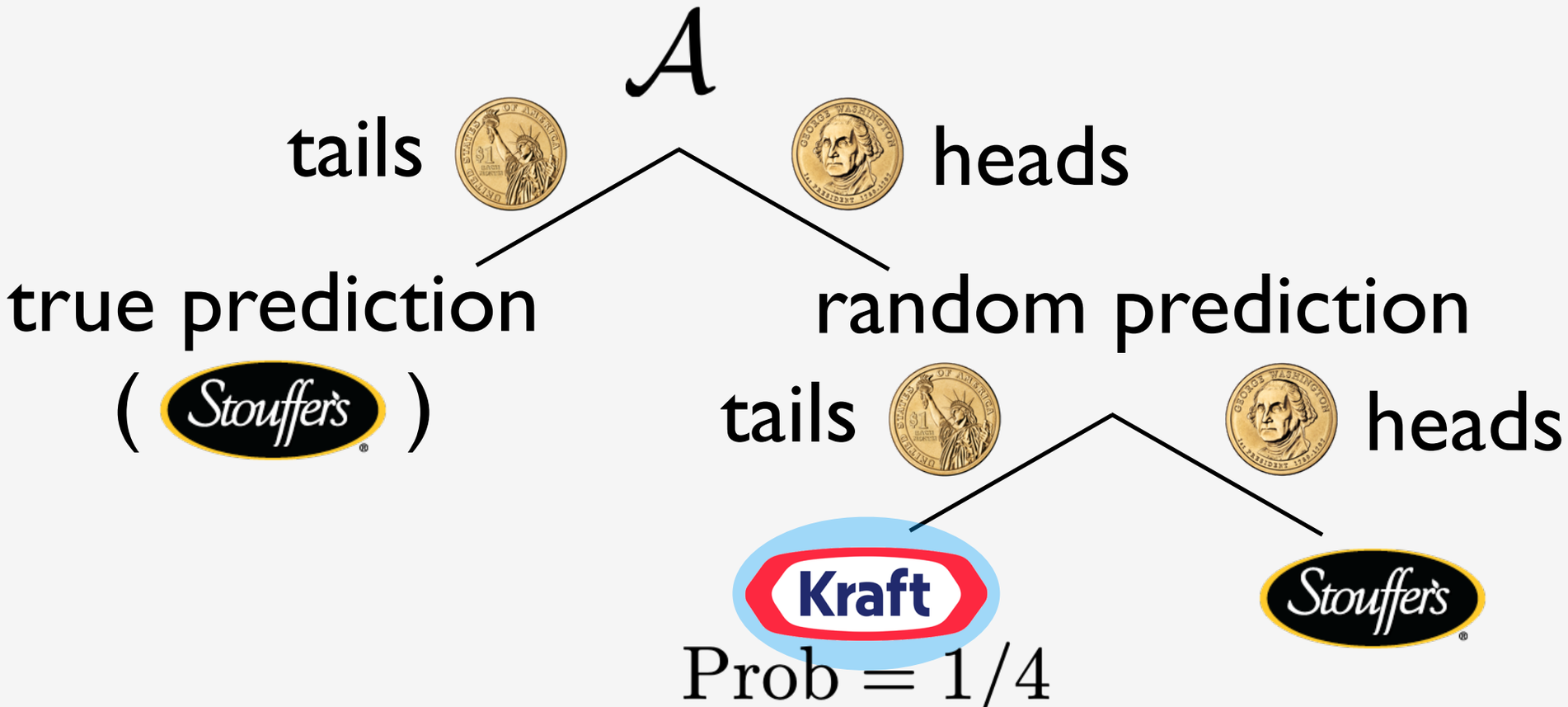
Randomized Response [Warner, 1965]

Claim:

Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if: $\log(3) \leq \epsilon$



Randomized Response [Warner, 1965]

Claim:

