

# DatashareNetwork: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists

---

**Kasra EdalatNejad (EPFL)**

Wouter Lueks (EPFL), Julien Martin, Soline Ledésert (ICIJ)

Anne Lhôte (ICIJ), Bruno Thomas (ICIJ), Laurent Girod (EPFL), Carmela Troncoso (EPFL)

**EPFL**





DONATE

FOLLOW

# Journalists

The International Consortium of Investigative Journalists is a global network of 267 investigative journalists in 100 countries who collaborate on in-depth investigative stories.





An ICIJ Investigation

# The Panama Papers: Exposing the Rogue Offshore Finance Industry

A giant leak of more than 11.5 million financial and legal records exposes a system that enables crime, corruption and wrongdoing, hidden by secretive offshore companies.



11.5 Million documents  
(Centralized)

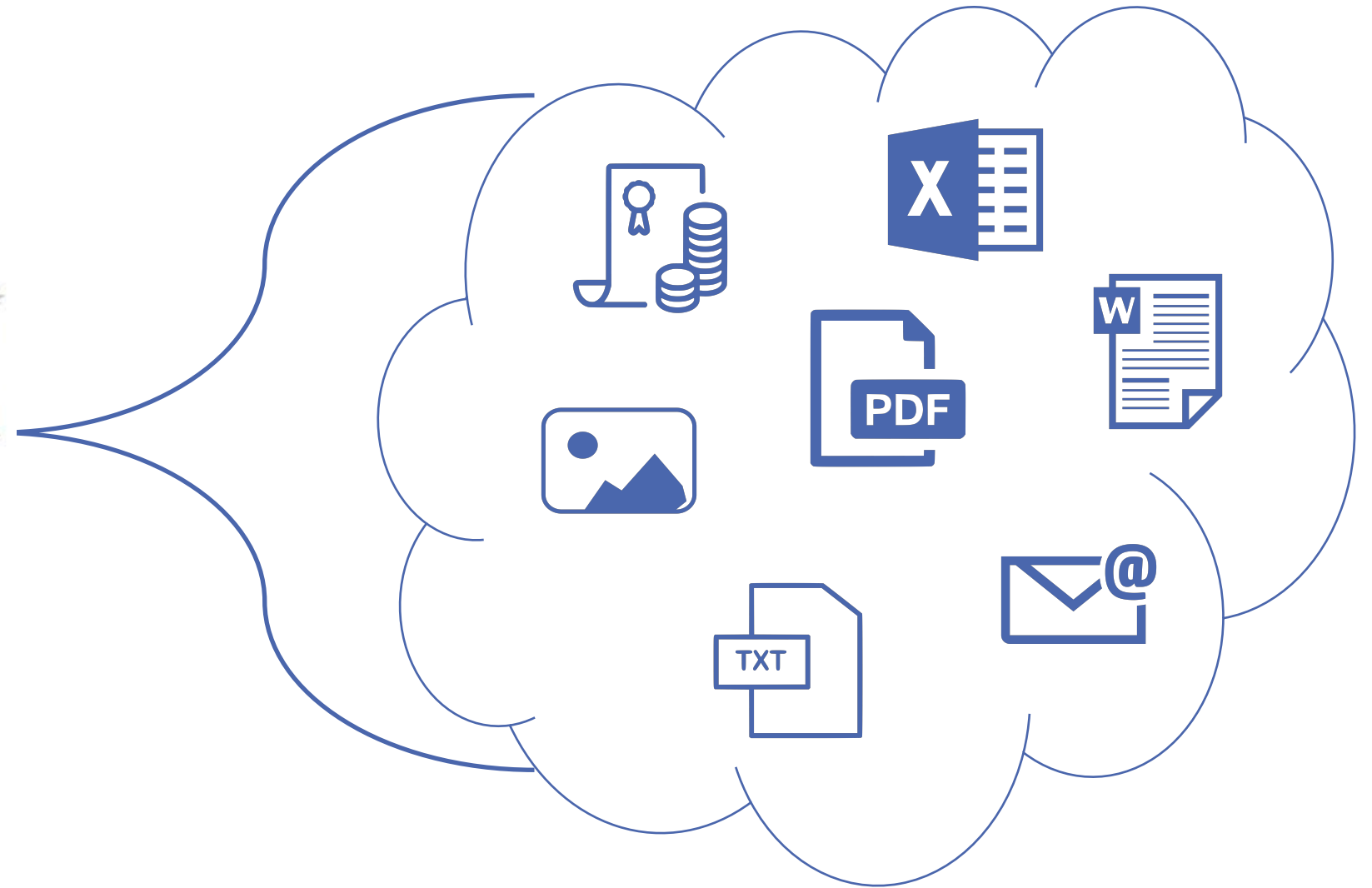


An ICIJ Investigation

## The Panama Papers: Exposing the Rogue Offshore Finance Industry

A giant leak of more than 11.5 million financial and legal records exposes a system that enables crime, corruption and wrongdoing, hidden by secretive offshore companies.

# Digital





# Datashare

beta

Better analyze information, in all its forms

al if you could provide us with your approval and transactions described below.

ng dated November 15, 2000 for a description of regular the UMTS activities it is developing in Europ

H4201030M.pdf

Private Equity Fund II

our client Sages Gestion SA, the investment advi equity Fund II (the "Fund"), and further to our February 7, 2002, we are pleased to submit for yo treatment of the following structure agreed could be pleased to receive your written comments o

mercantial\_fsrt\_page.pdf

communications (Vietnam) Sarl

bring the following developments to your attentio comments on the below structure.

H4204006M.pdf

Co

Sarl - Tax number: 2006 24 18398 x number: 2006 24 15399

pleased if you could examine and provide us with Luxembourg tax treatment regarding the transact ighy Hanson & Co as outlined in this letter.

d

al if you could provide us with your approval and transactions described below.

ng dated November 15, 2000 for a description of regular the UMTS activities it is developing in Europ

H4201032M.pdf

Holding Luxembourg (FFH Luxembourg) is pa group. More information about the group can l a site: <http://www.fairfax.ca/home.html>. For your ow pages from this site to this document.

Fairfax Financial Holdin...

ke to submit our analysis of the Luxembourg direc g of Centennial Partners SARL. We would be y and provide us with your agreement and / or are.

centenial\_20012005.pdf

ring dated 12 July 2006, we would like to submit ovementioned companies, the following situati our comments on the tax treatment described herei

# H4201030M.pdf

## 👤 People (36)

- KOHL HUTCHISON LUXCO HUTCHISON KOHL PEETERS LUXCO LUXCO LUXCO LUXCO LUXCO WIM PIOT WIM PIOT
- MARIUS KOHLLUXEMBOURG HUTCHISON CONFIDENTIAL HUTCHISON ROBERT ECBRT ECKERT LUXELLBOURG ILCJB DINE AUMIAN SCHILLING
- ROBIO SNG DIRECTOR HUTCHISON HUTCHISON ROBERT ECKERT ECKERT HUTCHISON ROBINDIRECTORHUTCHISON HUTCHISON ROBERT
- HUTCHISON HUTOHLSA DILLION ROBIN ROBERT ECKERT ECKERT HUTCHISON

Extracted using **CORENLP** in **ENGLISH**

...tria, the fiscal value of LuxCo's

participation in **H3G Holdings** should consist of its acquisition price, increased by the

amounts granted by LuxCo to H3G Austria. The total amount of these contributions will

## 🏢 Organizations (52)

- MR PEETERS ADMINISTRATION DES CONTR
- LUXEMBOURG TELEPHONE HUTCHISON
- HUTCHISON WHAMPOA LIMITED AUSTR
- R.C. LUXEMBOURG BUREAU D'IMPOSITIO
- RMS/VLN/H4201030M-WPIHUTCHISON WH
- HUTCHISON WHAMPOA LIMITED HUTCH
- H3G HOLDINGS R.C. LUXEMBOURG B LUXCO LUXCO H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS LUX CO LUXCO LUXCO
- H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS HUTCHISON 3G AUSTRIA INVESTMENTS S.A.R.L HUTCHISON 3G AUSTRIAGMBH
- AUSTRIA INVESTMENTS S.A.R.L. HDTCHISON 3G AUSTRIA GMBH HUTCHISON AUSTRIA INVESTMENTS YHUTCHISON 3G AUSTRIA INVESTMENTS
- HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA HOLDINGS HUTCHISON 3G AUSTRIA GMBH. HUTCHISON 3G AUSTRIA GMBH FCBRUAR
- AUSTRIA GMBH AUSLRIA INVESTMENTS S.A.R.L. HUTCHISON 3G AUSTRLA HOLDINGSGMBH HUTCHISON 3G AUSTRIA GMBH

## 📍 Locations (61)

- EUROPE AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG EUROPE AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA ILL AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- LUXEMBOURG AUSTRIA AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG LUXEMBOURG
- AUSTRIA AUSTRIA EUROPE AUSTRIA VIENNA AUSTRIA HATCBISOO AUSTRIA AUSTRIA EUROPE JC LUXEMBOURG VIENNA

Show more locations



1



Sort 1 - 100 on 1,086 documents

/vault/luxleaks/ Clear all filters

... if you could provide us with your approval and transactions described below.

... dated November 15, 2000 for a description of the UMTS activities it is developing in Europe.

H4201030M.pdf

... if you could provide us with your approval and transactions described below.

... dated November 15, 2000 for a description of the UMTS activities it is developing in Europe.

H4201032M.pdf

Private Equity Fund II

... or client Sages Gestion SA, the investment advisory Fund II (the "Fund"), and further to our January 7, 2002, we are pleased to submit for your treatment of the following structure agreed could be pleased to receive your written comments.

merccapital\_fsrt\_page.pdf

... Holding Luxembourg (FHH Luxembourg) is a group. More information about the group can be found at a site: <http://www.fairfax.ca/home.html>. For your review please refer to this document.

... g is held, but for one share, by a Dutch parent (BV). FHH Luxembourg acts as the holding company.

Fairfax Financial Holdings

communications (Vietnam) SARL

... bring the following developments to your attention and provide us with your comments on the below structure.

H4204006M.pdf

... ke to submit our analysis of the Luxembourg directorship of Centennial Partners SARL. We would be pleased to provide you with our agreement and conclusions.

... is Limited ("HWL") is a Hong Kong listed company.

centennial\_20012005.pdf

Ca

... if you could examine and provide us with Luxembourg tax treatment regarding the transactions described herein as outlined in this letter.

H4204006M.pdf

... ring dated 12 July 2006, we would like to submit our analysis of the Luxembourg directorship of Centennial Partners SARL. We would be pleased to provide you with our agreement and conclusions.

centennial\_20012005.pdf

Back to search results

< Previous Next >

Mark as recommended

1



Download

# H4201030M.pdf

- EXTRACTED TEXT
- PREVIEW
- TAGS & DETAILS
- NAMED ENTITIES**

## People (36)

- KOHL HUTCHISON LUXCO HUTCHISON KOHL PEETERS LUXCO LUXCO LUXCO LUXCO LUXCO WIM PIOT WIM PIOT
- MARIUS KOHLLUXEMBOURG HUTCHISON CONFIDENTIAL HUTCHISON ROBERT ECBRT ECKERT LUXELLBOURG ILCJB DINE AUMIAN SCHILLING
- ROBIO SNG DIRECTOR HUTCHISON HUTCHISON ROBERT ECKERT ECKERT HUTCHISON ROBINDIRECTORHUTCHISON HUTCHISON ROBERT
- HUTCHISON HUTOHLSA DILLION ROBIN ROBERT ECKERT ECKERT HUTCHISON

Extracted using CORENLP in ENGLISH

...tria, the fiscal value of LuxCo's participation in H3G Holdings should consist of its acquisition price, increased by the amounts granted by LuxCo to H3G Austria. The total amount of these contributions will

## Organizations (52)

- MR PEETERS ADMINISTRATION DES CONTR
- LUXEMBOURG TELEPHONE HUTCHISON
- HUTCHISON WHAMPOA LIMITED AUSTR
- R.C. LUXEMBOURG BUREAU D'IMPOSITIO
- RMS/VLN/H4201030M-WPIHUTCHISON WH
- HUTCHISON WHAMPOA LIMITED HUTCH
- H3G HOLDINGS R.C. LUXEMBOURG B LUXCO LUXCO H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS LUX CO LUXCO LUXCO
- H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS HUTCHISON 3G AUSTRIA INVESTMENTS S.A.R.L HUTCHISON 3G AUSTRIAGMBH
- AUSTRIA INVESTMENTS S.A.R.L. HDTCHISON 3G AUSTRIA GMBH HUTCHISON AUSTRIA INVESTMENTS YHUTCHISON 3G AUSTRIA INVESTMENTS
- HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA HOLDINGS HUTCHISON 3G AUSTRIA GMBH. HUTCHISON 3G AUSTRIA GMBH FCBRUAR
- AUSTRIA GMBH AUSLRIA INVESTMENTS S.A.R.L. HUTCHISON 3G AUSTRALIA HOLDINGSGMBH HUTCHISON 3G AUSTRIA GMBH

## Locations (61)

- EUROPE AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG EUROPE AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA ILL AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- LUXEMBOURG AUSTRIA AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG LUXEMBOURG
- AUSTRIA AUSTRIA EUROPE AUSTRIA VIENNA AUSTRIA HATCBISOO AUSTRIA AUSTRIA EUROPE JC LUXEMBOURG VIENNA

Show more locations





1



Sort 1 - 100 on 1,086 documents

/vault/luxleaks/ Clear all filters

al if you could provide us with your approval and transactions described below.

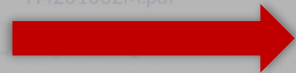
g dated November 15, 2000 for a description of the UMTS activities it is developing in Europe.

H4201030M.pdf

al if you could provide us with your approval and transactions described below.

g dated November 15, 2000 for a description of the UMTS activities it is developing in Europe.

H4201032M.pdf



Private Equity Fund II

mercaperital\_fsrt\_page.pdf

ommunications (Vietnam) Sàrl

H4204006M.pdf

Ca

H4204006M.pdf

1 Holding Luxembourg (FTH Luxembourg) is a group. More information about the group can be found at the site: <http://www.fairfax.com/home.html>. For your convenience, please refer to this document.

Fairfax Financial Holdings

to submit our analysis of the Luxembourg director of Centennial Partners Sàrl. We would be pleased to provide you with our agreement and our report.

centenial\_20012005.pdf

ing dated 12 July 2006, we would like to submit our analysis of the following situation: your comments on the tax treatment described below.

Back to search results

Previous Next

Mark as recommended

1



Download

# H4201030M.pdf

EXTRACTED TEXT PREVIEW TAGS & DETAILS NAMED ENTITIES

## People (36)

- KOHL HUTCHISON LUXCO HUTCHISON KOHL PEETERS LUXCO LUXCO LUXCO LUXCO LUXCO WIM PIOT WIM PIOT
- MARIUS KOHL LUXEMBOURG HUTCHISON CONFIDENTIAL HUTCHISON ROBERT ECBRT ECKERT LUXELLBOURG ILCJB DINE AUMIAN SCHILLING
- ROBIO SNG DIRECTOR HUTCHISON HUTCHISON ROBERT ECKERT ECKERT HUTCHISON ROBINDIRECTOR HUTCHISON HUTCHISON ROBERT
- HUTCHISON HUTOHLSA DILLION ROBIN ROBERT ECKERT ECKERT HUTCHISON

## Organizations (52)

- MR PEETERS ADMINISTRATION DES CONTR
- LUXEMBOURG TELEPHONE HUTCHISON
- HUTCHISON WHAMPOA LIMITED AUSTR
- R.C. LUXEMBOURG BUREAU D'IMPOSITIO
- RMS/VLN/H4201030M-WPIHUTCHISON WH
- HUTCHISON WHAMPOA LIMITED HUTCH
- H3G HOLDINGS R.C. LUXEMBOURG B LUXCO LUXCO H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS LUX CO LUXCO LUXCO
- H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS HUTCHISON 3G AUSTRIA INVESTMENTS S.A.R.L HUTCHISON 3G AUSTRIAGMBH
- AUSTRIA INVESTMENTS S.A.R.L. HDTCHISON 3G AUSTRIA GMBH HUTCHISON AUSTRIA INVESTMENTS YHUTCHISON 3G AUSTRIA INVESTMENTS
- HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA HOLDINGS HUTCHISON 3G AUSTRIA GMBH. HUTCHISON 3G AUSTRIA GMBH FCBRUAR
- AUSTRIA GMBH AUSLRIA INVESTMENTS S.A.R.L. HUTCHISON 3G AUSTRALIA HOLDINGSGMBH HUTCHISON 3G AUSTRIA GMBH

Extracted using CORENLP in ENGLISH

...tria, the fiscal value of LuxCo's

participation in H3G Holdings should consist of its acquisition price, increased by the

amounts granted by LuxCo to H3G Austria. The total amount of these contributions will

## Locations (61)

- EUROPE AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG EUROPE AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA ILL AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- LUXEMBOURG AUSTRIA AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG LUXEMBOURG
- AUSTRIA AUSTRIA EUROPE AUSTRIA VIENNA AUSTRIA HATCBISOO AUSTRIA AUSTRIA EUROPE JC LUXEMBOURG VIENNA

Show more locations



1



Sort 1 - 100 on 1,086 documents

/vault/luxleaks/ Clear all filters

... if you could provide us with your approval and transactions described below.

... dated November 15, 2000 for a description of the UMTS activities it is developing in Europe.

H4201030M.pdf

... if you could provide us with your approval and transactions described below.

... dated November 15, 2000 for a description of the UMTS activities it is developing in Europe.

H4201032M.pdf

Private Equity Fund II

... or client Sages Gestion SA, the investment advisory Fund II (the "Fund"), and further to our January 7, 2002, we are pleased to submit for your treatment of the following structure agreed could be pleased to receive your written comments.

mercantile\_fsrt\_page.pdf

... Holding Luxembourg (FTH Luxembourg) is a group. More information about the group can be found at a site: <http://www.fairfax.ca/home.html>. For your review please refer to the attached document.

... g is held, but for one share, by a Dutch parent: (BV) FHH Luxembourg acts as the holding company.

