Data-Driven Privacy Indicators

Hamza Harkous, Rameez Rahman, Karl Aberer

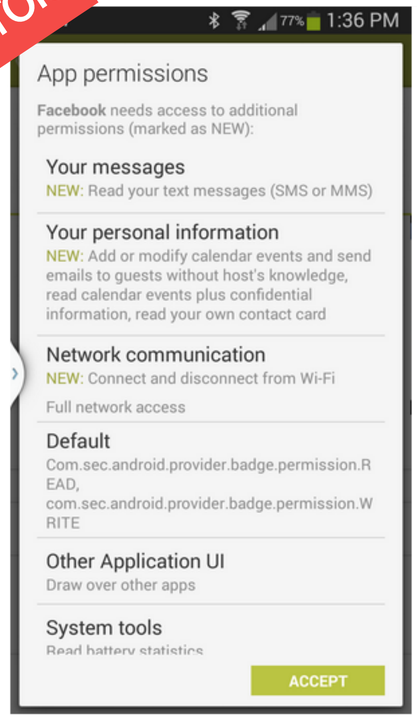


EPFL, Switzerland

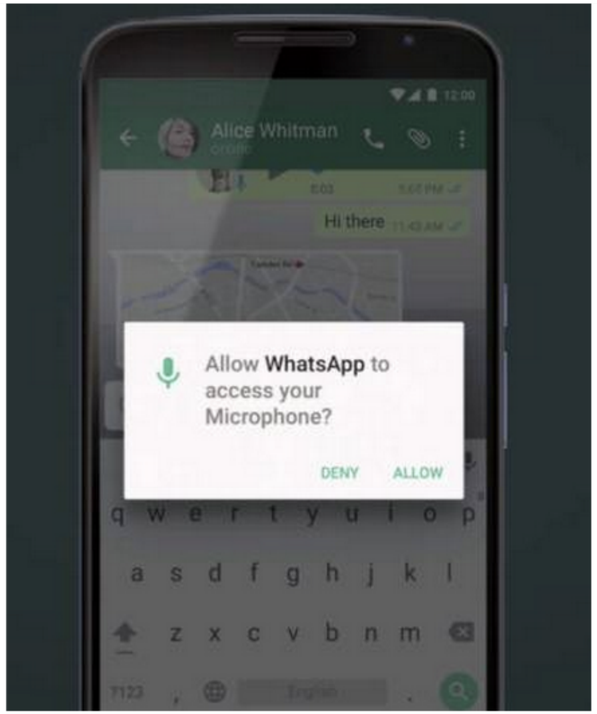
Workshop on Privacy Indicators, SOUPS 2016