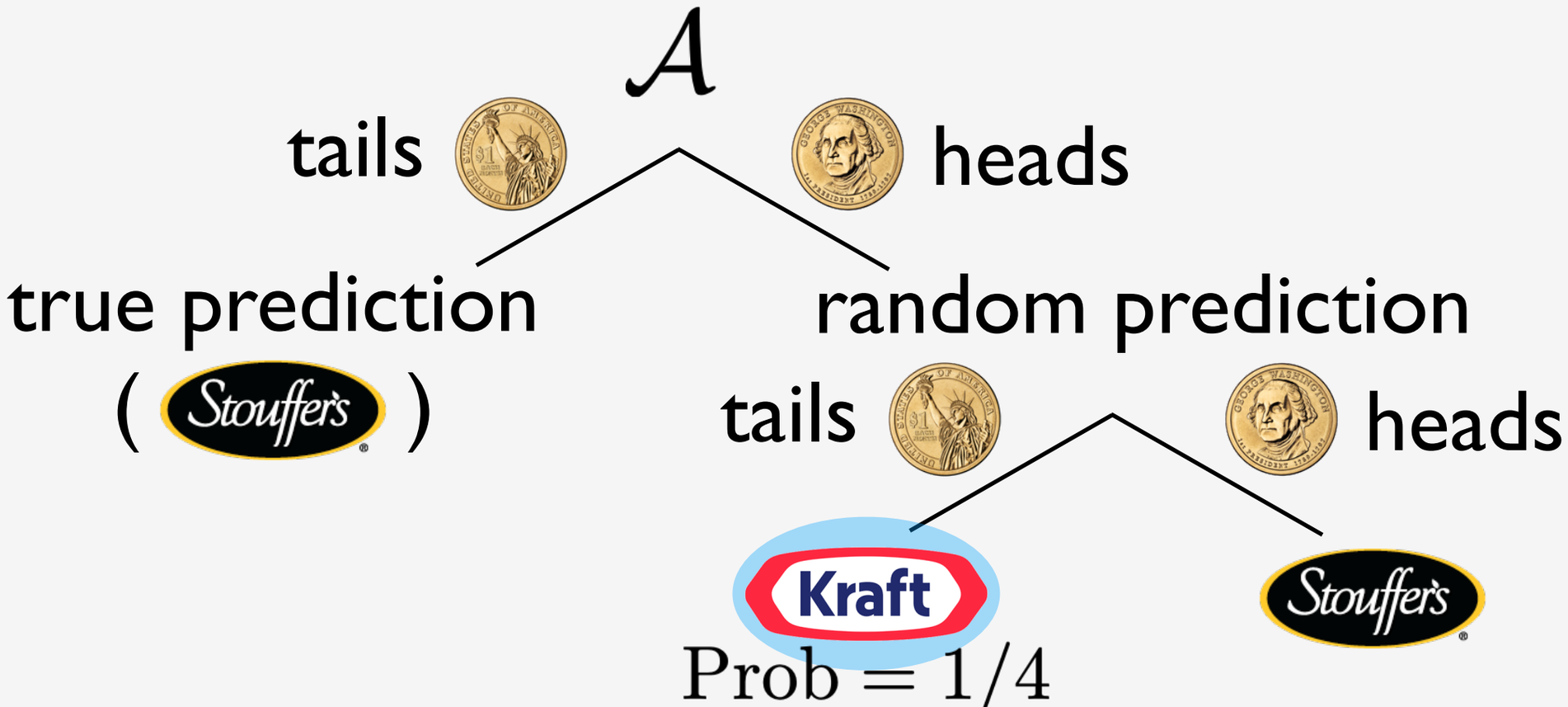
Randomized response is (log 3)-differentially private

Proof:

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\log(3) \leq \epsilon$$

□



Differential Privacy

[Dwork et al., 2006]

A formalization of "privacy through randomness"

Definition. *A randomized algorithm $\mathcal{A}$ is (ϵ, δ)-**differentially private** if for all $\mathbf{x} \subseteq Range(\mathcal{A})$ and for neighboring datasets $\mathcal{D}, \mathcal{D}'$ we have that,*

$$\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}] \leq e^{\epsilon} \Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}] + \delta$$

Differential Privacy [Dwork et al., 2006]

A formalization of "privacy through randomness"

properties

Differential Privacy [Dwork et al., 2006]

A formalization of "privacy through randomness"

properties

1. k (ϵ, δ)-differentially private runs is $(k\epsilon, k\delta)$-diff. private

Differential Privacy [Dwork et al., 2006]

A formalization of "privacy through randomness"

properties

1. k (ϵ, δ)-differentially private runs is $(k\epsilon, k\delta)$-diff. private
2. Post-processing doesn't decrease privacy

Differential Privacy [Dwork et al., 2006]

A formalization of "privacy through randomness"

properties

1. k (ϵ, δ)-differentially private runs is $(k\epsilon, k\delta)$-diff. private

2. Post-processing doesn't decrease privacy

3. Immune to common attacks:
   - linkage attacks
   - differencing attacks

Differential Privacy [Dwork et al., 2006]