Fairfax Financial Holdings...

communications (Vietnam) S&P

... bring the following developments to your attention. Comments on the below structure.

H4204006M.pdf

... We would like to submit our analysis of the Luxembourg structure of Continental Partners S&P. We would like to discuss this structure and provide us with your agreement and comments.

... is Limited ("HWL") is a Hong Kong listed company.

Ca

... if you could examine and provide us with Luxembourg tax treatment regarding the transaction with Hannon & Co as outlined in this letter.

... We would like to submit our analysis of the Luxembourg structure of Continental Partners S&P. We would like to discuss this structure and provide us with your agreement and comments on the tax treatment described herein.

... dated 12 July 2006, we would like to submit our analysis of the Luxembourg structure of Continental Partners S&P. We would like to discuss this structure and provide us with your agreement and comments on the tax treatment described herein.

Back to search results

Previous Next

Mark as recommended

1



Download

# H4201030M.pdf

- EXTRACTED TEXT
- PREVIEW
- TAGS & DETAILS
- NAMED ENTITIES**

## People (36)

- KOHL HUTCHISON LUXCO HUTCHISON KOHL PEETERS LUXCO LUXCO LUXCO LUXCO LUXCO WIM PIOT WIM PIOT
- MARIUS KOHL LUXEMBOURG HUTCHISON CONFIDENTIAL HUTCHISON ROBERT ECBRT ECKERT LUXELLBOURG ILCJB DINE AUMIAN SCHILLING
- ROBIO SNG DIRECTOR HUTCHISON HUTCHISON ROBERT ECKERT ECKERT HUTCHISON ROBIN DIRECTOR HUTCHISON HUTCHISON ROBERT
- HUTCHISON HUTOHLSA DILLION ROBIN ROBERT ECKERT ECKERT HUTCHISON

Extracted using CORENLP in ENGLISH

...tria, the fiscal value of LuxCo's

participation in H3G Holdings should consist of its acquisition price, increased by the

amounts granted by LuxCo to H3G Austria. The total amount of these contributions will

## Organizations (52)

- MR PEETERS ADMINISTRATION DES CONTR
- LUXEMBOURG TELEPHONE HUTCHISON
- HUTCHISON WHAMPOA LIMITED AUSTR
- R.C. LUXEMBOURG BUREAU D'IMPOSITIO
- RMS/VLN/H4201030M-WPIHUTCHISON WH
- HUTCHISON WHAMPOA LIMITED HUTCH
- H3G HOLDINGS R.C. LUXEMBOURG B LUXCO LUXCO H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS LUX CO LUXCO LUXCO
- H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS HUTCHISON 3G AUSTRIA INVESTMENTS S.A.R.L HUTCHISON 3G AUSTRIAGMBH
- AUSTRIA INVESTMENTS S.A.R.L. HDTCHISON 3G AUSTRIA GMBH HUTCHISON AUSTRIA INVESTMENTS YHUTCHISON 3G AUSTRIA INVESTMENTS
- HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA HOLDINGS HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA GMBH FCBRUAR
- AUSTRIA GMBH AUSRIA INVESTMENTS S.A.R.L. HUTCHISON 3G AUSTRALIA HOLDINGSGMBH HUTCHISON 3G AUSTRIA GMBH

## Locations (61)

- EUROPE AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG EUROPE AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA ILL AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- LUXEMBOURG AUSTRIA AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG LUXEMBOURG
- AUSTRIA AUSTRIA EUROPE AUSTRIA VIENNA AUSTRIA HATCBISOO AUSTRIA AUSTRIA EUROPE JC LUXEMBOURG VIENNA

Show more locations

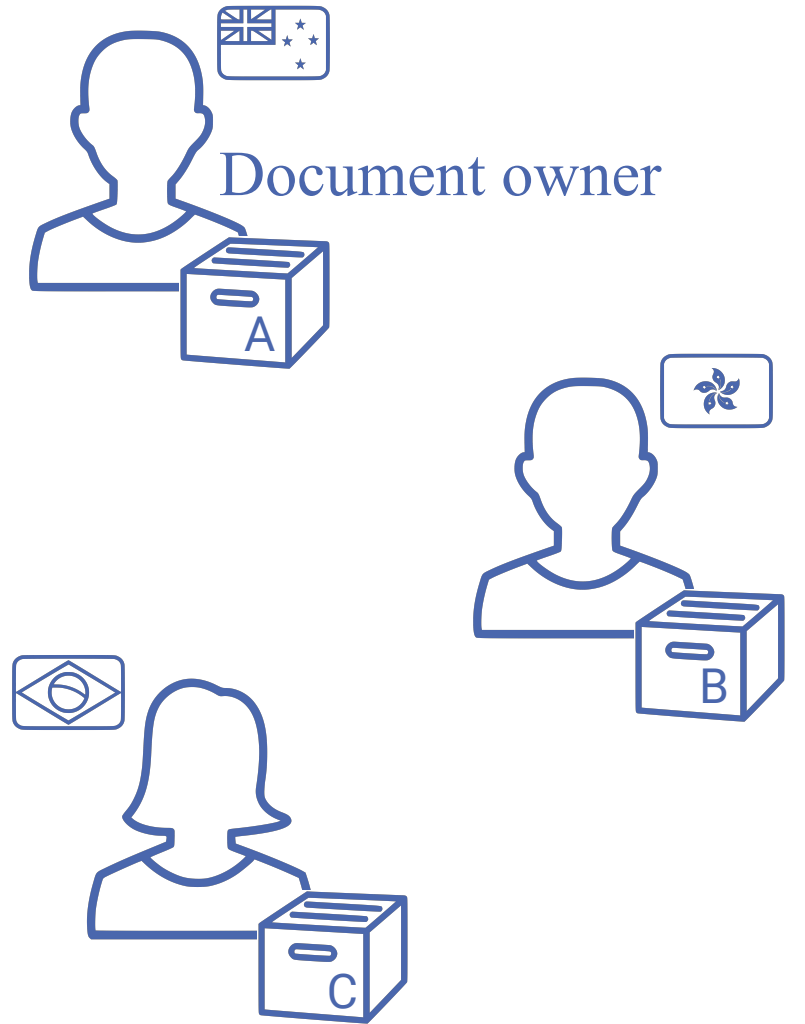
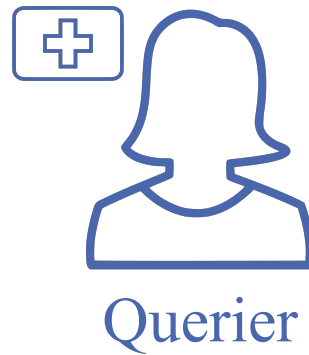


# DatashareNetwork



Journalist ↔ Journalist  
search

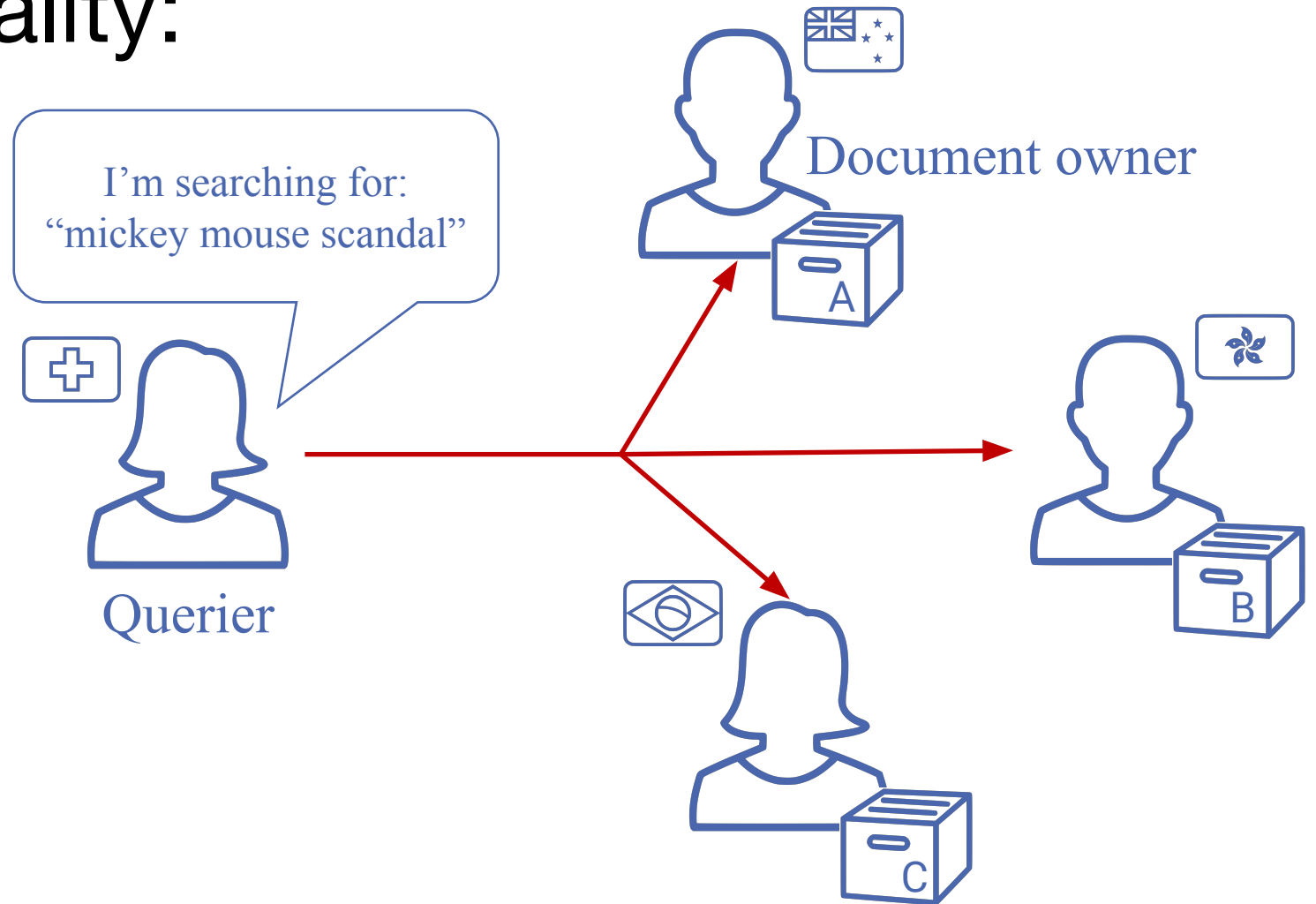
# Needed functionality:



# Needed functionality:



Search



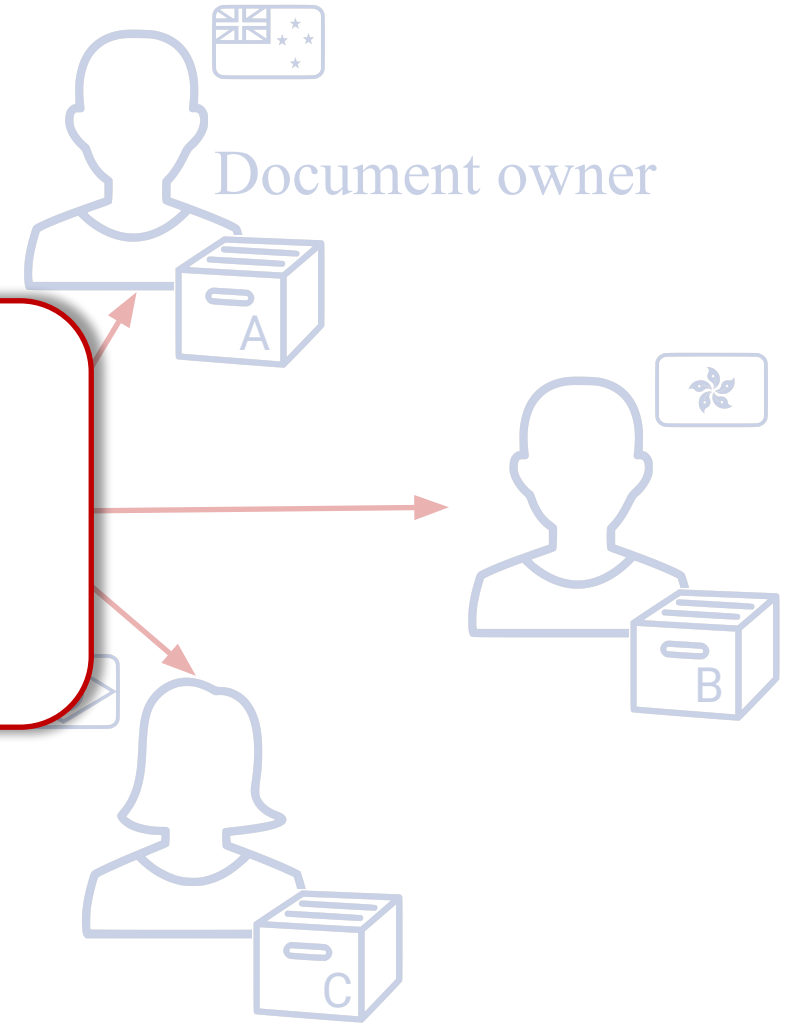
# Needed functionality:



Search

I'm searching for:  
"mickey mouse scandal"

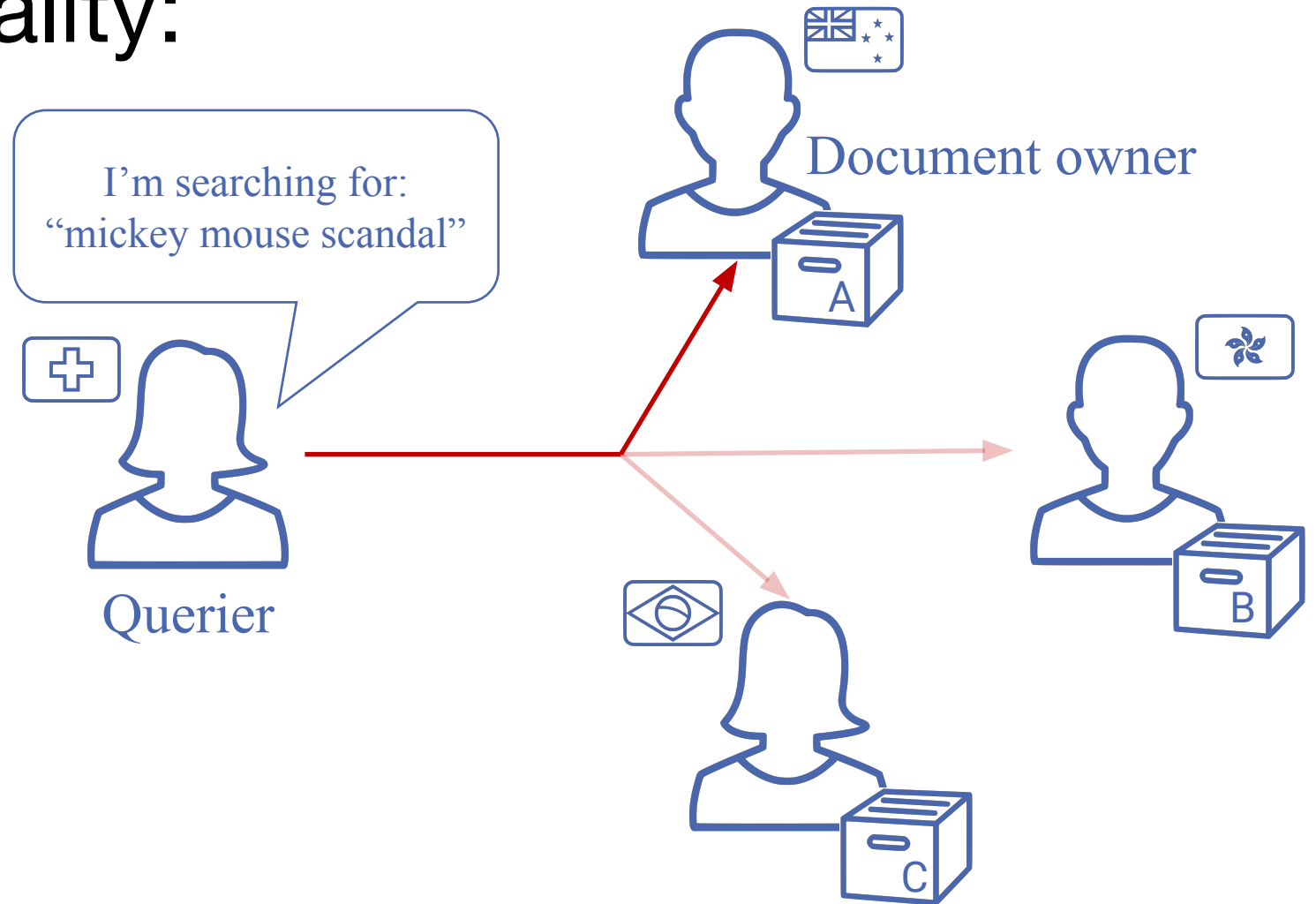
Does another journalist have  
documents relevant to my  
investigation?