Permissions in 3rd Party Apps

Android

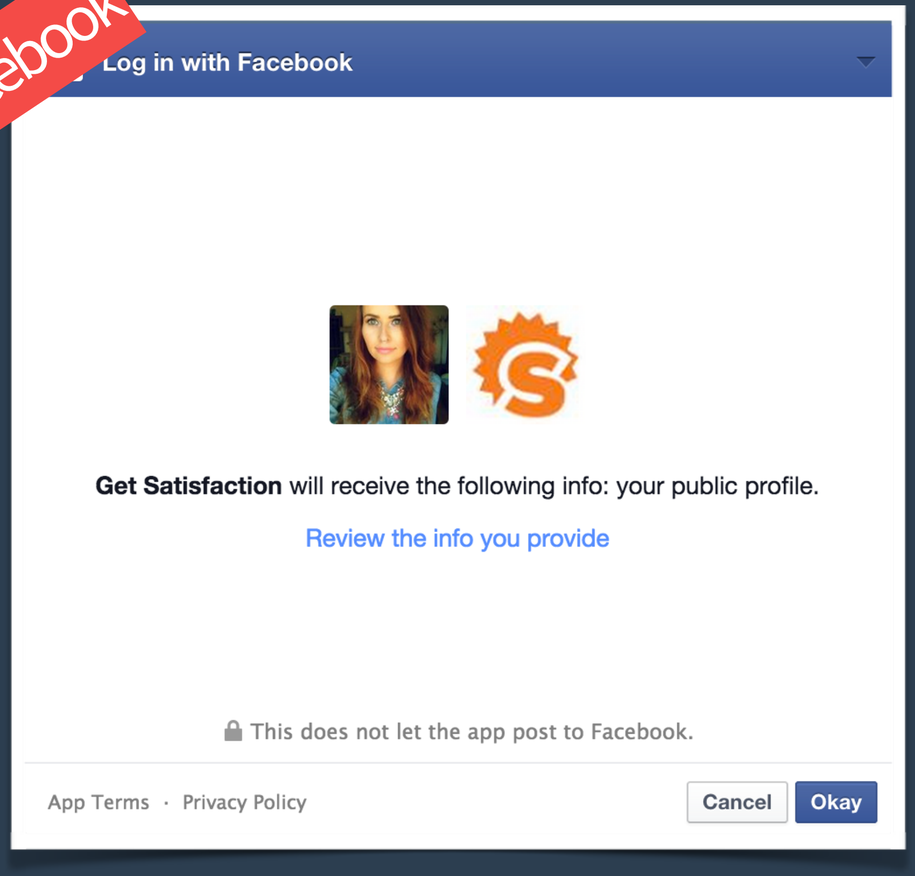


Old Model



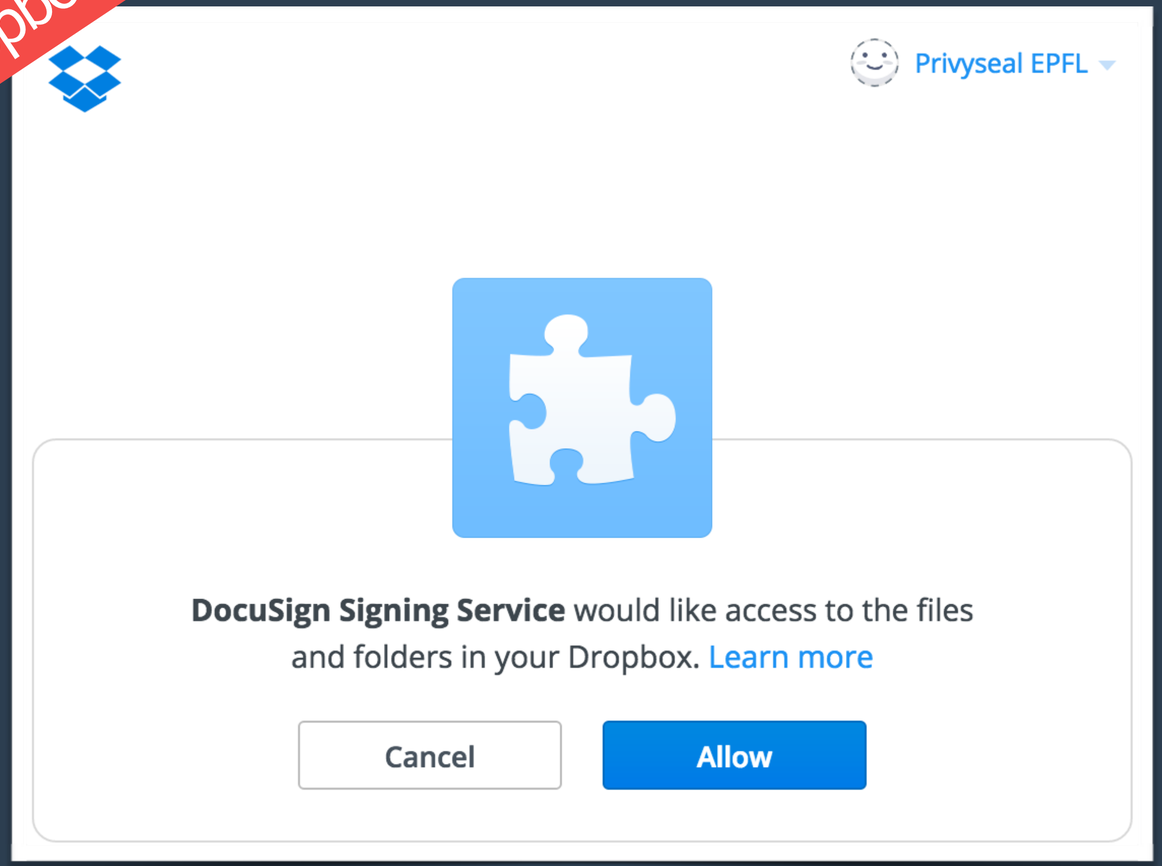
New Model

Facebook

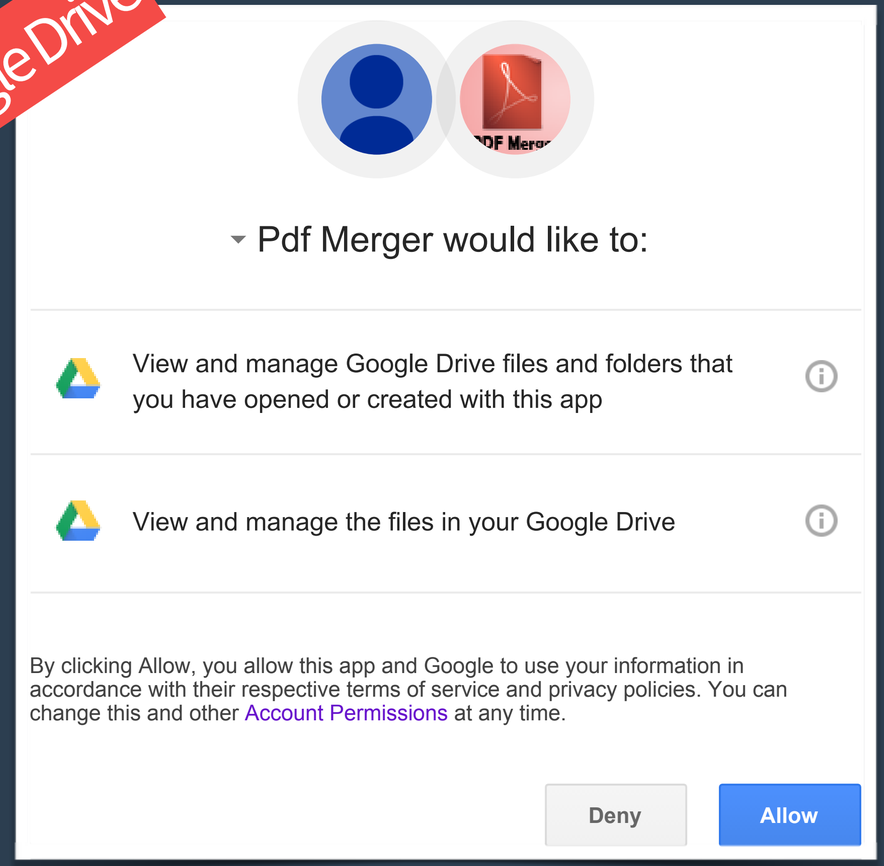


Permissions in 3rd Party Apps

Dropbox

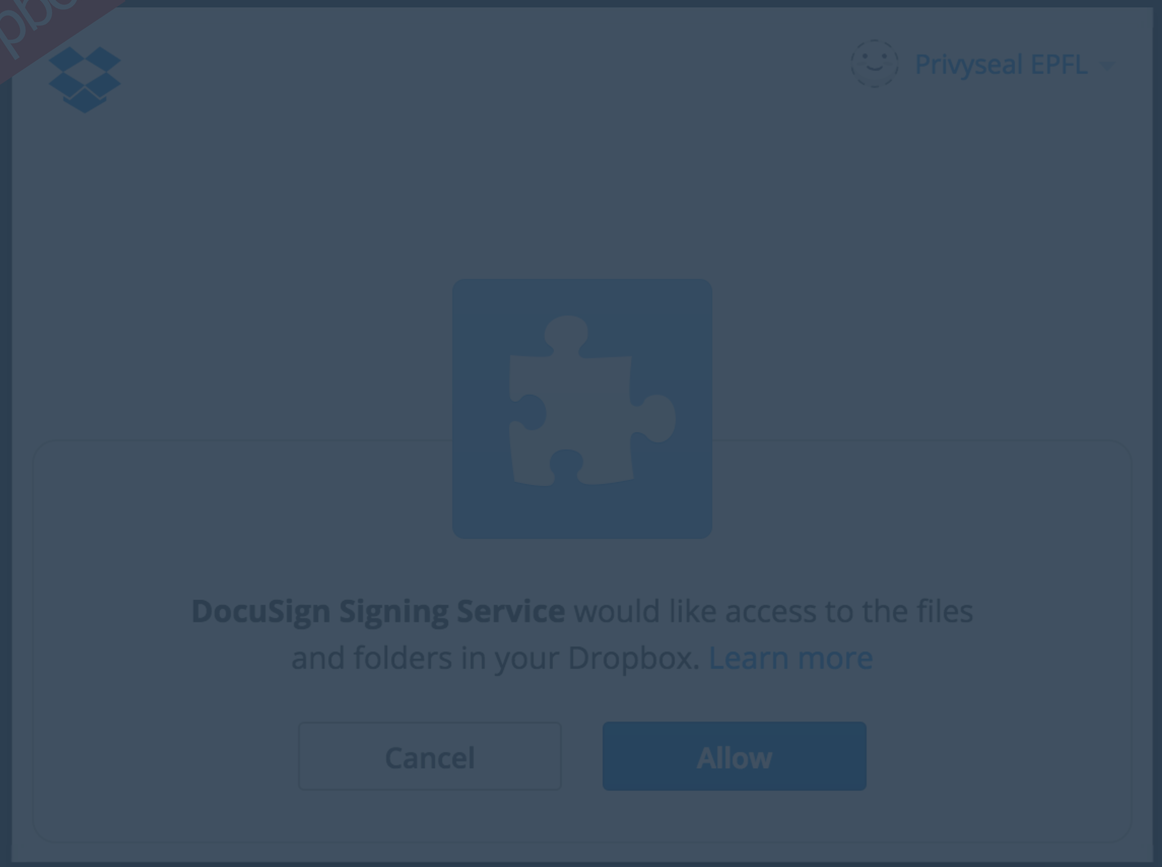


Google Drive

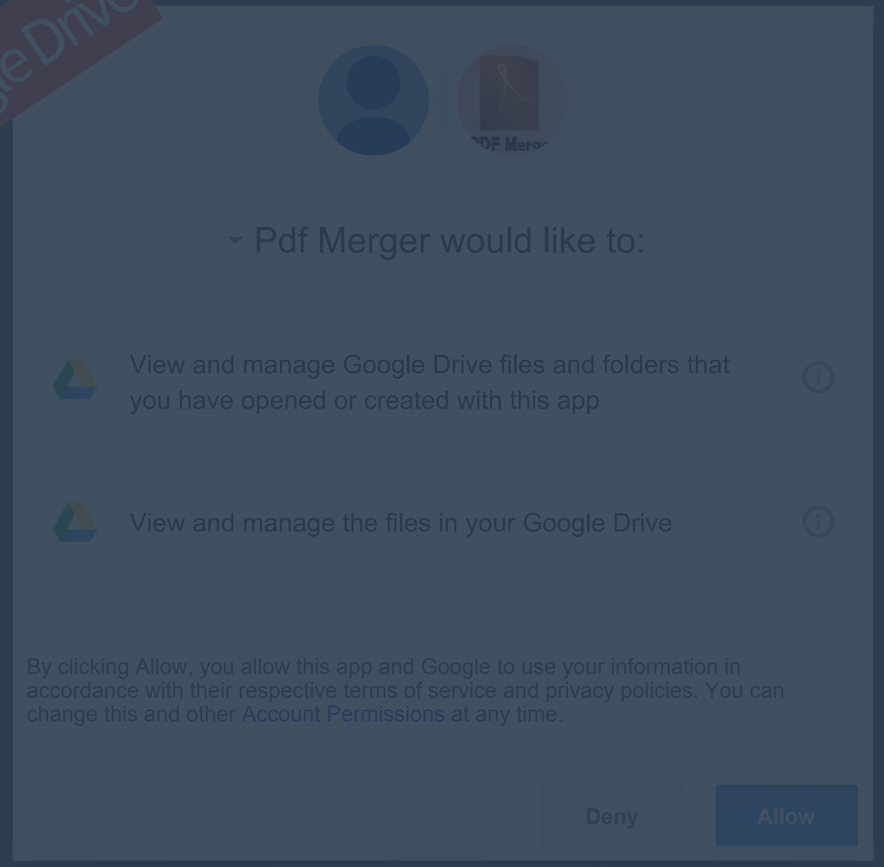


Permissions in 3rd Party Apps

Dropbox



Google Drive



Permissions in 3rd Party Apps

Challenges

- One size fits all
- Habituation effects
- Different from user expectations

Data-Driven Privacy Indicators (DDPIS)

Dynamic indicators as a function of users' data

Data-Driven Privacy Indicators (DDPIS)

Dynamic indicators as a function of users' data

Service provider delivers insights that help users make privacy-aware decisions.

Focus on 3rd Party Cloud Apps

3rd party apps









CSPs







Files



Your Files



Problem 1:
Dealing with App Over-privilege

Dealing with App Over-privilege

64%



of 3rd party apps request more data than needed*

*H. Harkous, R. Rahman, B. Karlas, and K. Aberer.
"The Curious Case of the PDF Converter that Likes Mozart:
Dissecting and Mitigating the Privacy Risk of Personal Cloud Apps", PoPETs

Current Interface

ZIP Extractor wants to:

- View your basic profile info
- View your email address

per-file access

- View and manage Google Drive files and folders that you have opened or created with this app.

full access

- View the files in your Google Drive

ZIP Extractor wants to:

obtain permissions it doesn't need

View the files in your Google Drive

obtain permissions it needs to function

View your basic profile info

View your email address

View and manage Google Drive files and folders that you have opened or created with this app.

ZIP Extractor wants to:

obtain permissions it doesn't need

View the files in your Google Drive

obtain permissions it needs to function

View your basic profile info

View your email address

View and manage Google Drive files and folders that you have opened or created with this app.

Labelling

ZIP Extractor wants to:

obtain permissions it doesn't need

View the files in your Google Drive

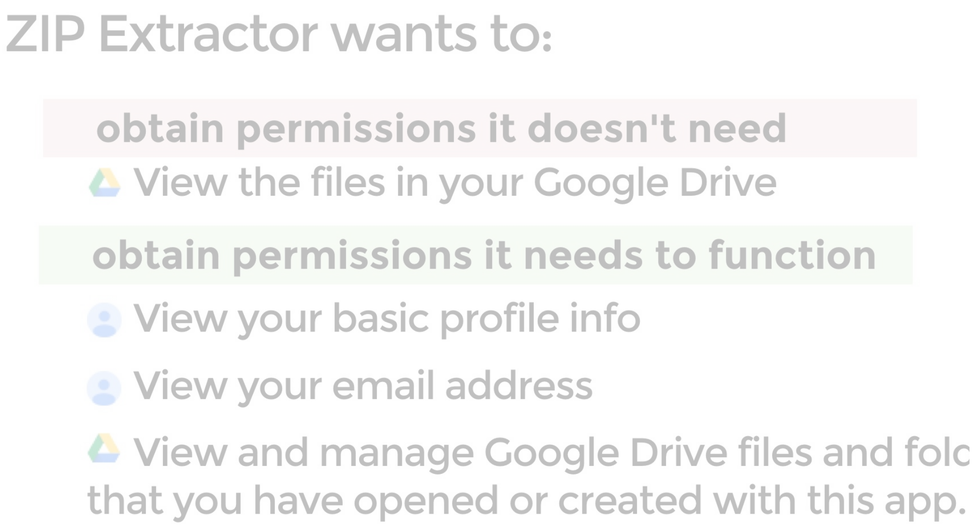
obtain permissions it needs to function

View your basic profile info

View your email address

View and manage Google Drive files and folc
that you have opened or created with this app.

1- Immediate Insights



What do the unneeded permissions say about you?

Immediate Insights (examples) from your Data

1- Immediate Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

- View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

They tell the app that you have the below image, named 'brithday21.jpg':



1- Immediate Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

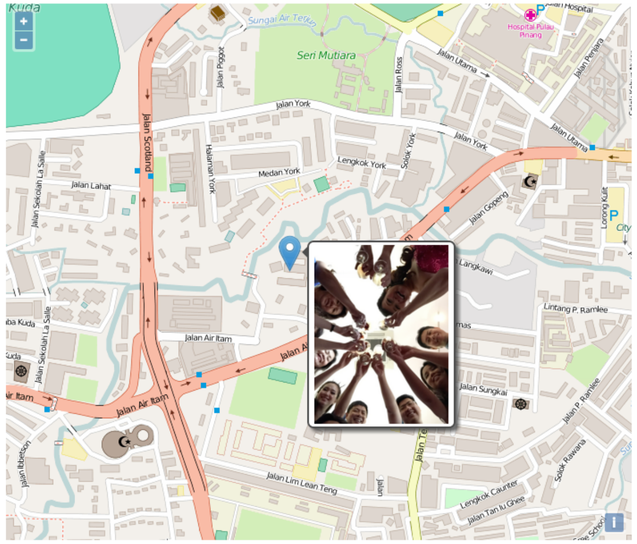
- View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

They tell the app that you have an image, named 'dinner.jpg', which was captured at this location:



2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

View the files in your Google Drive

obtain permissions it needs to function

View your basic profile info

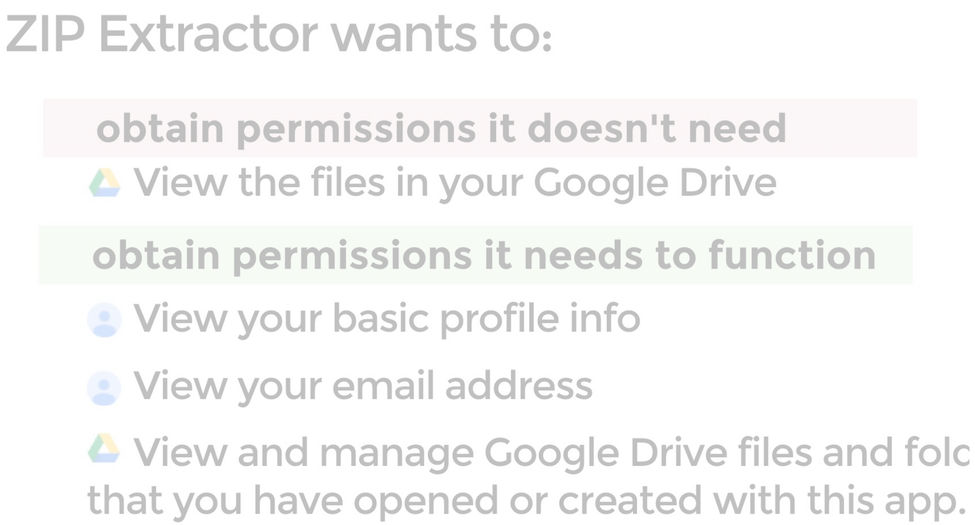
View your email address

View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

Far-reaching Insights from your Data

2- Far-reaching Insights



What do the unneeded permissions say about you?