A formalization of "privacy through randomness"

properties

1. k (ϵ, δ)-differentially private runs is $(k\epsilon, k\delta)$-diff. private

2. Post-processing doesn't decrease privacy

3. Immune to common attacks:
   - linkage attacks
   - differencing attacks

4. Doesn't compromise privacy of few for sake of all

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

Global Sensitivity

[Dwork et al., 2006]

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

Global Sensitivity

[Dwork et al., 2006]

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

holds for any $\mathcal{D}, \mathcal{D}'$ that differ in one row

Global Sensitivity

[Dwork et al., 2006]

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

holds for any $\mathcal{D}, \mathcal{D}'$ that differ in one row

How much could $\mathcal{A}$ change?

Global Sensitivity

[Dwork et al., 2006]

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

holds for any $\mathcal{D}, \mathcal{D}'$ that differ in one row

How much could $\mathcal{A}$ change?

Global Sensitivity of $\mathcal{A}$

$$\Delta_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|$$

Global Sensitivity

[Dwork et al., 2006]

$\mathcal{A}$ is (ϵ)-differentially private if:

$$\frac{\Pr[\mathcal{A}(\mathcal{D}) = \mathbf{x}]}{\Pr[\mathcal{A}(\mathcal{D}') = \mathbf{x}]} \leq e^{\epsilon}$$

holds for any $\mathcal{D}, \mathcal{D}'$ that differ in one row

How much could $\mathcal{A}$ change?

Global Sensitivity of $\mathcal{A}$

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

$$\Delta^2_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_2$$

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta_{\mathcal{A}}^{1} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$

The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta_{\mathcal{A}}^{1} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)

The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)
2. Draw $r \sim \mathrm{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$

The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)
2. Draw $r \sim \mathrm{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$ — Laplace distribution (with mean 0)

$$\mathrm{Lap}(r \mid \theta) = \frac{1}{2\theta} \exp\left(-\frac{|r|}{\theta}\right)$$

The Laplace Mechanism

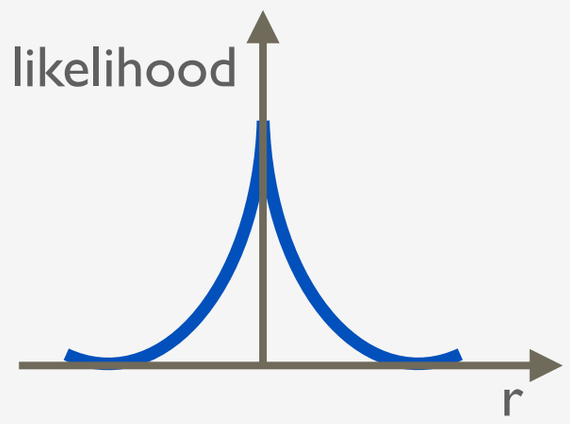
[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)
2. Draw $r \sim \text{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$ — Laplace distribution (with mean 0)

$$\text{Lap}(r \mid \theta) = \frac{1}{2\theta} \exp\left(-\frac{|r|}{\theta}\right)$$



The Laplace Mechanism

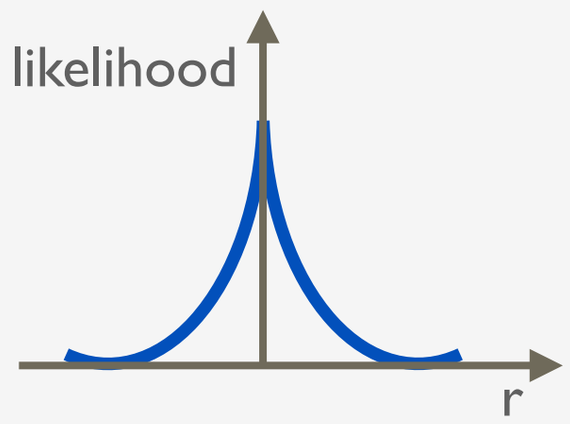
[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)
2. Draw $r \sim \mathrm{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$ — Laplace distribution (with mean 0)
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$

$$\mathrm{Lap}(r \mid \theta) = \frac{1}{2\theta} \exp\left(-\frac{|r|}{\theta}\right)$$