# Needed functionality:



Search



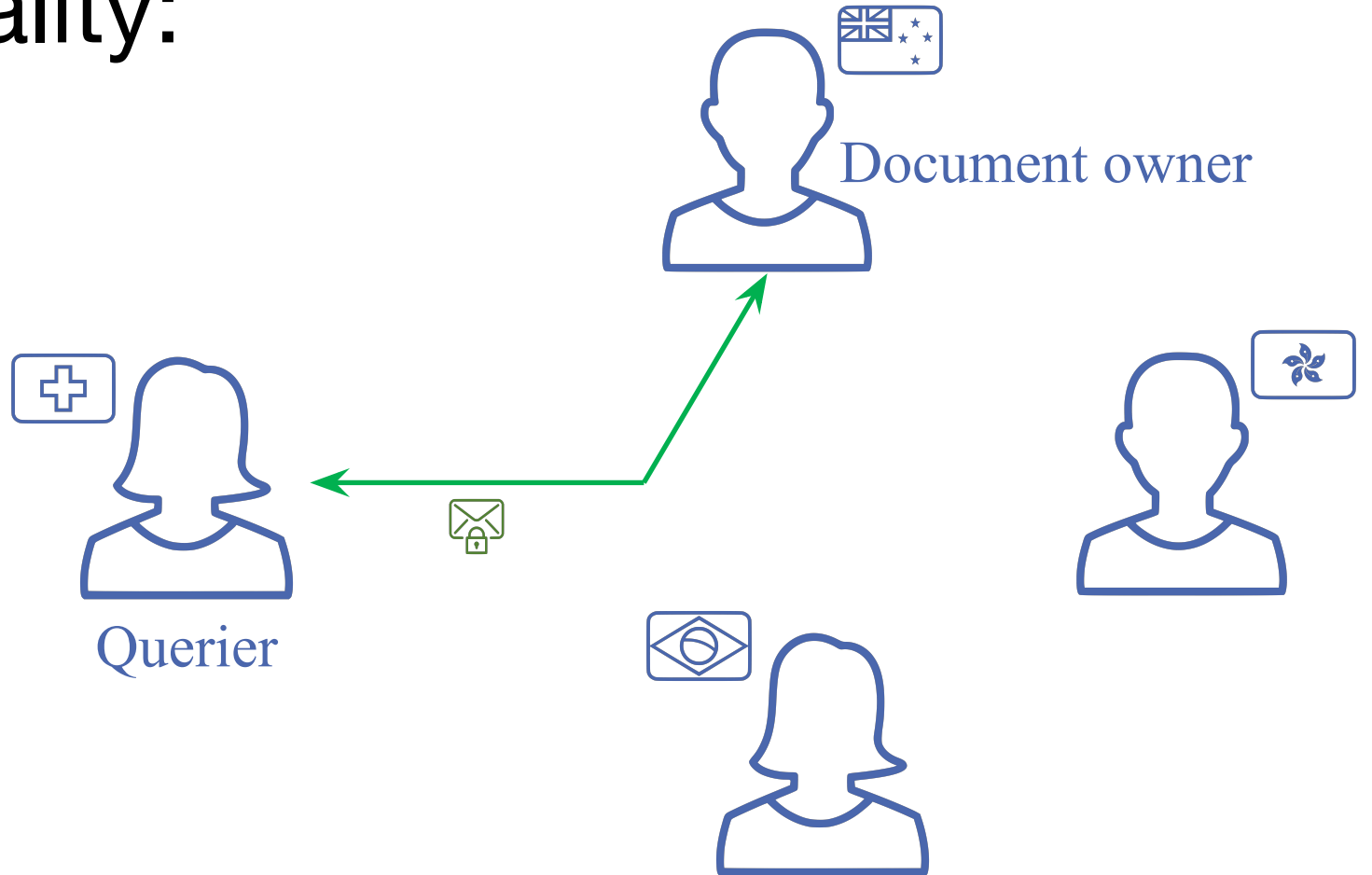
# Needed functionality:



Search



Contact





# Needed functionality:



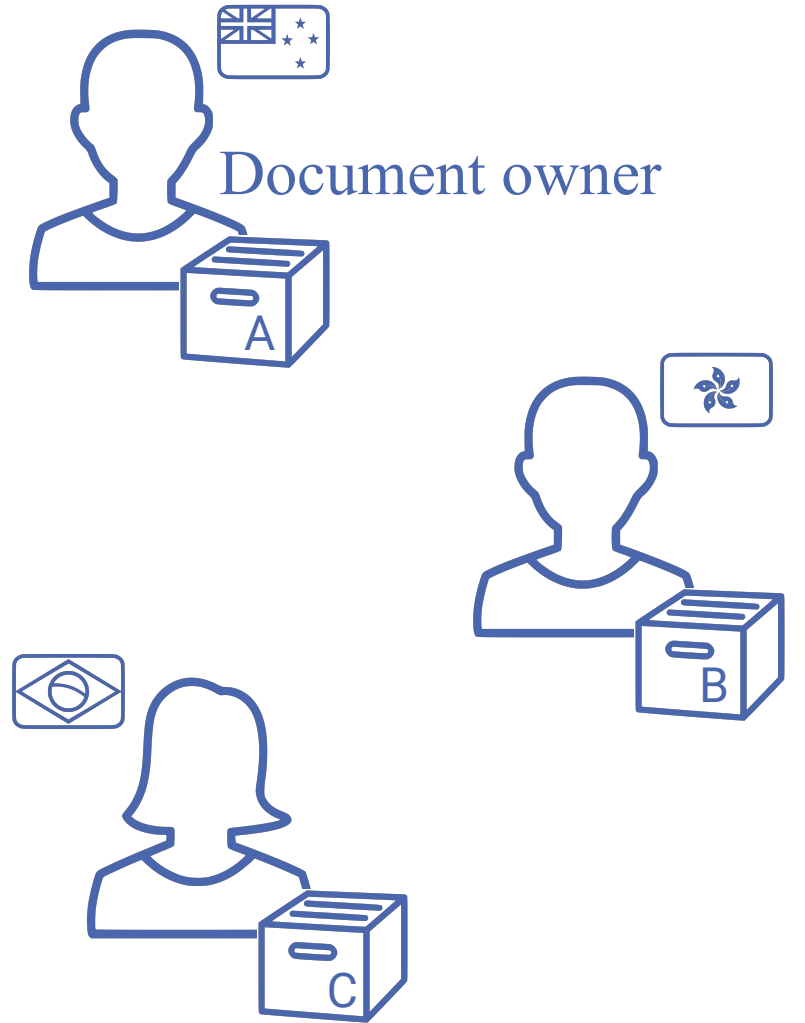
Search



Contact



No retrieval



# Survey: threat model



Journalists



ICIJ



Third party

# Survey: threat model



Journalists



ICIJ



Third party



# Survey: threat model



Journalists



ICIJ



Third party



# Survey: threat model



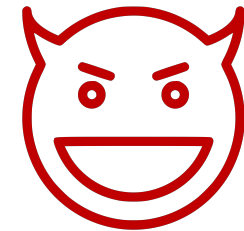
Journalists



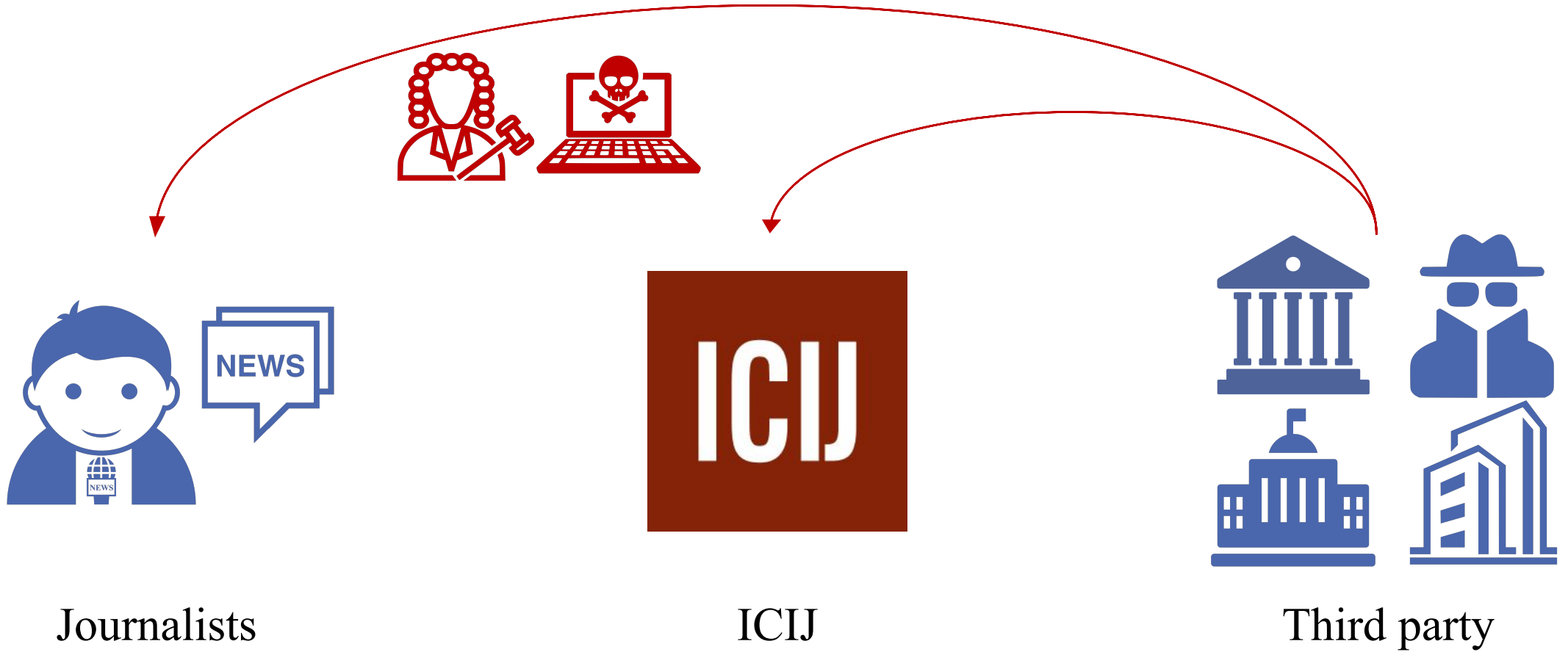
ICIJ



Third party



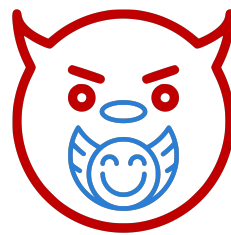
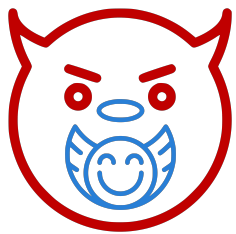




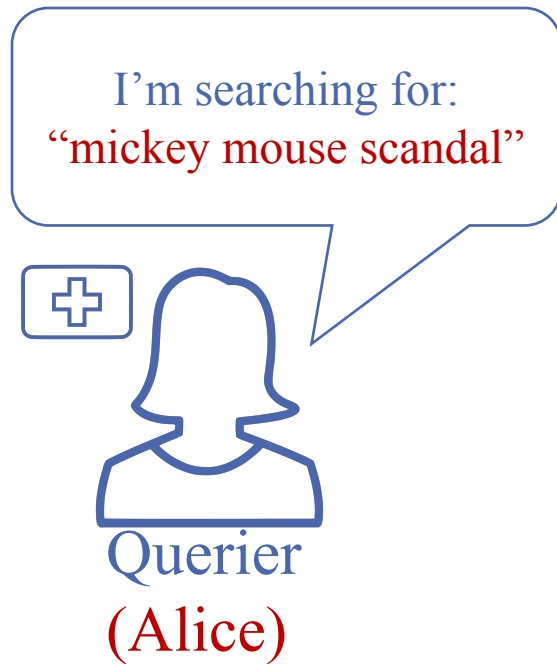
Journalists

ICIJ

Third party



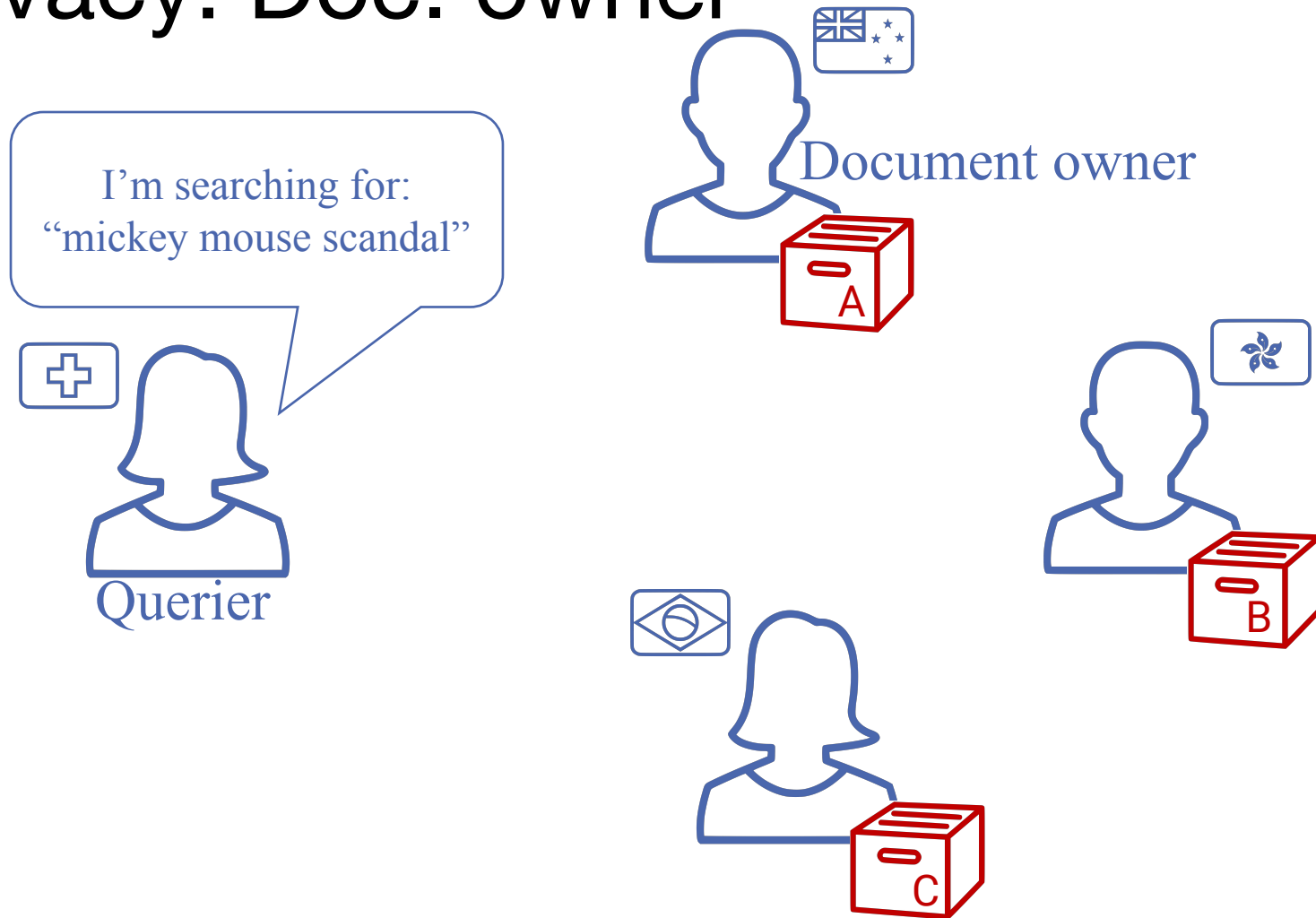
# Privacy: querier



- Protect:
- The query
  - The querier's identity



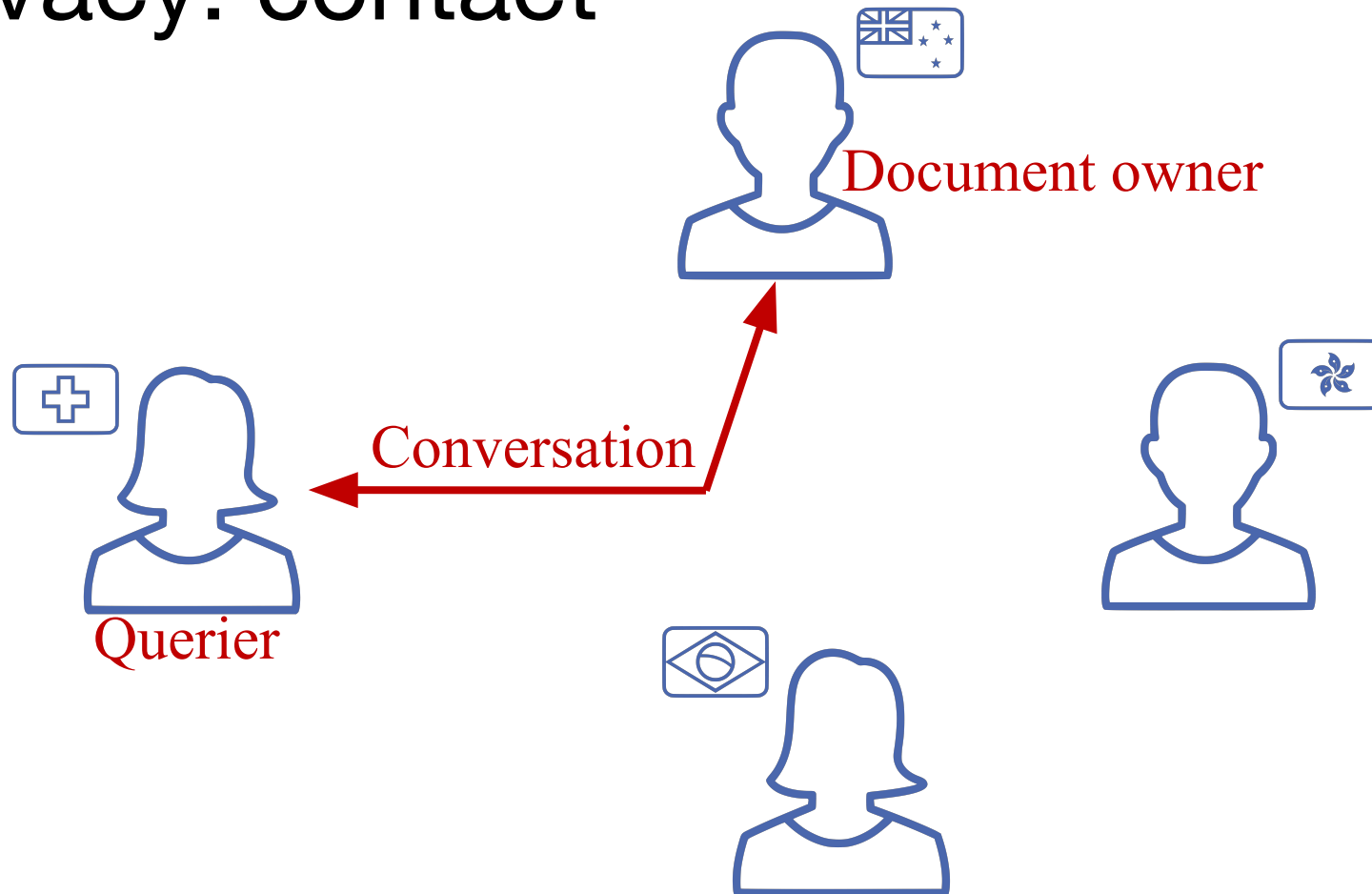
# Privacy: Doc. owner



Protect:

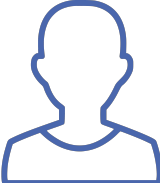
- The documents

# Privacy: contact

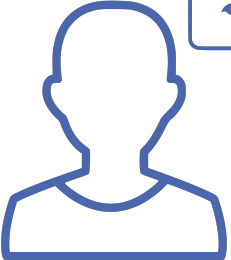
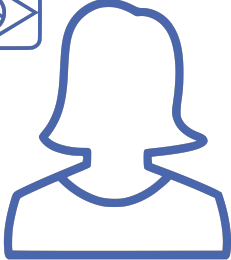
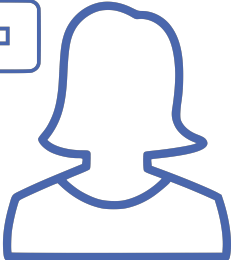


- Protect:
- The content of conversation
  - The existence of conversation

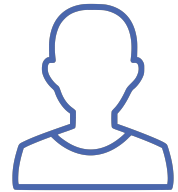
# Constraints



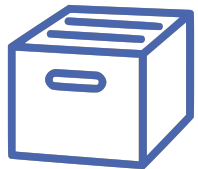
1000 journalists



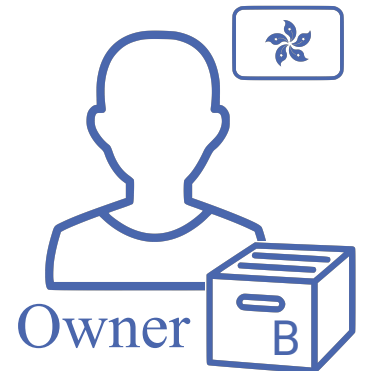
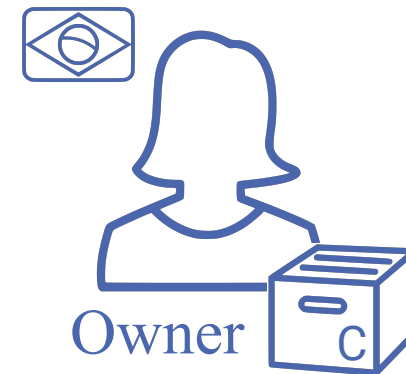
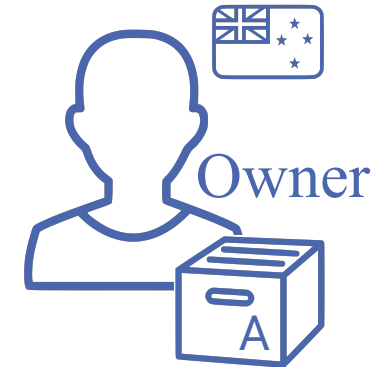
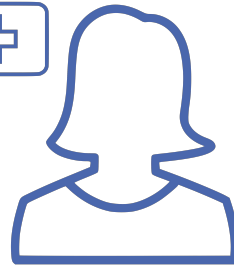
# Constraints



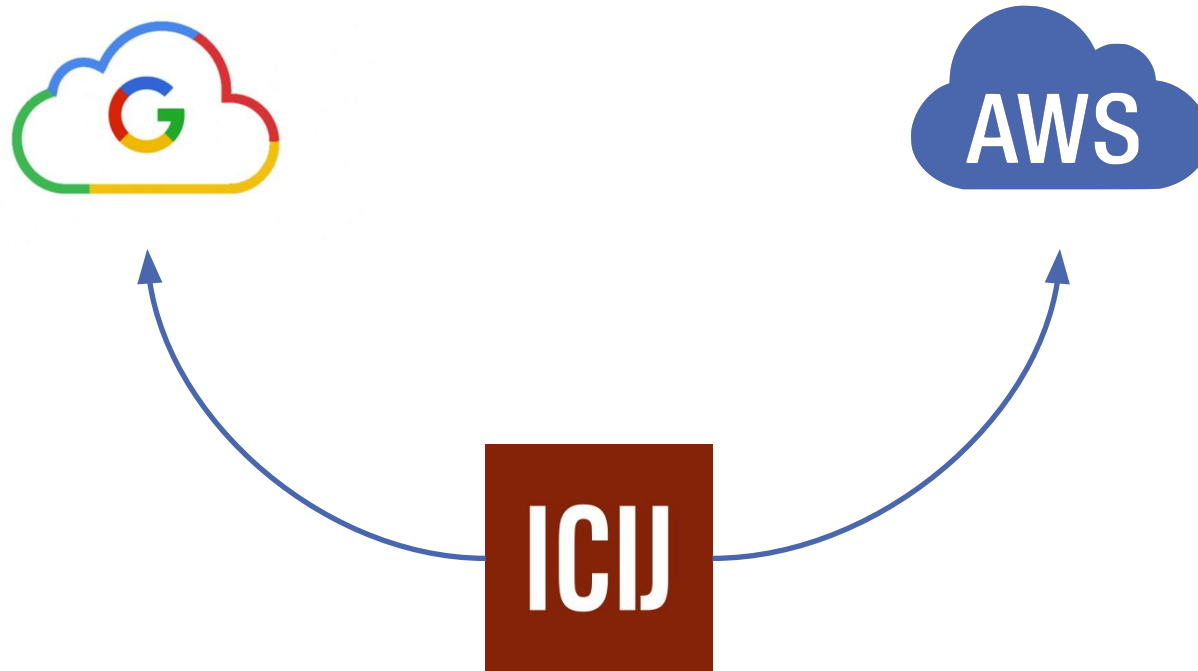
1000 journalists



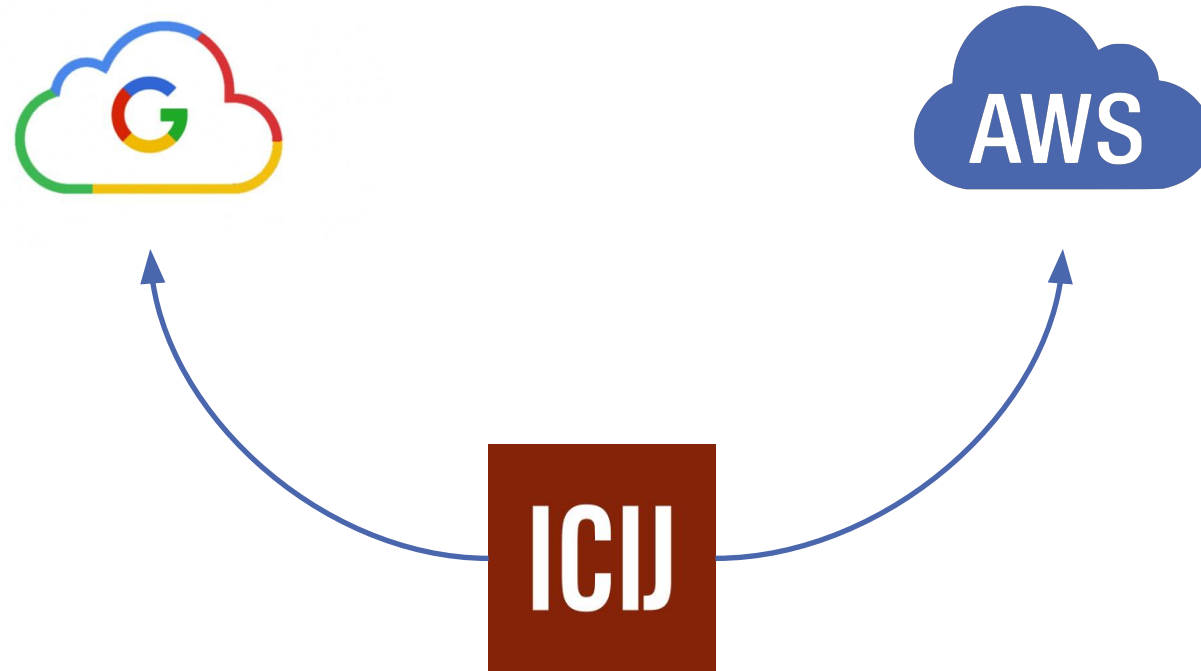
1000 documents  
per journalist



# Real-world constraints: decentralization

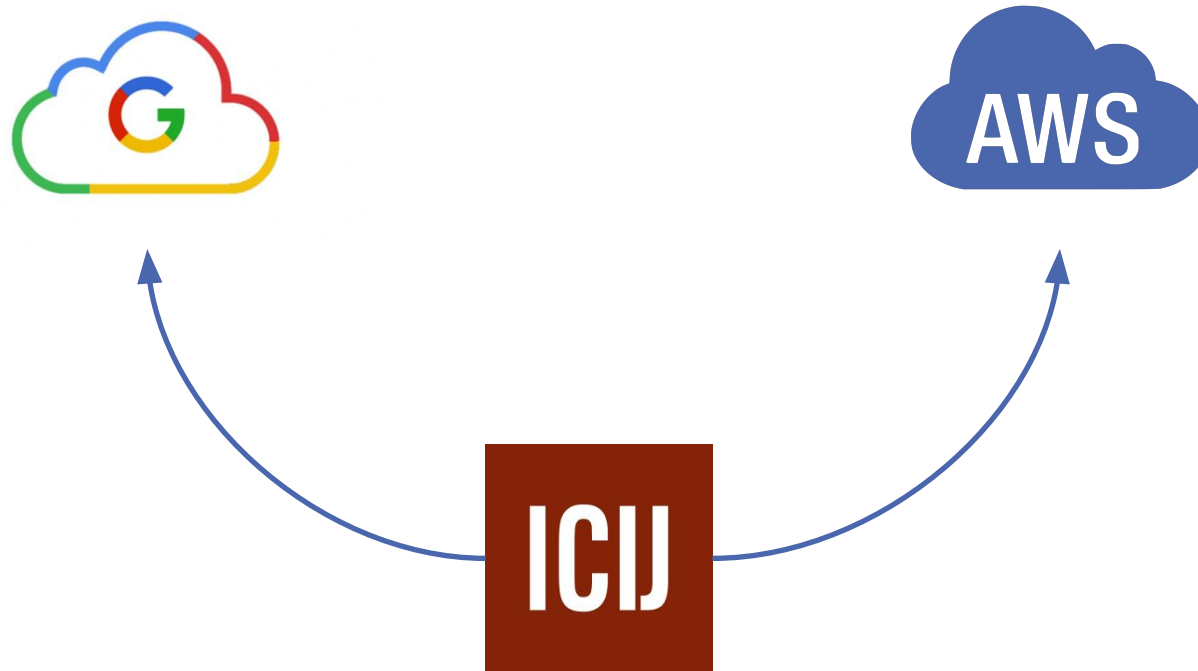


# Real-world constraints: decentralization



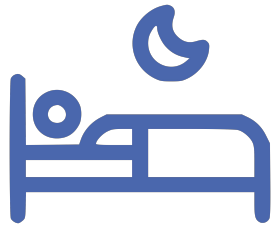
Decentralized  
~~Any-trust~~

# Real-world constraints: decentralization



~~Decentralized~~  
~~Any-trust~~  
~~Trusted 3<sup>rd</sup> party~~

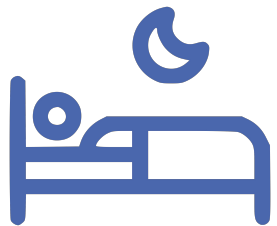
# Real-world constraints: asynchrony



~~Decentralized~~  
~~Any-trust~~  
~~Trusted 3<sup>rd</sup> party~~



# Real-world constraints: asynchrony



~~Decentralized~~  
~~Any-trust~~  
~~Trusted 3<sup>rd</sup> party~~  
~~SMC (multi-round)~~  
MPC

# Real-world constraints: communication



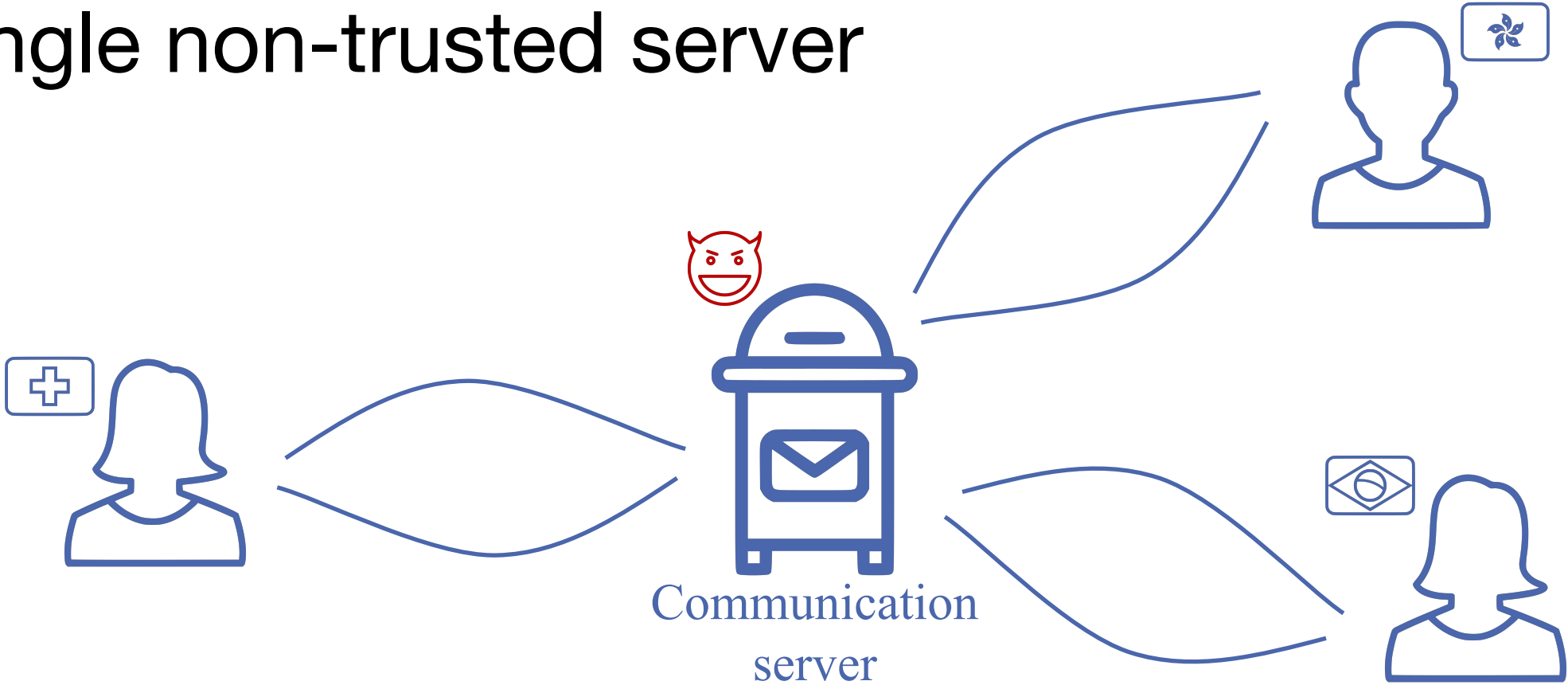
~~Decentralized~~  
~~Any-trust~~  
~~Trusted 3<sup>rd</sup> party~~  
~~SMC (multi-round)~~  
MPC

# Real-world constraints: communication

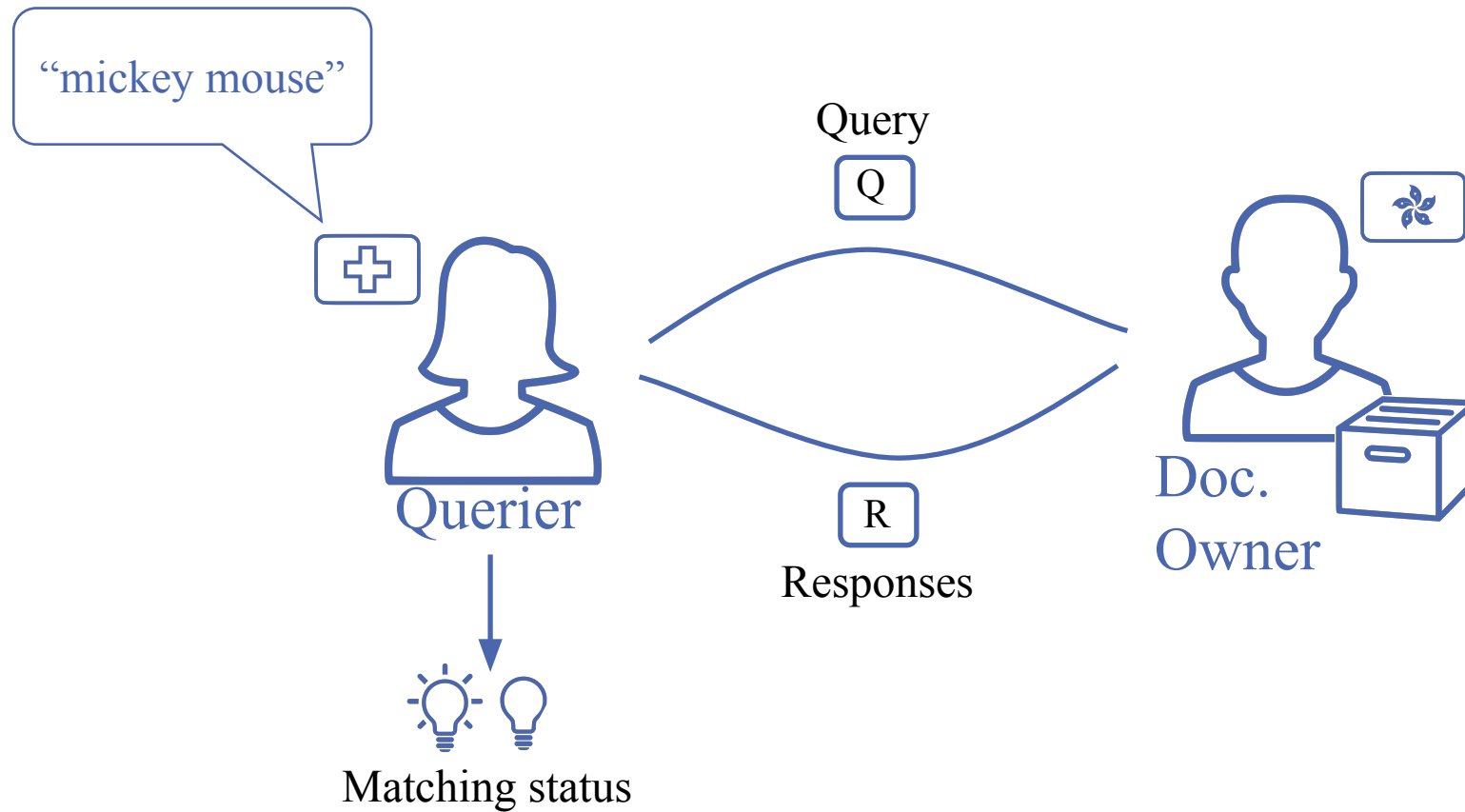


~~Decentralized~~  
~~Any-trust~~  
~~Trusted 3<sup>rd</sup> party~~  
~~SMC (multi-round)~~  
MPC  
Circuits  
FHE