Far-reaching Insights from your Data

2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

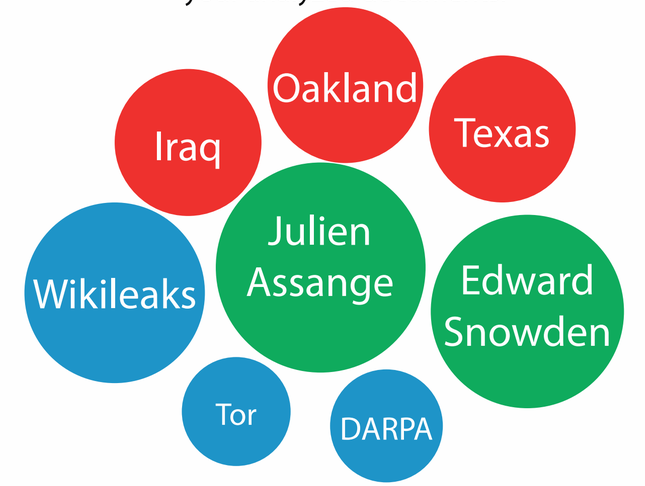
- View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

They tell the app that the following **People, Places, Companies**, etc., are important to you based on your analyzed documents:



...with Entities/Concepts/Topics

2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

- View the files in your Google Drive

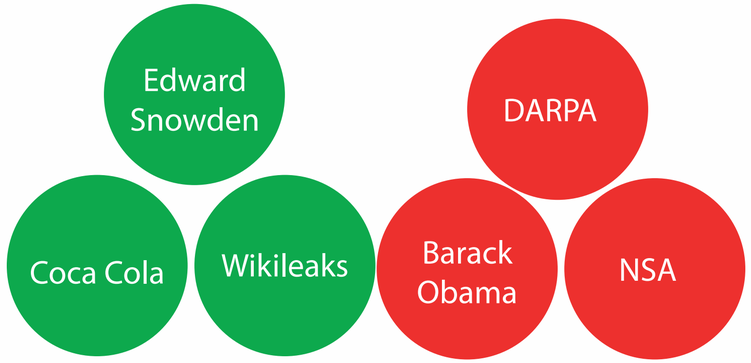
obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

They tell the app that you have the following views:

You're positive about: You're negative about:



...Sentiments

2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

View the files in your Google Drive

obtain permissions it needs to function

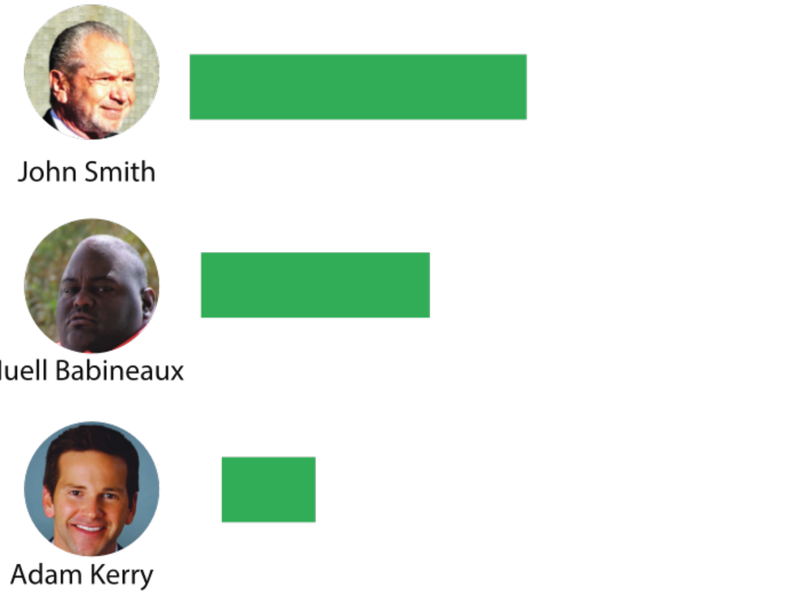
View your basic profile info

View your email address

View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

They tell the app that these People are your top collaborators.



...Top Collaborators

2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

- View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?


John Smith


Huell Babineaux


Adam Kerry

They tell the app that, with the above people, you share documents on these topics:

Technology | War & Crime | Access Control

...Shared Interests

2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

- View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?



They tell the app that the above faces appear in your photos along with these items

Gun | Musical Instrument | Dish

Alcohol | Computer | Office

...Faces with Context

2- Far-reaching Insights

ZIP Extractor wants to:

obtain permissions it doesn't need

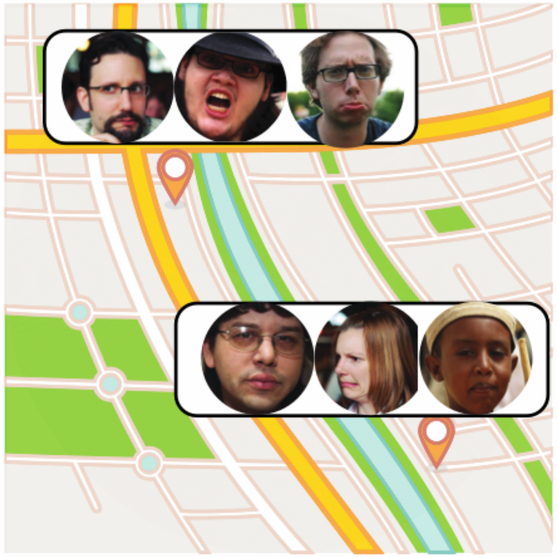
- View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and folc that you have opened or created with this app.