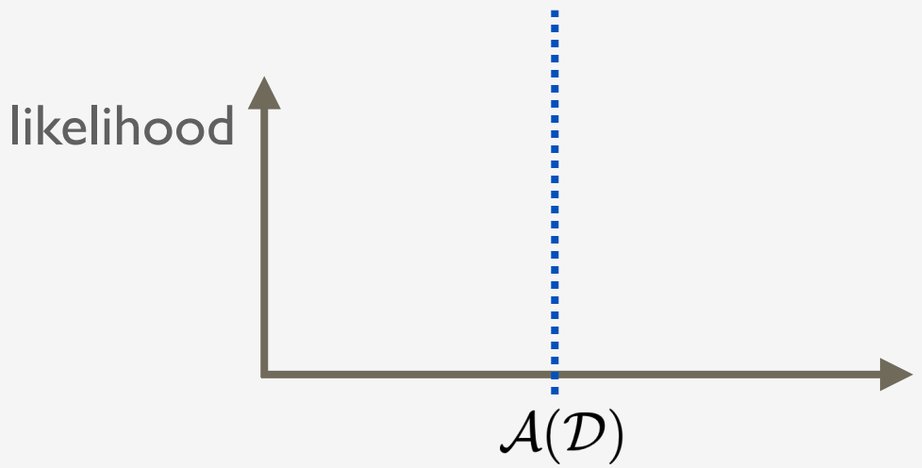
The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$
2. Draw $r \sim \mathrm{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$



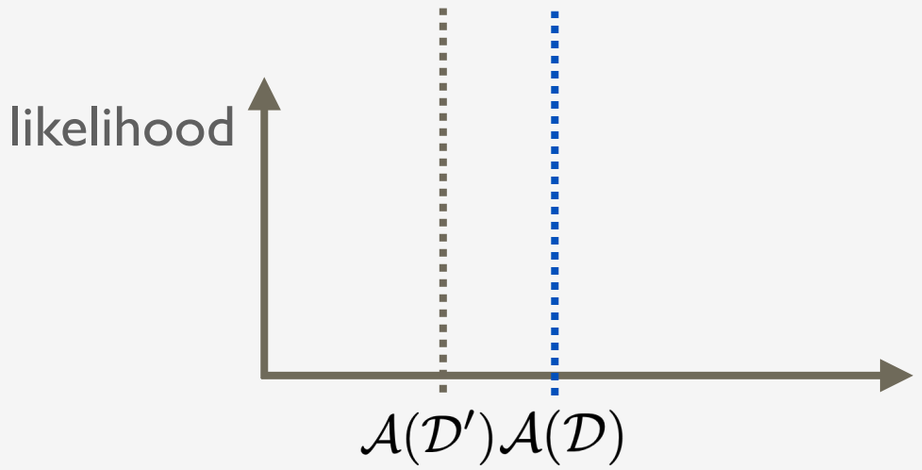
The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$
2. Draw $r \sim \mathrm{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$



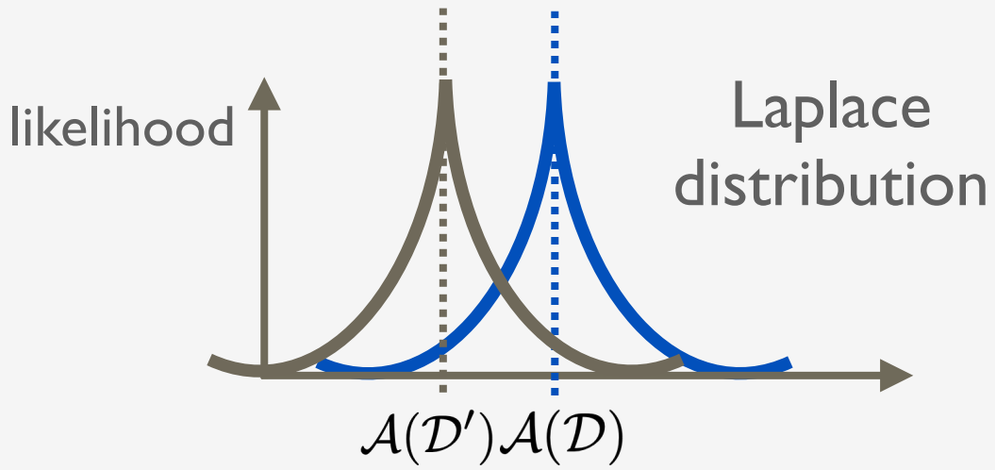
The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$
2. Draw $r \sim \text{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$