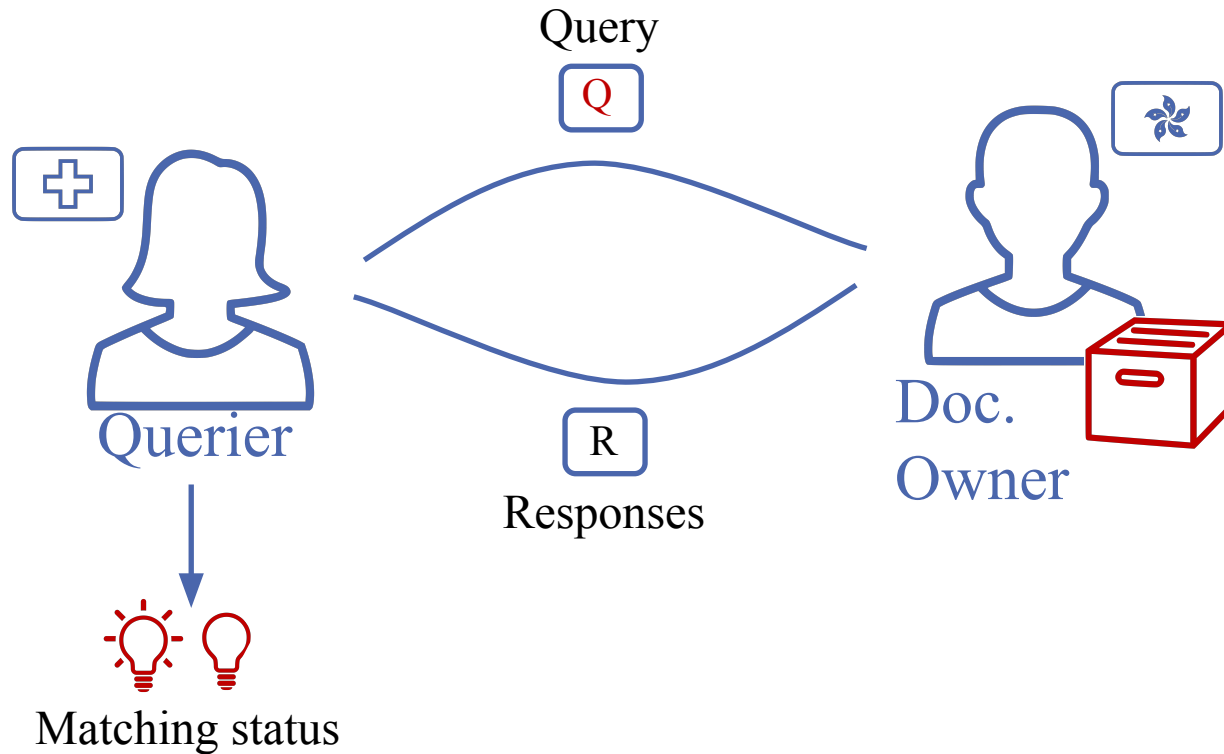
# Single non-trusted server



# Document search



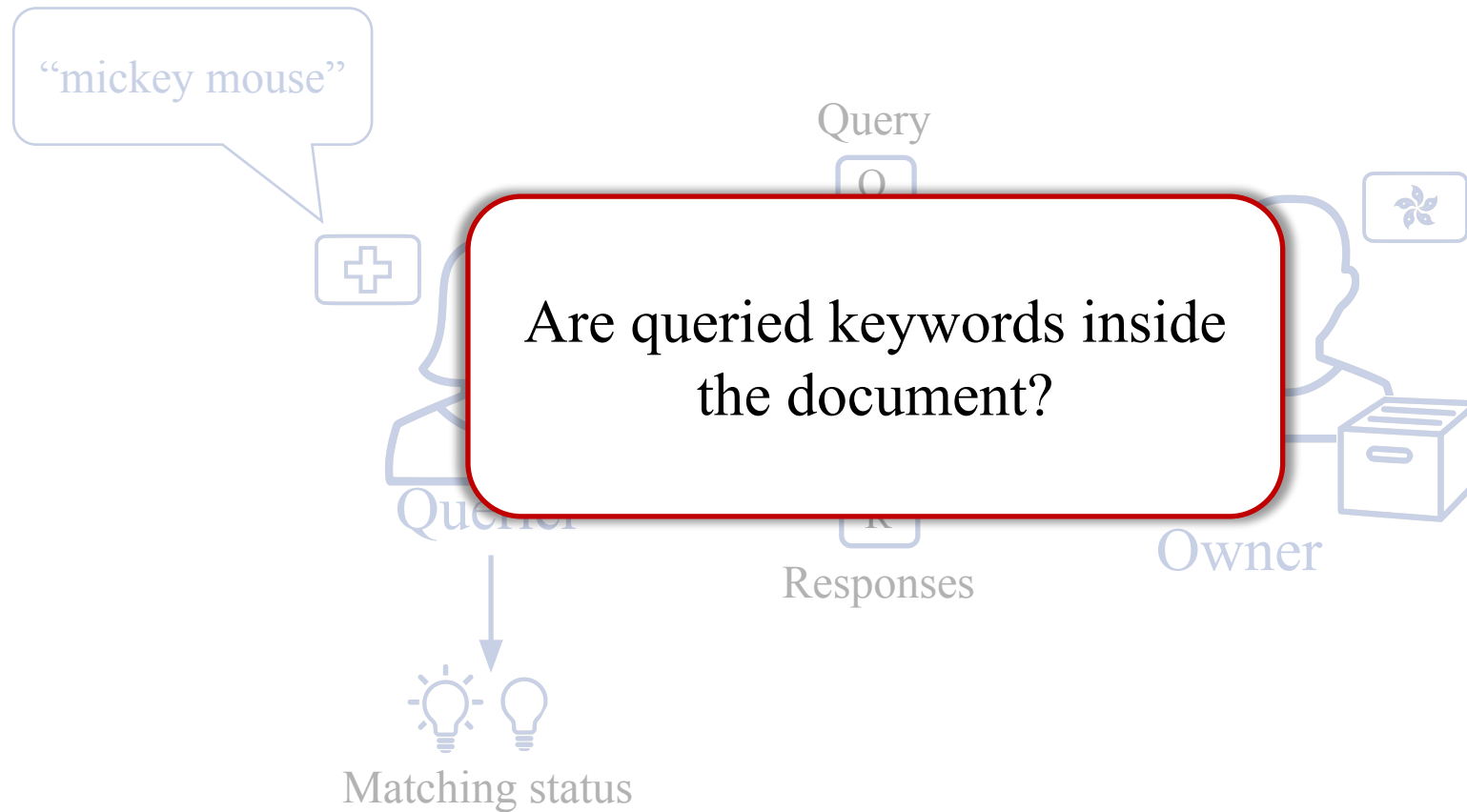
# Document search: privacy recap



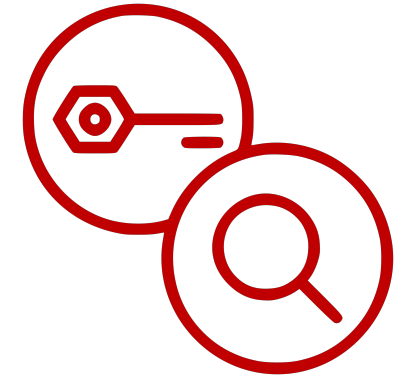
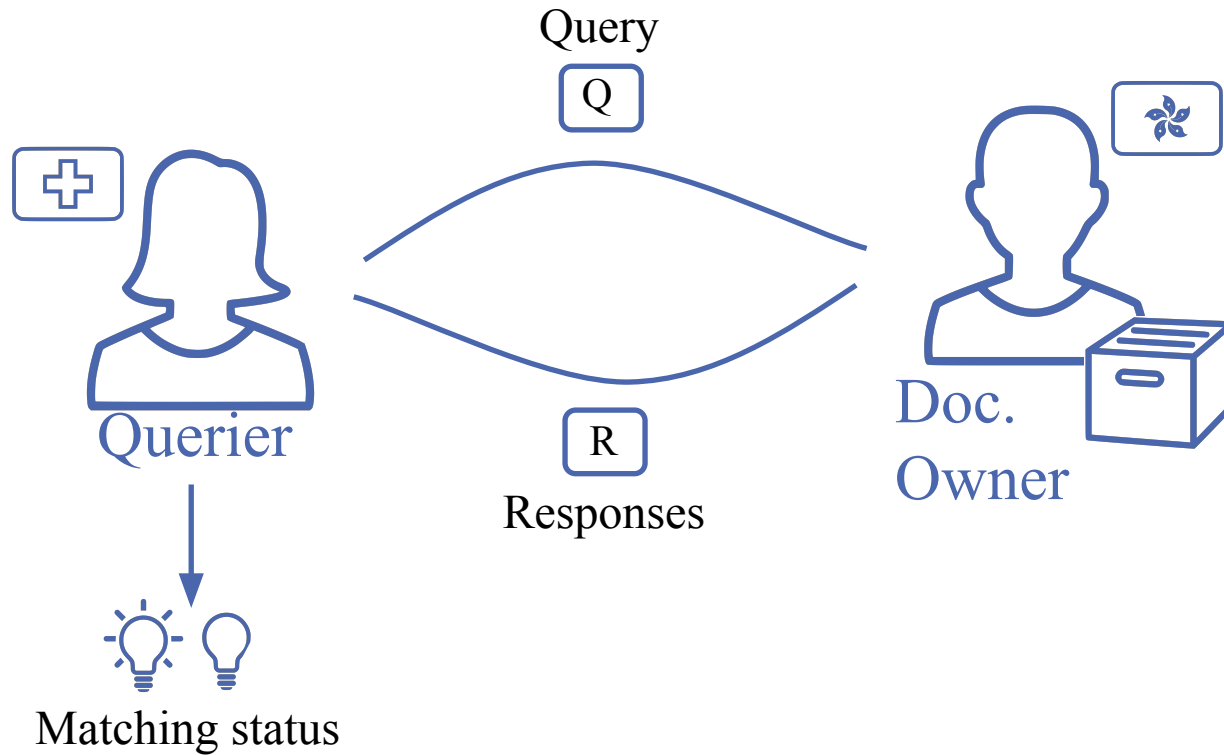
## Protect:

- The query
- The documents
- The result

# Document search



# Document search



Multiset private  
set intersection



# Private Set Intersection (PSI)



Alice

Input:  
 $\{q_1, \dots, q_m\}$

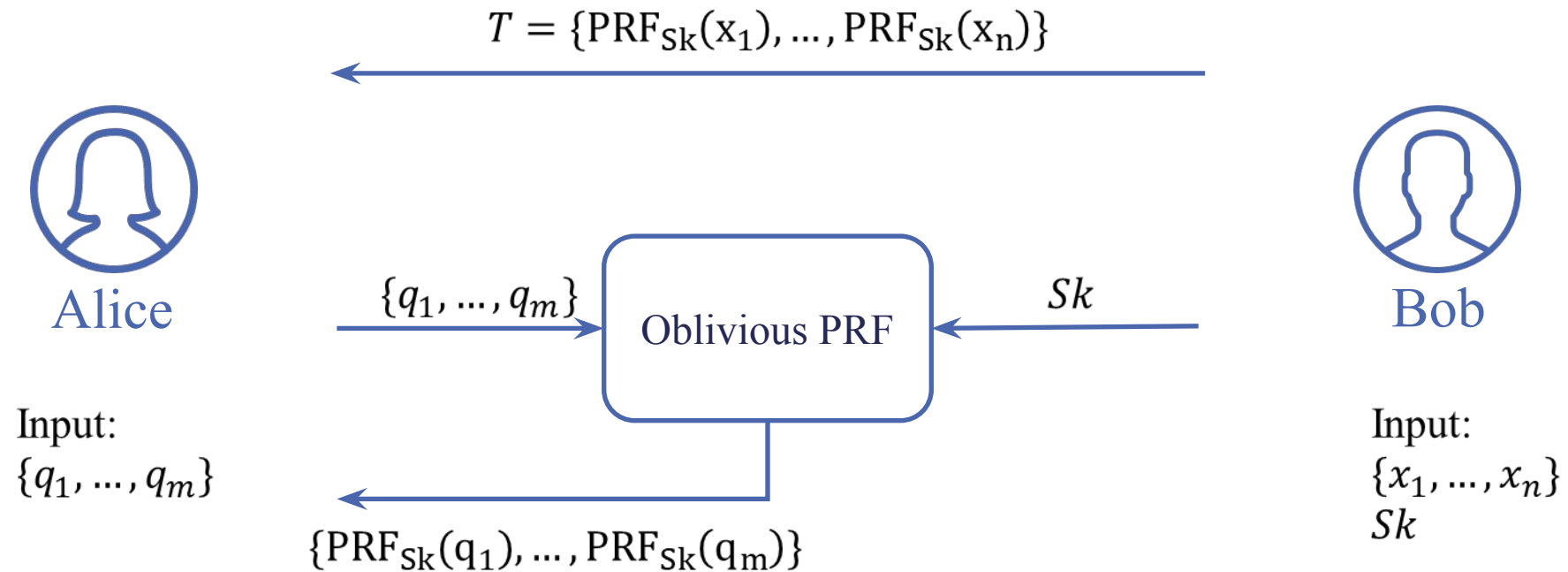
$T = \{\text{PRF}_{sk}(x_1), \dots, \text{PRF}_{sk}(x_n)\}$



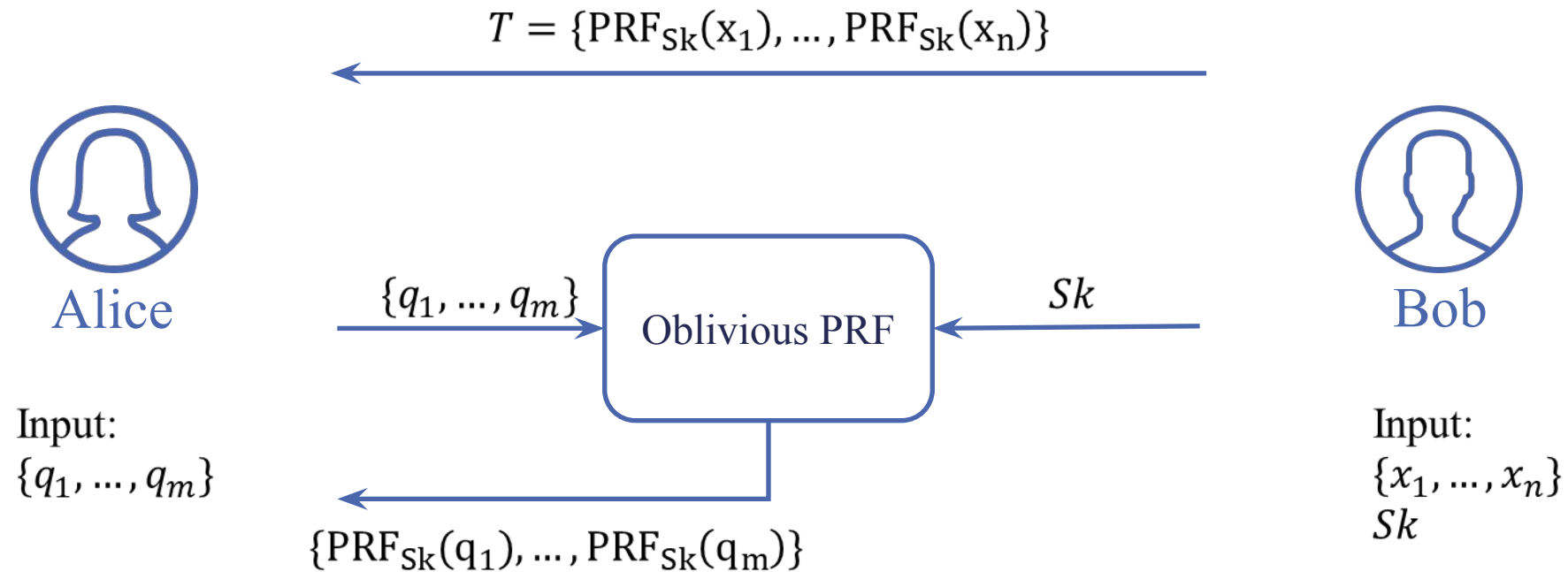
Bob

Input:  
 $\{x_1, \dots, x_n\}$   
 $Sk$

# Private Set Intersection (PSI)



# Private Set Intersection (PSI)



$$I = T \cap \{PRF_{Sk}(q_i)\}$$

---

		Querier comp.	Comm.	Owner comp.
PSI	1 Document	2 ms	3.84 KB	11 ms

---

Setting:

#keyword per document: 100

#keyword per query: 10

Performance:

Time(hash) =  $1\mu\text{s}$

Time(exp) =  $100\mu\text{s}$

		Querier comp.	Comm.	Owner comp.
PSI	1 Document	2 ms	3.84 KB	11 ms
	1000 Documents	2 sec	3.84 MB	11 sec

Setting:

#keyword per document: 100

#keyword per query: 10

Performance:

Time(hash) =  $1\mu s$

Time(exp) =  $100\mu s$

		Querier comp.	Comm.	Owner comp.
PSI	1 Document	2 ms	3.84 KB	11 ms
	1000 Documents	2 sec	3.84 MB	11 sec
	1000 Journalists	<b>33 min</b>	<b>3.84 GB</b>	-

Setting:

#keyword per document: 100

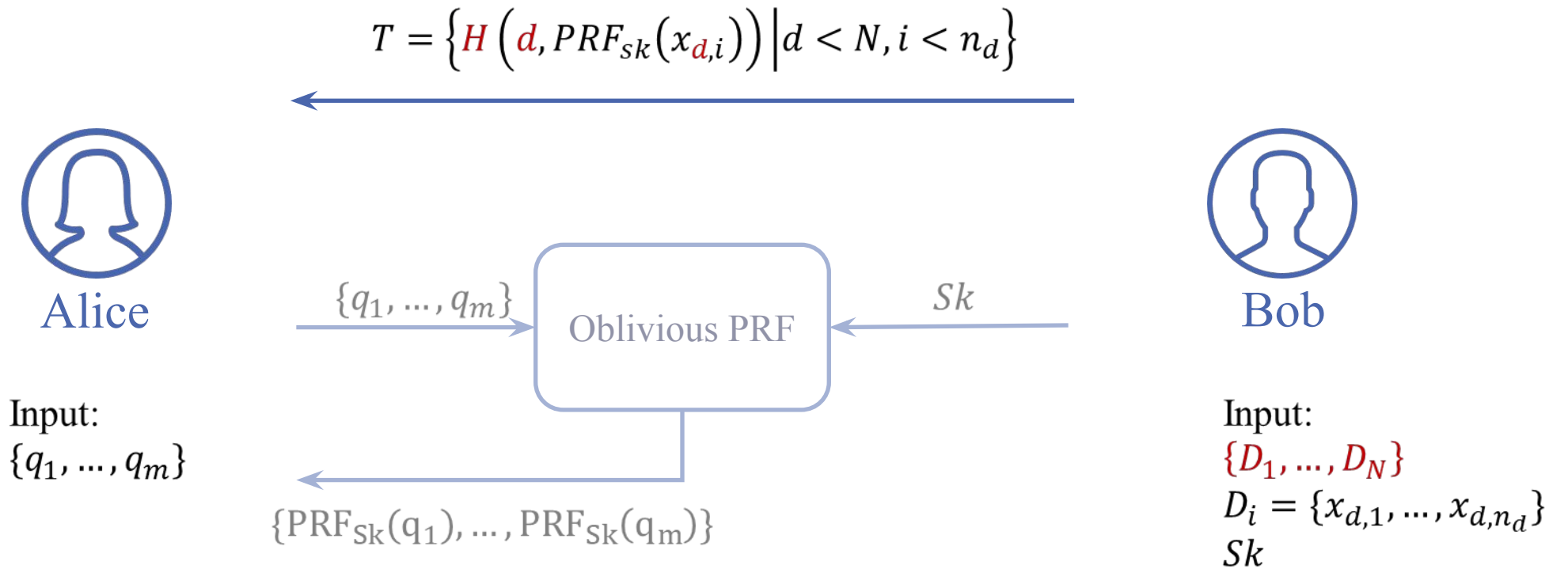
#keyword per query: 10

Performance:

Time(hash) =  $1\mu s$

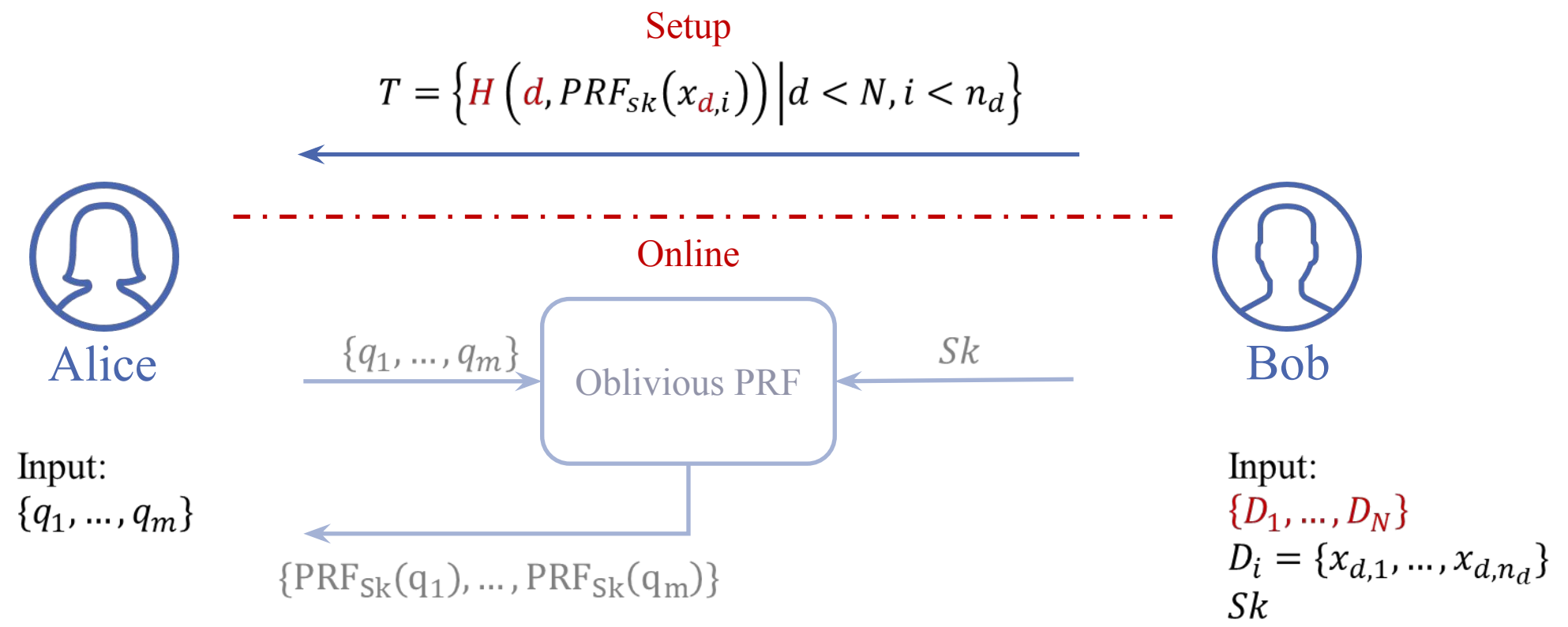
Time(exp) =  $100\mu s$

# Multiset Private Set Intersection (MS-PSI)



$$I_d = T \cap \{H(d, PRF_{sk}(q_i))\}$$

# Multiset Private Set Intersection (MS-PSI)



$$I_d = T \cap \{H(d, PRF_{sk}(q_i))\}$$



		Querier comp.	Comm.	Owner comp.
PSI	1 Document	2 ms	3.84 KB	11 ms
	1000 Documents	2 sec	3.84 MB	11 sec
	1000 Journalists	<b>33 min</b>	<b>3.84 GB</b>	-
MS-PSI (online)	1 Journalist	12 ms	640 B	1 ms
	1000 Journalists	<b>12 sec</b>	<b>640 KB</b>	-
MS-PSI (setup)	1 Journalist	-	200 KB	1 ms
	1000 Journalists	-	200 MB	-

Setting:

#keyword per document: 100

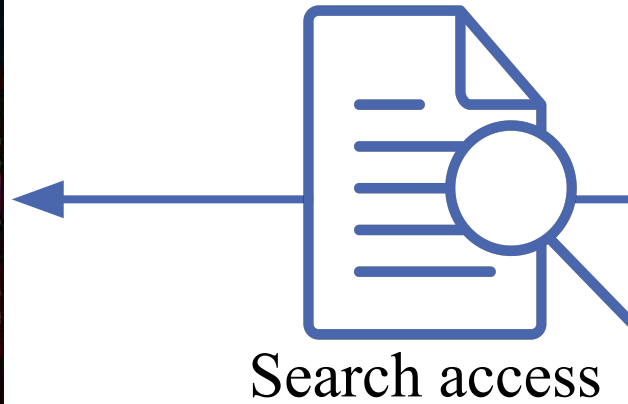
#keyword per query: 10

Performance:

Time(hash) =  $1\mu s$

Time(exp) =  $100\mu s$

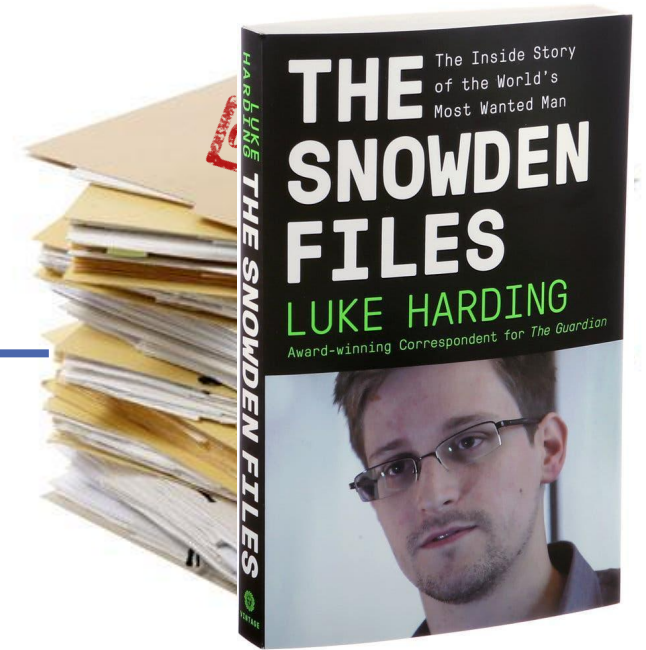
# Privacy: a new (stronger) setting

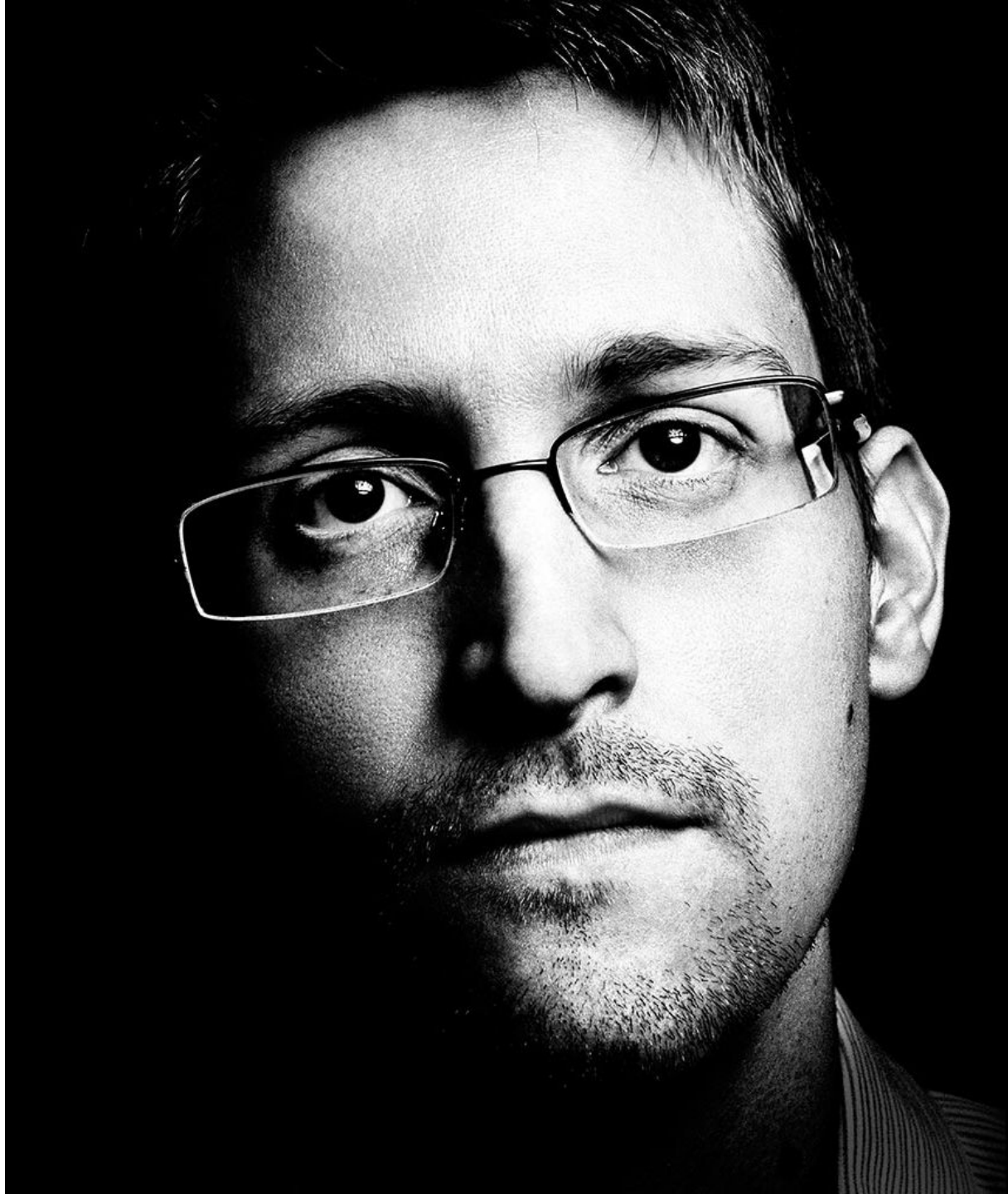


# Can we hide the existence of Snowden leaks?



Search access

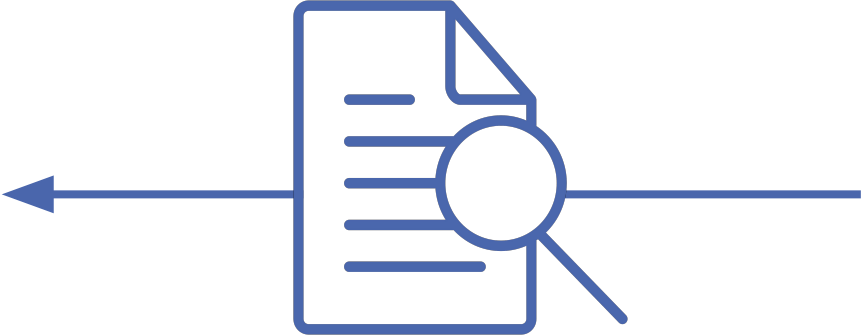




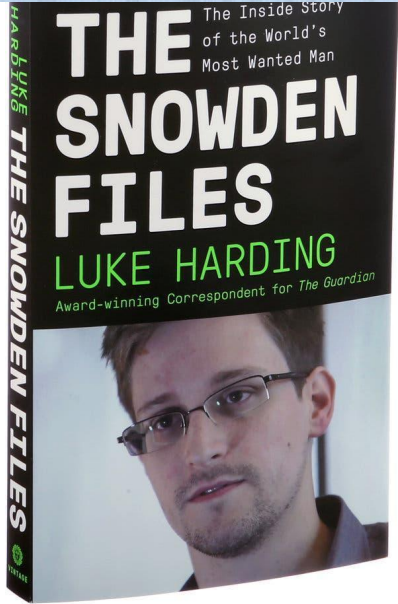
*“lol no”*

-Edward Snowden

# Can we hide the existence of Snowden leaks?



Search access

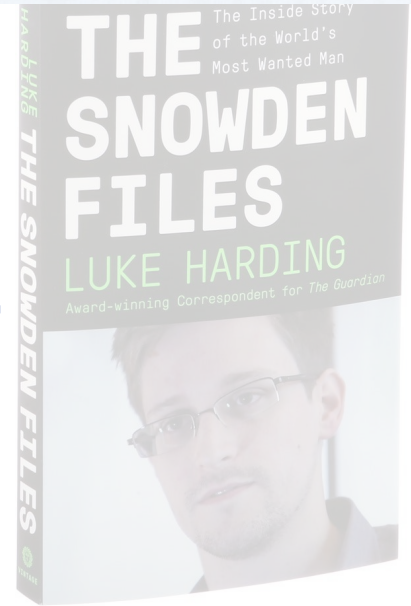


# Can we hide the existence of Snowden leaks?

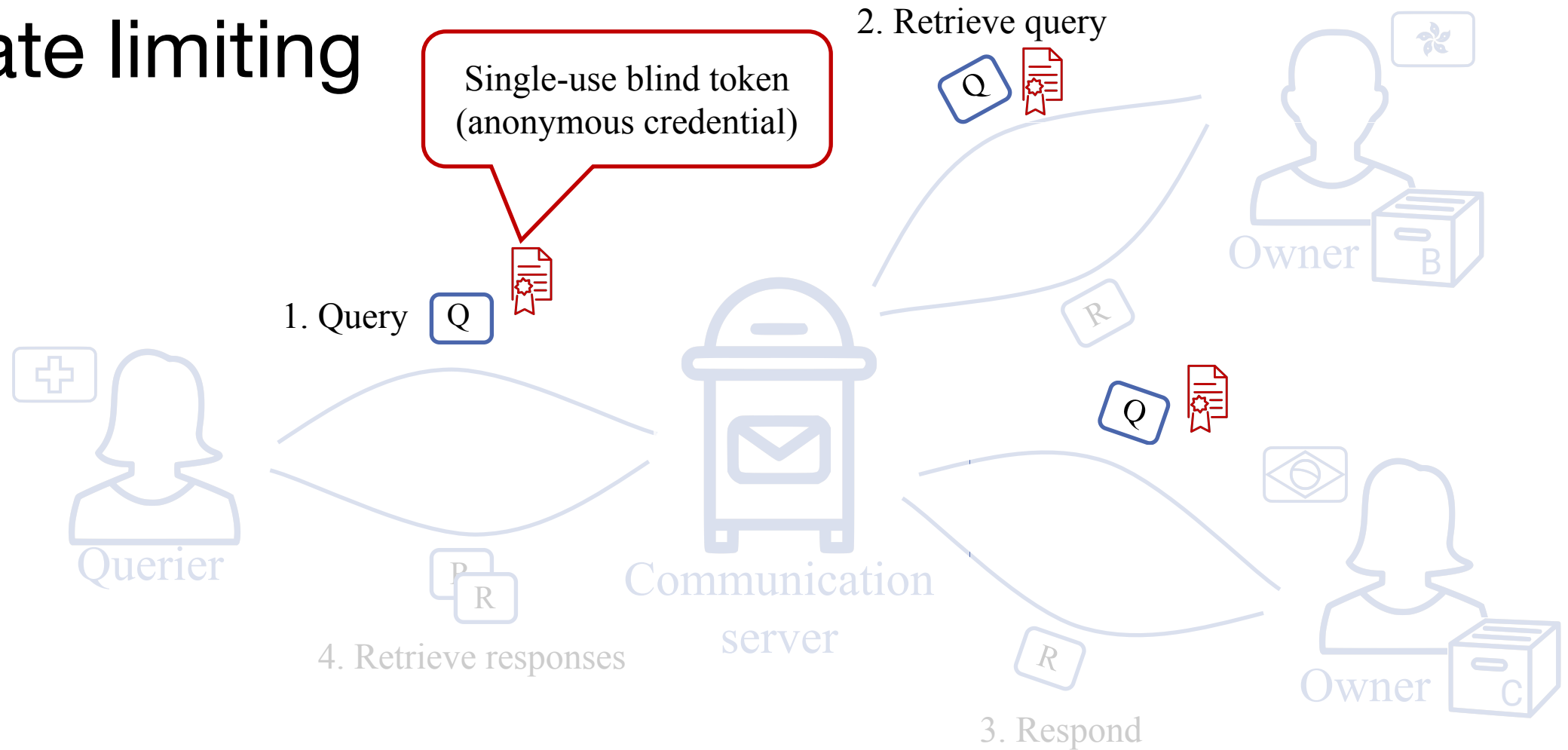


Prevent extracting all keywords from documents?