What do the unneeded permissions say about you?

They tell the app where your photos were taken, who appeared in them, and what things appeared in the photos.



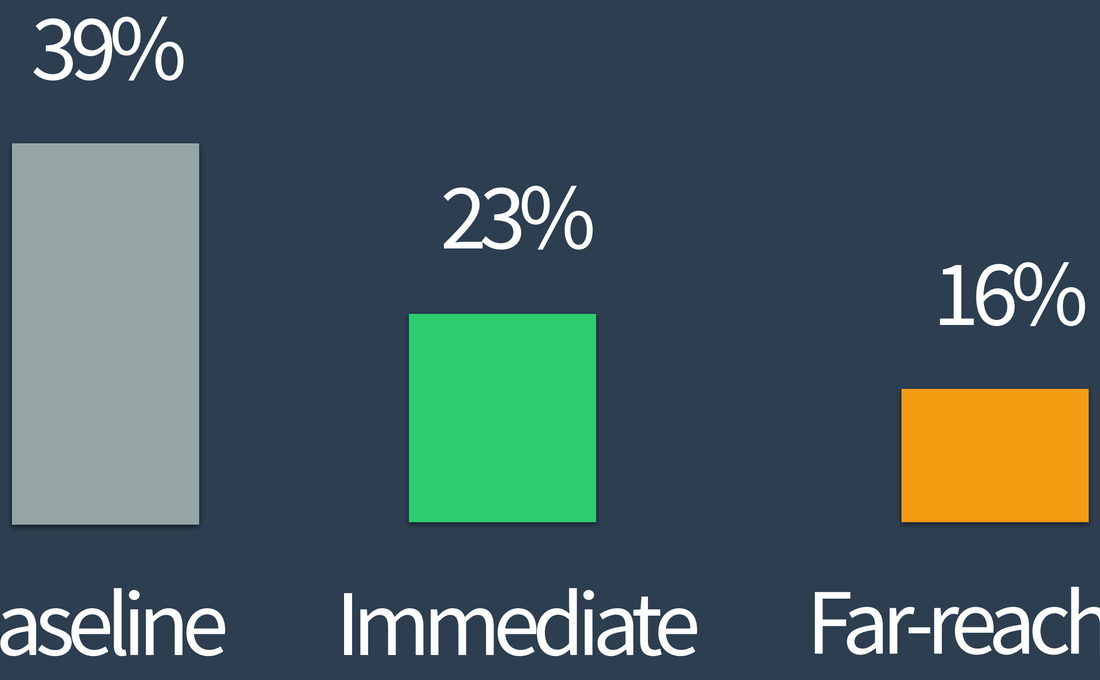
Fish | Sport | Butcher Shop

...Faces on Map

Inefficacy of Baseline Permissions

Acceptance Likelihood

(Percentage of users who would still accept over-privileged apps)



- Online experiment
- Actual user's data
- 160 participants in 3 groups
- GLMMs for significance tests

*H. Harkous, R. Rahman, B. Karlas, and K. Aberer.
"The Curious Case of the PDF Converter that Likes Mozart:
Dissecting and Mitigating the Privacy Risk of Personal Cloud Apps", PoPETs

The Power of Relational Insights



They tell the app that the above faces appear in your photos along with these items

Gun | Musical Instrument | Dish

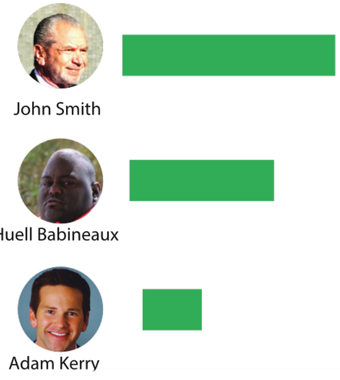
Alcohol | Computer | Office



They tell the app that, with the above people, you share documents on these topics:

Technology | War & Crime | Access Control

They tell the app that these People are your top collaborators.