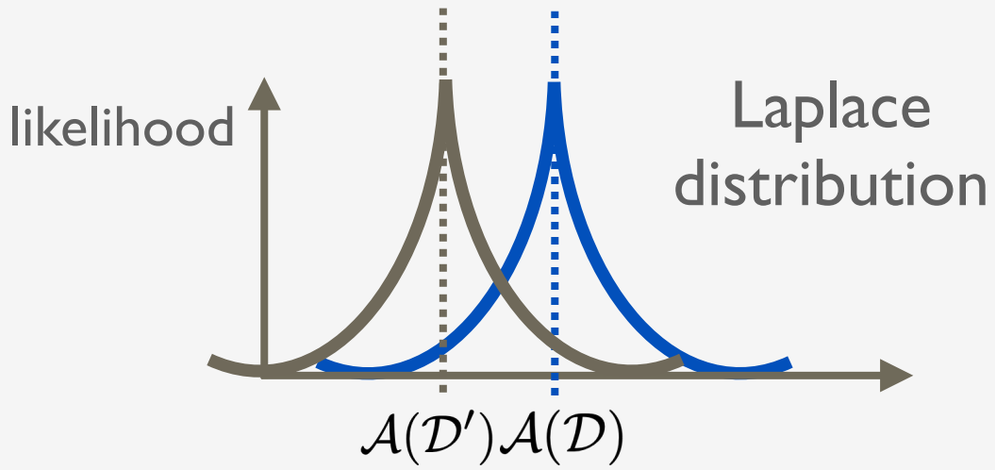
The Laplace Mechanism

[Dwork et al., 2006]

$$\Delta^1_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_1$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$
2. Draw $r \sim \text{Lap}(r \mid \Delta^1_{\mathcal{A}}/\epsilon)$
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$



The Laplace Mechanism guarantees $(\epsilon, 0)$ differential privacy

The Gaussian Mechanism

[Dwork & Roth, 2014]

$$\Delta_{\mathcal{A}}^2 := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_2$$

The Gaussian Mechanism

[Dwork & Roth, 2014]

$$\Delta_{\mathcal{A}}^2 := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_2$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)
2. Draw $r \sim \mathcal{N}(r \mid \Delta_{\mathcal{A}}^2 \sqrt{2 \log(1.25/\delta)}/\epsilon)$
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$

Gaussian distribution (mean 0)

$$\mathcal{N}(r \mid \sigma) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{r^2}{2\sigma^2}\right)$$

The Gaussian Mechanism

[Dwork & Roth, 2014]

$$\Delta_{\mathcal{A}}^2 := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|_2$$

Goal: Make $\mathcal{A}(\mathcal{D})$ public, but keep $\mathcal{D}$ differentially private

1. Compute $\mathcal{A}(\mathcal{D})$ — scalar (for simplicity)
2. Draw $r \sim \mathcal{N}(r \mid \Delta_{\mathcal{A}}^2 \sqrt{2\log(1.25/\delta)}/\epsilon)$
3. Publicly release $\mathcal{A}(\mathcal{D}) + r$

Gaussian distribution (mean 0)

$$\mathcal{N}(r \mid \sigma) = \frac{1}{\sqrt{2}} \exp\left(-\frac{r^2}{2\sigma^2}\right)$$

The Gaussian Mechanism guarantees (ϵ, δ) differential privacy

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

The Laplace Mechanism
The Gaussian Mechanism
— Continuous data

The Exponential Mechanism — Discrete data

Local Sensitivity

The Exponential Mechanism

[McSherry and Talwar, 2007]

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \rightarrow \mathbb{R}$

$\mathbf{x} \in Range(\mathcal{A})$

discrete

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

e.g., score of ranking $\mathbf{x}$ for dataset $\mathcal{D}$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$$

"quality function"

ideally...

$$\mathcal{A}(\mathcal{D}) = \arg\max_{\mathbf{x} \in \mathcal{X}} q(\mathcal{D}, \mathbf{x})$$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$$

"quality function"

deterministic!

$$\mathcal{A}(\mathcal{D}) = \arg\max_{\mathbf{x} \in \mathcal{X}} q(\mathcal{D}, \mathbf{x})$$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$

"quality function"

deterministic!

$$\mathcal{A}(\mathcal{D}) = \arg\max_{\mathbf{x} \in \mathcal{X}} q(\mathcal{D}, \mathbf{x})$$

changes in $\mathcal{D}$ may cause changes in q!