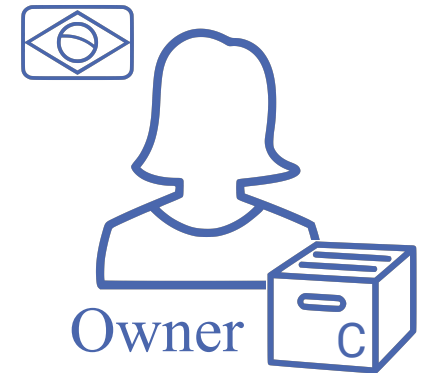
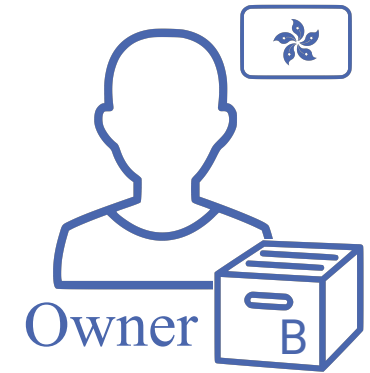
Search access



# Rate limiting

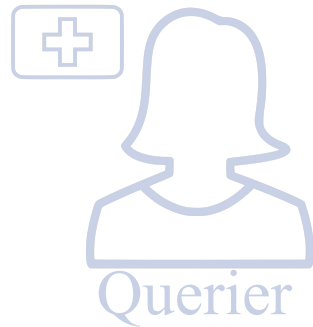


# Enable contact



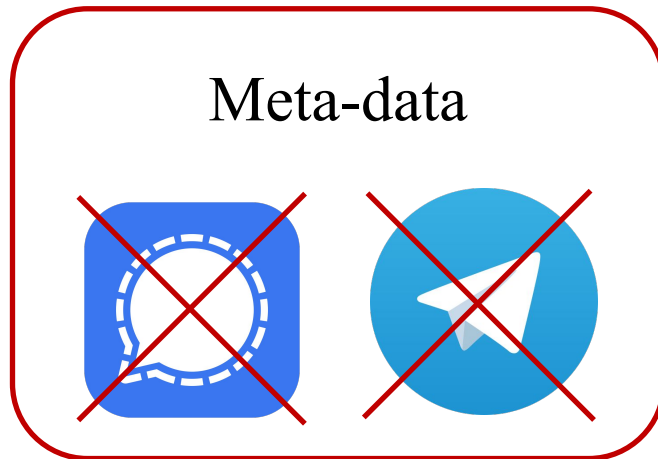


# Enable Contact



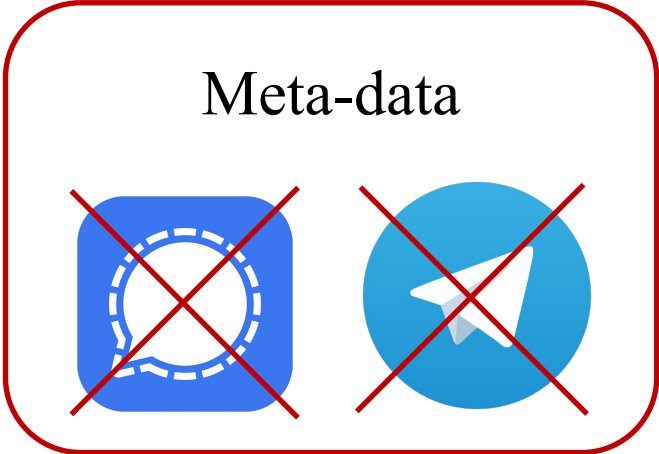
# Why not use existing systems?

# Why not use existing systems?



# Why not use existing systems?

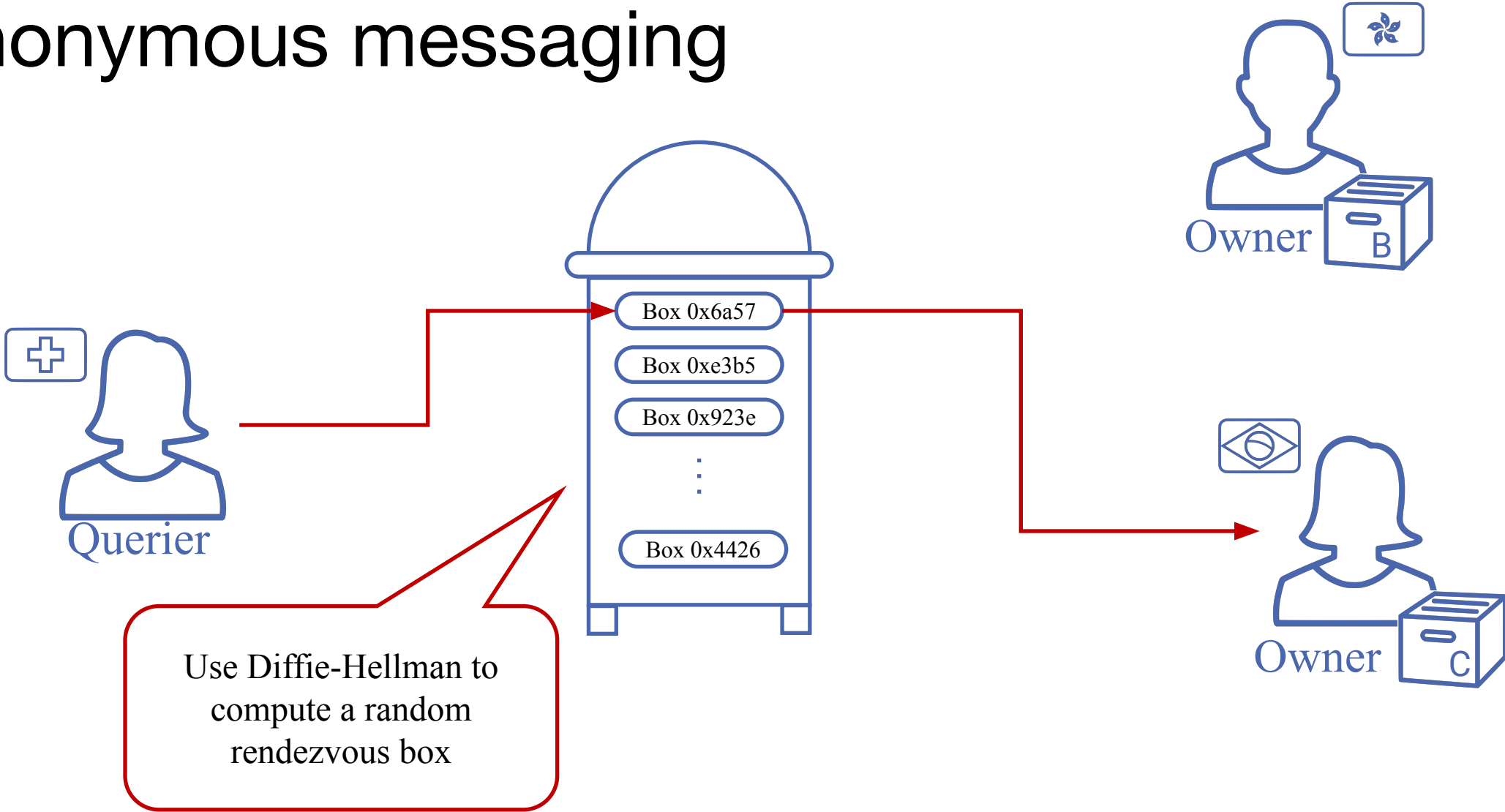
Meta-data



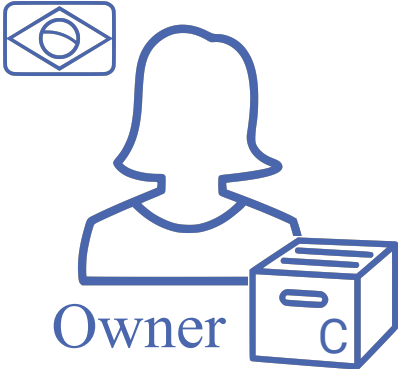
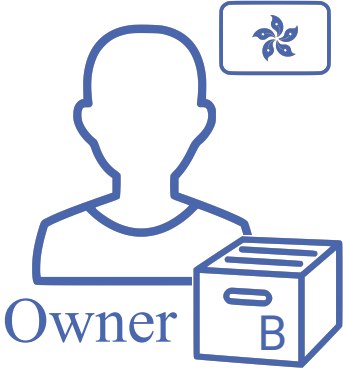
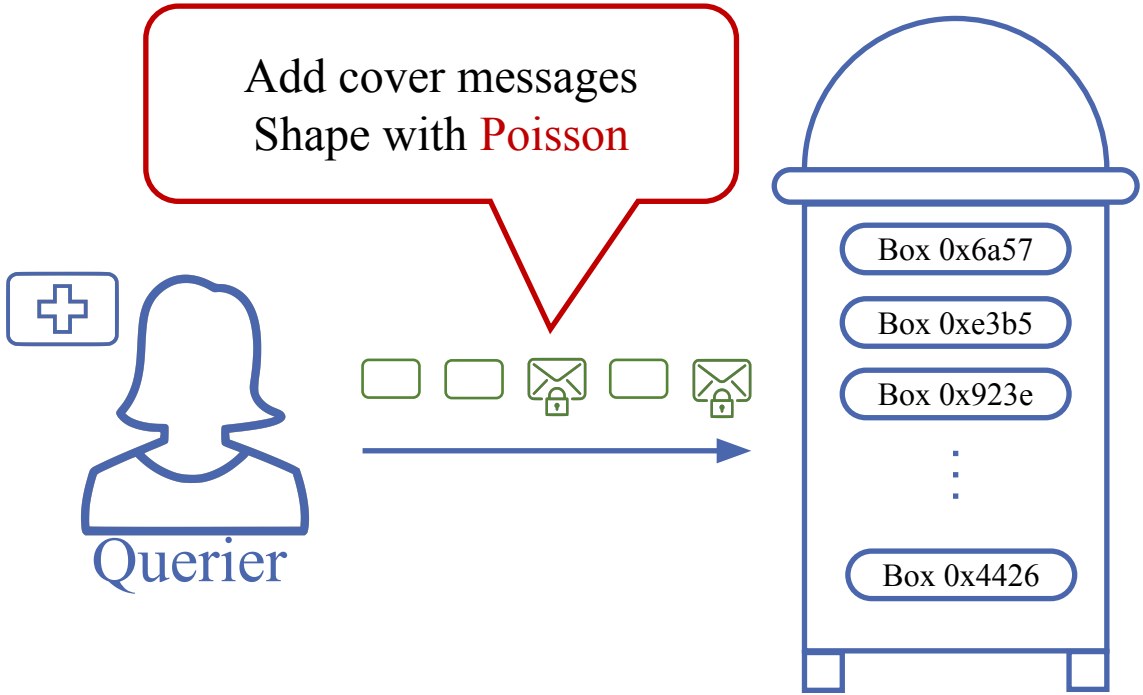
Asynchrony



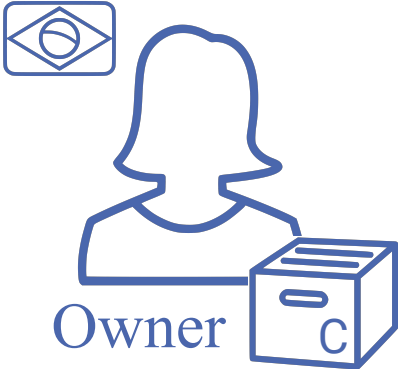
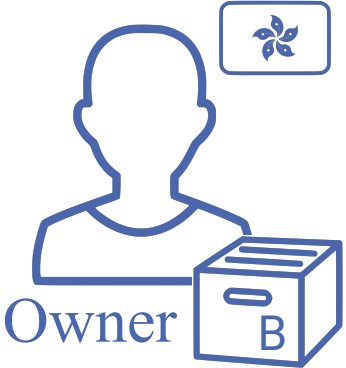
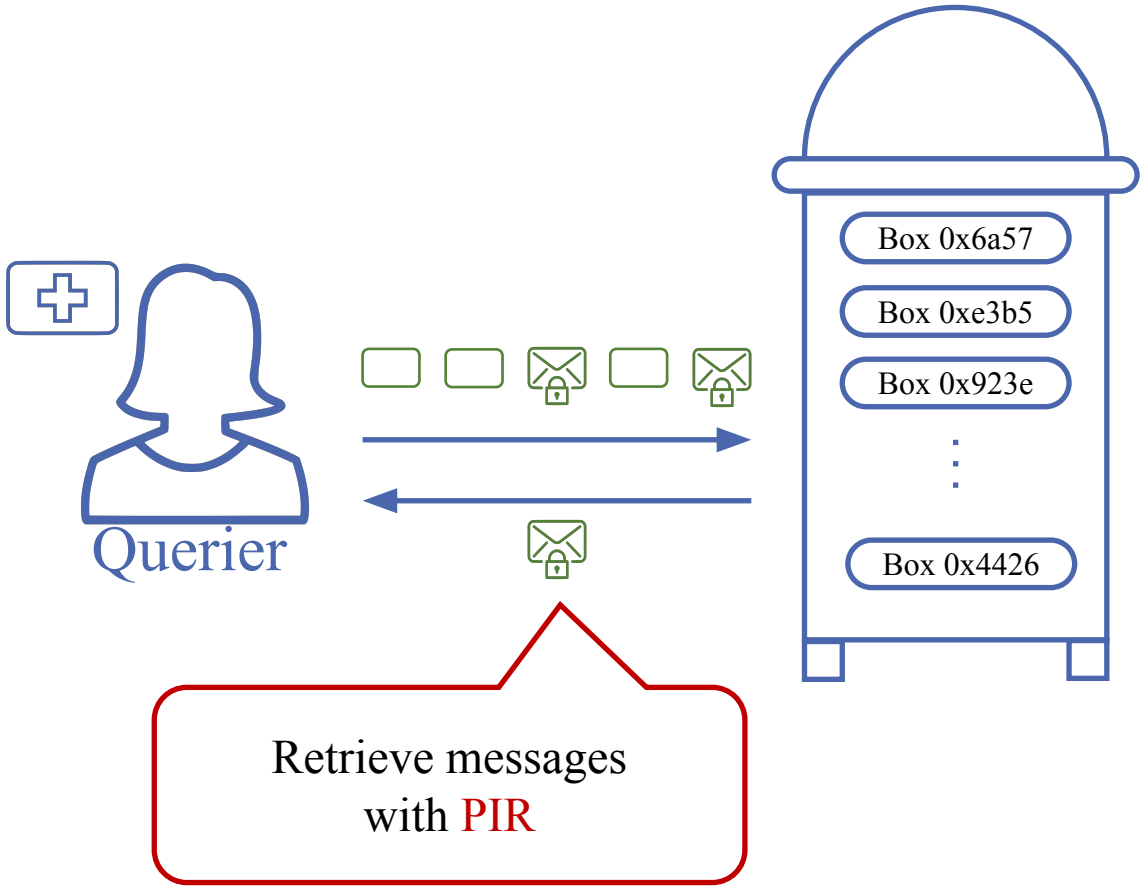
# Anonymous messaging



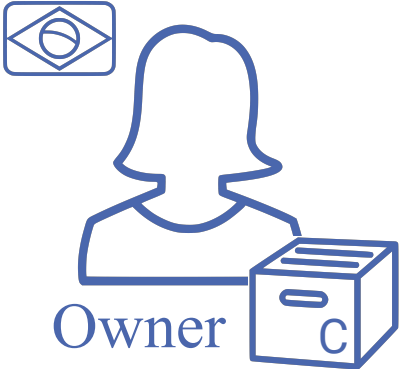
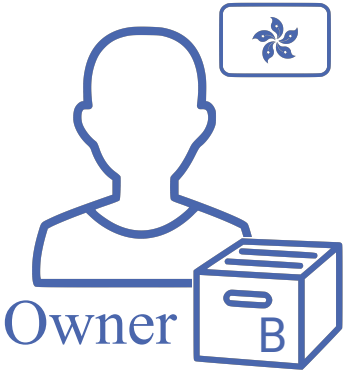
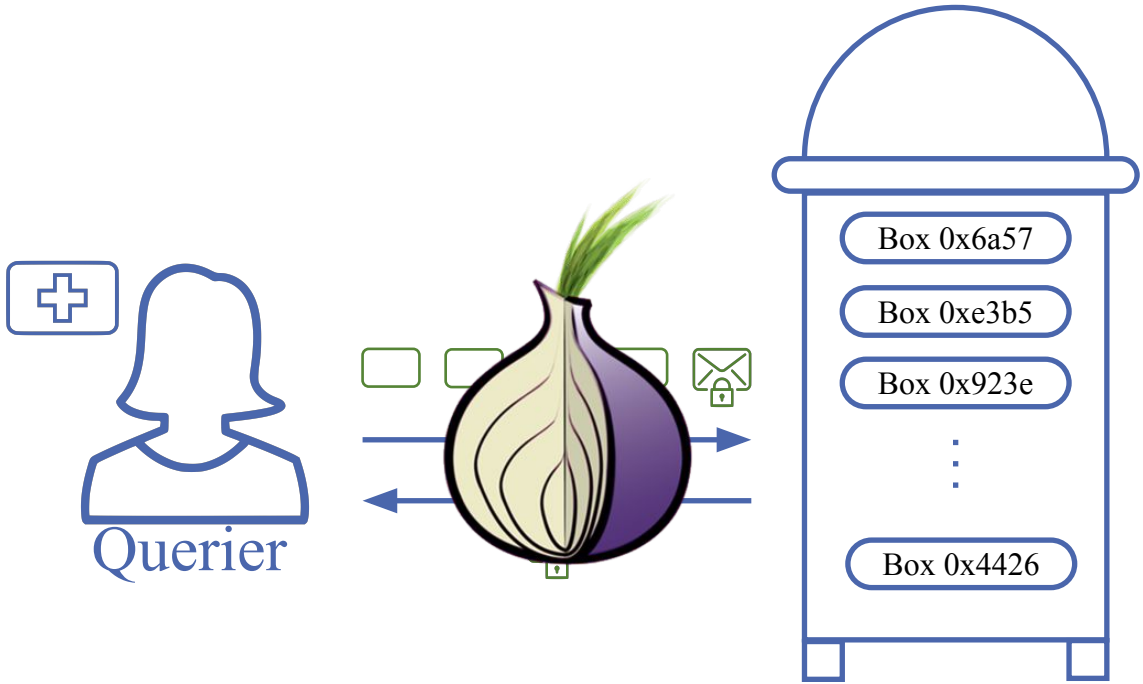
# Anonymous messaging



# Anonymous messaging



# Anonymous messaging





# User study



# Configure trade-offs



Functionality

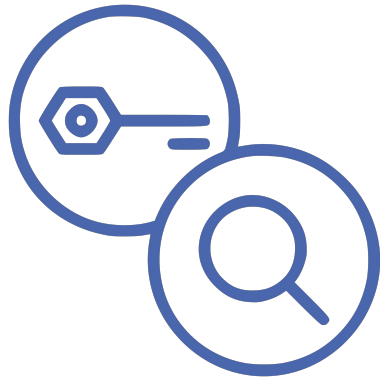


Querier privacy



Document owner  
privacy

# 3 search systems



MS-PSI

# 3 search systems



MS-PSI



Lucene

↓ Privacy

↑ Functionality

# 3 search systems

**Results**

Show all details Hide all details

Document Owner	Number of matches	
J1	1 full match(es) / 0 partial match(es)	Hide Details Anonymously contact owner
1 document(s) contain(s) the queried named entity(ies) trump.		
11 document(s) contain(s) none of the queried named entities.		
J5	1 full match(es) / 0 partial match(es)	Show Details Anonymously contact owner
J2	0 full match(es) / 0 partial match(es)	Show Details

MS-PSI

**Results**

Show all details Hide all details

Document Owner	Number of matches	
J9	4	Hide Details Anonymously contact owner
Document 0 is containing the following snippets:		
100s of Drugs, Industry Pledges Restraint By Robert Langreth, Cynthia Koons and Jackie Gu Published: July 16, 2018   Updated: August 1, 2018 President trump		
Last month, Bloomberg introduced a tool to track what's happened to prices for some of the most widely used, best-known drugs in the world since trump		
The trump administration has said it's committed to getting prices down. The list prices matter.		
Document 3 is containing the following snippets:		
"Here's What 'The Most Hated Man in America' Thinks About Donald trump" (http://fortune.com/2016/06/03/shkreli-trump-twitter-rant). Fortune.		
"Donald trump trashes former hedge-fund guy who jacked up drug price: 'He looks like a spoiled brat'" (http://www.businessinsider.com/donald-trump-martin-shkreli-daraprim-drug-cost		
"Martin Shkreli Will Drop Unreleased Wu-Tang Clan Music If Donald trump Wins Presidential Election" (http://www.xlmag.com/news/2016/10/martin-shkreli-unreleased-wu-tang-clan-donald-trump-wins-election		
Document 5 is containing the following snippets:		
The criticism has come from across the political spectrum, from President Donald trump, a Republican, to progressive Democrats including U.S.		
Document 6 is containing the following snippets:		
President Donald trump has frequently promised to dismantle the Affordable Care Act (ACA), better known as Obamacare, which was designed to make medical		
7 documents are not matching this query.		
J3	1	Show Details Anonymously contact owner
J1	0	Show Details

Lucene

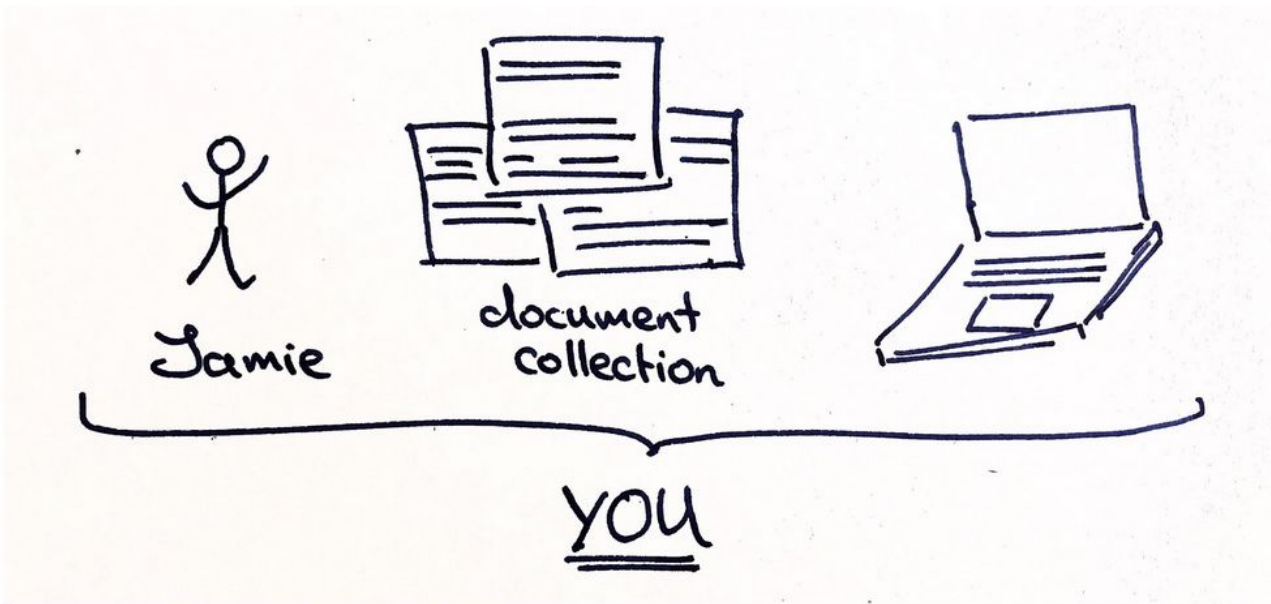
# Designing user interview



Build a fake story

(only use public leaks)

Pretend you are **Jamie**



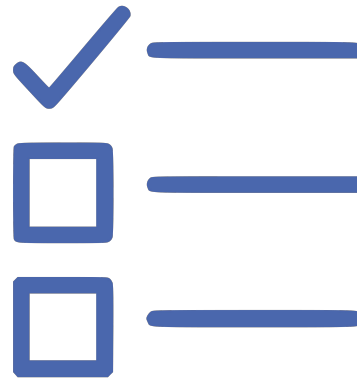
Jamie's interests:  
*tax evasion by large corporations*

# Designing user interview



Build a fake story

(only use public leaks)



Give tasks



# Designing user interview



Build a fake story

(only use public leaks)

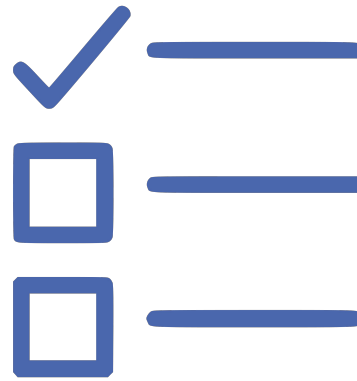
You have heard rumours that Verizon use a special construction to avoid paying taxes. Can you find out which journalist has more information about Verizon?

# Designing user interview

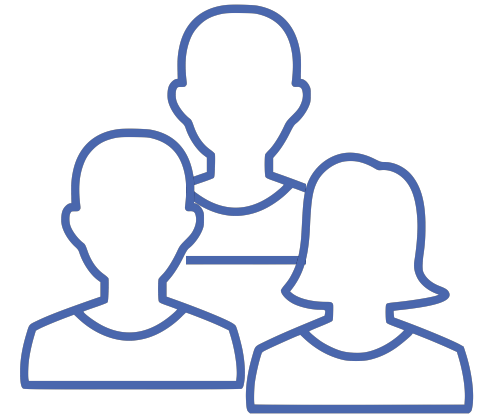


Build a fake story

(only use public leaks)

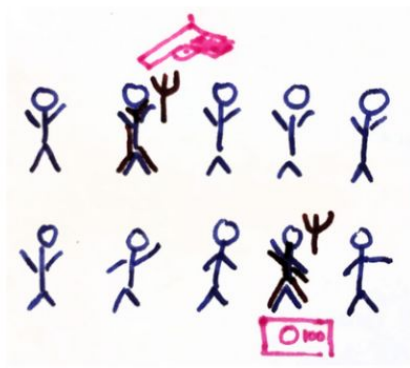


Give tasks



Simulate journalists

D



# 10

## OTHER JOURNALISTS

- 10 -- 20 documents
- They make queries

# 2

## BAD GUYS

(government agents, intelligence operatives, competitors, etc.)

- Bribe/threaten honest journalists or attack their machines (they will not attack you)
- Can also make search queries

### Goals:

- Learn what you are searching for
- Learn what your documents are about

Bu  
(only

ists

# How to show privacy?



Interactive hints

### Confirm New Query ✕

To make the query **tax** Datashare will send the encrypted query

**N44bRx1oXpQK**

to every journalist in the system.

Please copy the first 8 characters (**N44bRx1o**) to confirm your query:

✓ Confirm

Press [Confirm] to make your query.

Making PSI query

### Confirm New Query ✕

To make the query **trump** Datashare will send the query

**trump**

to every journalist in the system.

Please copy it (**trump**) to confirm your query:

✓ Confirm

Press [Confirm] to make your query.

Making Lucene query

# How to show privacy?

Date	↑↓ Event
2023.03.06 16:47:45	Someone queried your documents using the encrypted query <b>c6htbpsJwGBD</b> (1 named entity).
2023.03.06 16:47:38	Someone queried your documents using the encrypted query <b>4k4q58pku99e</b> <b>yS2uoNmoFsoy</b> <b>TqyewrebPjXN</b> (3 named entities).
2023.03.06 16:47:14	Someone queried your documents using the encrypted query <b>S9foYq6kmYrv</b> <b>78vFrqx1QTcy</b> <b>xvRgHFZsUkA6</b> (3 named entities).
2023.03.06 16:47:04	Someone queried your documents using the encrypted query <b>kWkGaXhDsUhU</b> (1 named entity).

Explanation video

Interactive hints

**Received PSI queries**

# How to show privacy?



Interactive hints



Adversary's view

# Over the shoulder view

MS-PSI



I made 3 queries, from which I learned:

J11 (you) has 10 documents

... containing **luxembourg**,

... and not containing **papers**, **panama**, **brogstein**, **marc**, and **exinor**.

J11 (you) has 5 documents

... not containing **papers**, **panama**, **brogstein**, **marc**, **luxembourg**, and **exinor**.

I made 2 queries, from which I learned:

J11 (you) has 1 document matching the query: **Novartis epinephrine**

Document 3:

**Novartis** to sell **epinephrine** shot in U.S. pharmacies amid EpiPen shortage 3 Min Read (Reuters) - **Novartis** AG (NOVN.S) said on Tuesday it would make its REUTERS/Jim Bourg/File Photo **Novartis**' Sandoz unit launched the Symjepi **epinephrine** shots for use in hospitals in January and had said it would make the **Novartis** said both the adult and pediatric doses of Symjepi would be immediately available in local U.S. pharmacies.

J11 (you) has no documents matching the query:

- **Mylan** **GlaxoSmithKline**



Lucene



# Over the shoulder view

MS-PSI

J3

I made 3 queries, from which I learned:

J11 (you) has 10 documents  
... containing **luxembourg**.

**stein**, **marc**, and **exinor**.

**marc**, **luxembourg**, and **exinor**.

The over the shoulder view is only available in the simulation

I made 2 queries, from which I learned:

J11 (you) has 1 document matching the query:

Document 3:

**Novartis** to sell **epinephrine** shot in hospitals. **Novartis** Sandoz unit launched the Symjepi **epinephrine** shots for use in hospitals in January and had said it would make the **Novartis** said both the adult and pediatric doses of Symjepi would be immediately available in local U.S. pharmacies.

J11 (you) has no documents matching the query:

- **Mylan** **GlaxoSmithKline**

J3

(bryson)

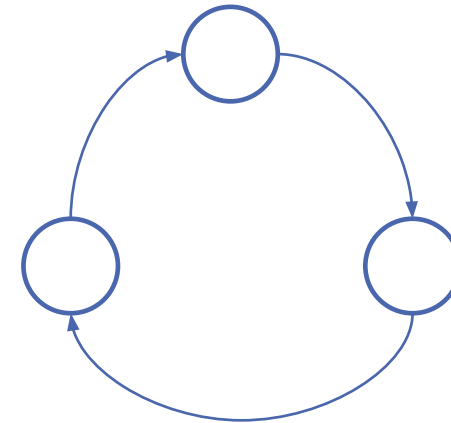


Lucene

# Performing user study



Over 30 journalist



Within subject  
study

Despite the lower functionality, journalists prefer the **MS-PSI** solution.

# Lessons from deployment



# Deployment



UX



Authentication



Document search



Messaging

# Lesson: prepare to deal with legacy

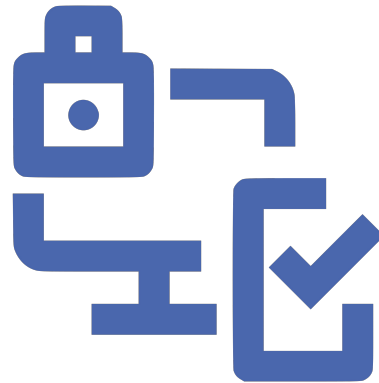


Token server  
(ACL / Abe's blind sig)

# Lesson: prepare to deal with legacy



Token server  
(ACL / Abe's blind sig)

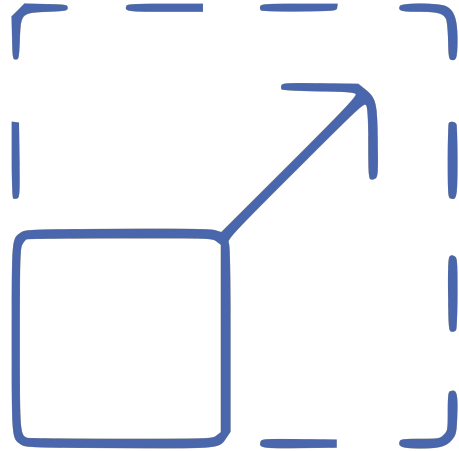


2 Factor auth



Internal OAuth

# Lesson: cold start

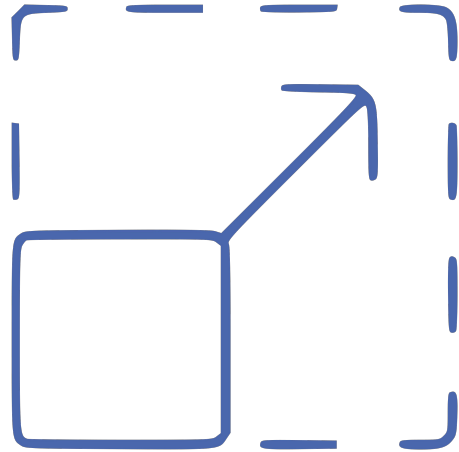


Designed to:

- Scale to 1000s of journalist
- Support millions of documents



# Lesson: cold start



## Deployment:

- Begin with 10s of journalists
- Plans to reach ~300 journalists

Lesson: don't think complicated

Keep it simple!

# Why DatashareNetwork succeeded?

# Why DatashareNetwork succeeded?



Real userbase

# Why DatashareNetwork succeeded?



Real userbase



User involvement  
in all stages

# Why DatashareNetwork succeeded?



Real userbase



User involvement  
in all stages



A dedicated  
engineering team

# Why DatashareNetwork succeeded?



Real userbase



User involvement  
in all stages



A dedicated  
engineering team



Time & resource

[kasra.edalat@epfl.ch](mailto:kasra.edalat@epfl.ch)

Thank you for your attention!





# Conclusion

- Requirement analysis of investigative journalists
  - Asynchronous users, communication limits, no trusted infrastructure
- Designing DatashareNetwork
  - A new document search
  - A new anonymous messaging system
  - End-to-end system design and privacy analysis
- A user study with 30+ experienced journalists
  - Study functionality, querier privacy, and document owner privacy
- Deploying DatashareNetwork
  - Legacy, cold start, and begin simple