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

changes in $\mathcal{D}$ may cause changes in q!

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

changes in $\mathcal{D}$ may cause changes in q!

Definition. *The* ***global sensitivity*** *of q is defined as,*

$$\Delta_q \triangleq \max_{\mathcal{D},\mathcal{D}',\mathbf{x}} |q(\mathcal{D}, \mathbf{x}) - q(\mathcal{D}', \mathbf{x})|$$

where $\mathcal{D}, \mathcal{D}'$ are neighboring datasets.

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

Definition. *Given a dataset $\mathcal{D}$ the* ***exponential mechanism*** *$\mathcal{A}$ selects an element $\mathbf{x} \in \mathcal{X}$ with probability,*

$$\Pr[\mathbf{x}] = \exp\left(\frac{\epsilon q(\mathcal{D}, \mathbf{x})}{2\Delta_q}\right)\frac{1}{\mathbf{Z}}$$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

Definition. *Given a dataset $\mathcal{D}$ the* ***exponential mechanism*** *$\mathcal{A}$ selects an element $\mathbf{x} \in \mathcal{X}$ with probability,*

$$\Pr[\mathbf{x}] = \exp\left(\frac{\epsilon q(\mathcal{D}, \mathbf{x})}{2\Delta_q}\right)\frac{1}{\mathbf{Z}}$$

normalizing constant over all $\mathbf{x} \in \mathcal{X}$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

Definition. *Given a dataset $\mathcal{D}$ the* ***exponential mechanism*** *$\mathcal{A}$ selects an element $\mathbf{x} \in \mathcal{X}$ with probability,*

$$\Pr[\mathbf{x}] = \exp\left(\frac{\epsilon q(\mathcal{D}, \mathbf{x})}{2\Delta_q}\right)\frac{1}{\mathbf{Z}}$$

$$\mathcal{A}(\mathcal{D}) \approx \arg\max_{\mathbf{x}\in\mathcal{X}} q(\mathcal{D}, \mathbf{x})$$

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

Definition. *Given a dataset $\mathcal{D}$ the* ***exponential mechanism*** *$\mathcal{A}$ selects an element $\mathbf{x} \in \mathcal{X}$ with probability,*

$$\Pr[\mathbf{x}] = \exp\left(\frac{\epsilon q(\mathcal{D}, \mathbf{x})}{2\Delta_q}\right)\frac{1}{\mathbf{Z}}$$

Theorem. *The exponential mechanism $\mathcal{A}$ is ϵ-differentially private.*

The Exponential Mechanism

[McSherry and Talwar, 2007]

a general mechanism for ϵ-differential privacy

$q(\mathcal{D}, \mathbf{x}) \to \mathbb{R}$ "quality function"

Definition. *Given a dataset $\mathcal{D}$ the* ***exponential mechanism*** *$\mathcal{A}$ selects an element $\mathbf{x} \in \mathcal{X}$ with probability,*

$$\Pr[\mathbf{x}] = \exp\left(\frac{\epsilon q(\mathcal{D}, \mathbf{x})}{2\Delta_q}\right)\frac{1}{\mathbf{Z}}$$

Theorem. *The exponential mechanism $\mathcal{A}$ is ϵ-differentially private.*

Theorem. *Given that $\hat{\mathbf{x}}$ is output by the exponential mechanism, then*

$$q(\mathcal{D}, \hat{\mathbf{x}}) \geq \max_{\mathbf{x} \in \mathcal{X}} q(\mathcal{D}, \mathbf{x}) - \frac{2\Delta_q}{\epsilon}(\log|\mathcal{X}| + t)$$

with probability at least $1 - e^{-t}$.

This Talk

A Web Search Example

Privacy via Randomization

Differential Privacy

Global Sensitivity

Privacy Mechanisms

- The Laplace Mechanism
- The Gaussian Mechanism
- The Exponential Mechanism

Local Sensitivity

Local Sensitivity [Nissim et al., 2007]

Global Sensitivity of $\mathcal{A}$

$$\Delta_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|$$

Local Sensitivity [Nissim et al., 2007]

Global Sensitivity of $\mathcal{A}$

$$\Delta_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|$$

Local Sensitivity of $\mathcal{A}$, for specific dataset $\mathcal{D}$

$$\Delta(\mathcal{D})_{\mathcal{A}} := \max_{D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D})\|$$

Local Sensitivity [Nissim et al., 2007]

Global Sensitivity of $\mathcal{A}$

$$\Delta_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|$$

$$\Delta(\mathcal{D})_{\mathcal{A}} < \Delta_{\mathcal{A}}$$

Local Sensitivity of $\mathcal{A}$, for specific dataset $\mathcal{D}$

$$\Delta(\mathcal{D})_{\mathcal{A}} := \max_{D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D})\|$$

Local Sensitivity [Nissim et al., 2007]

Global Sensitivity of $\mathcal{A}$

$$\Delta_{\mathcal{A}} := \max_{D,D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D}')\|$$

$$\Delta(\mathcal{D})_{\mathcal{A}} < \Delta_{\mathcal{A}}$$

Local Sensitivity of $\mathcal{A}$, for specific dataset $\mathcal{D}$

$$\Delta(\mathcal{D})_{\mathcal{A}} := \max_{D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D})\|$$

Multiple DP algorithms use local sensitivity

[Nissim et al., 2007] [Dwork & Lei, 2009] [Smith & Thakurta, 2013] [Dwork & Roth, 2014]

Takeaways

Losing privacy is easier than it seems

Takeaways

Losing privacy is easier than it seems

account

old@yahoo.com

age: 50

Differential privacy quantifies

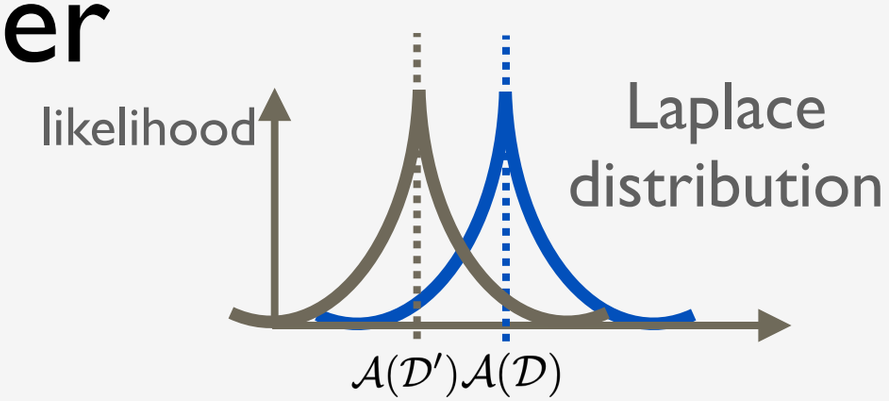
privacy via randomisation

Takeaways

Losing privacy is easier than it seems

Differential privacy quantifies
privacy via randomisation

Main idea: add noise on the order of the **global sensitivity**

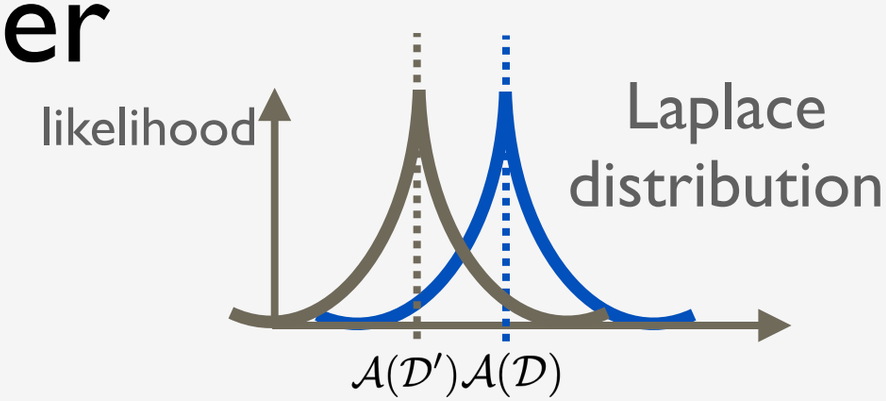


Takeaways

Losing privacy is easier than it seems

Differential privacy quantifies **privacy via randomisation**

Main idea: add noise on the order of the **global sensitivity**



If too much noise, can sometimes use **local sensitivity** instead!

$$\Delta(\mathcal{D})_{\mathcal{A}} := \max_{D' \text{ s.t. } D,D' \text{ diff by one row}} \|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{D})\|$$