<

Acceptance Likelihood

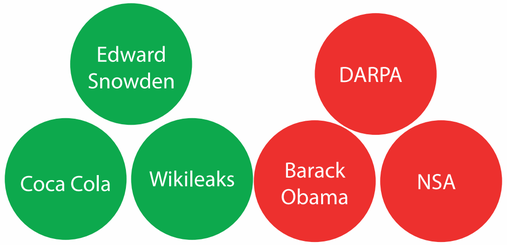
They tell the app that you have the below image, named 'brithday21.jpg':



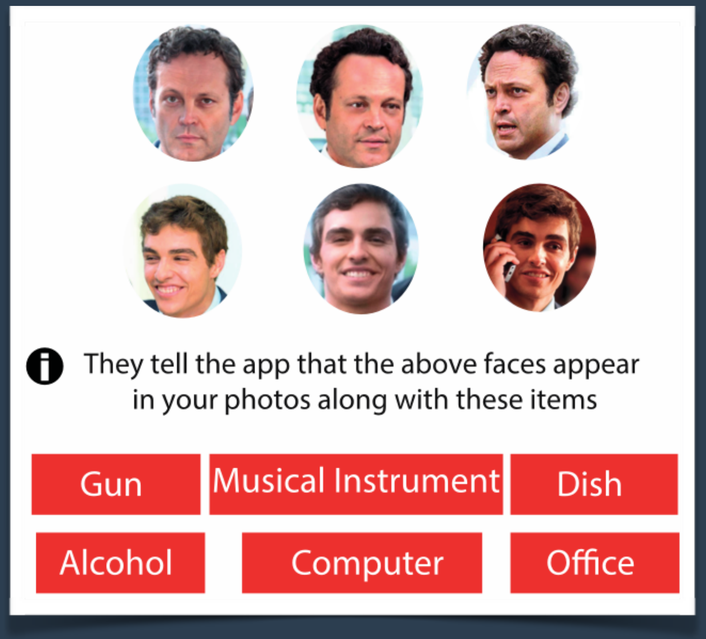
They tell the app that the following **People, Places, Companies**, etc., are important to you based on your analyzed documents:



They tell the app that you have the following views:



Impact of Face Recognition



<

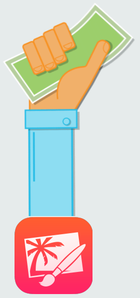
Acceptance Likelihood



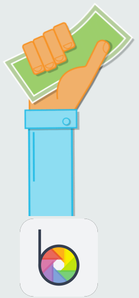
8%

21%

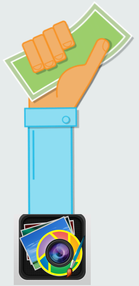
Problem 2:
Minimizing Interdependent Privacy



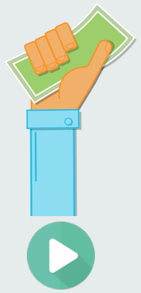
Company 1



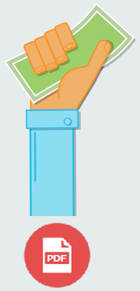
Company 2



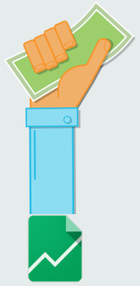
Company 3



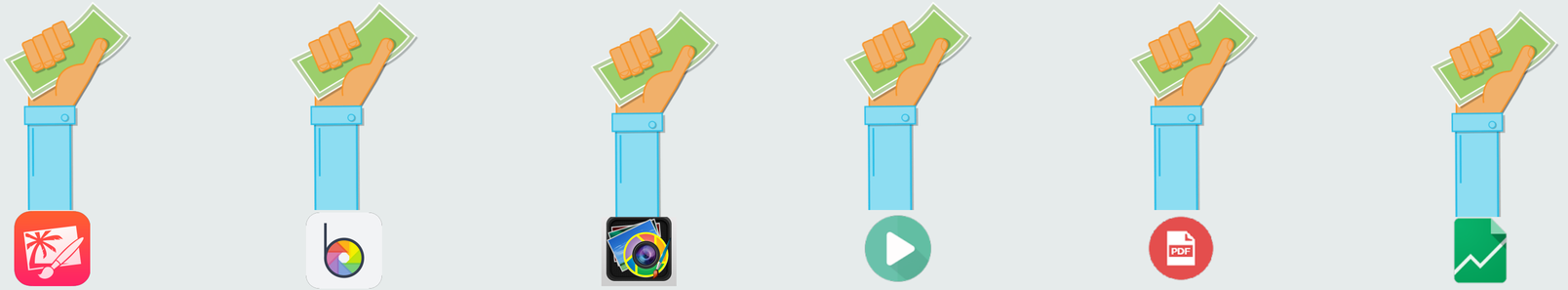
Company 4



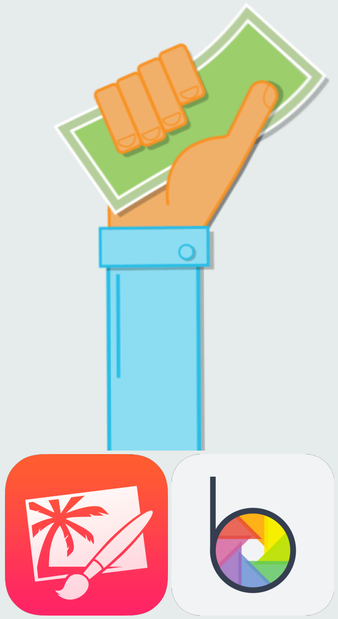
Company 5



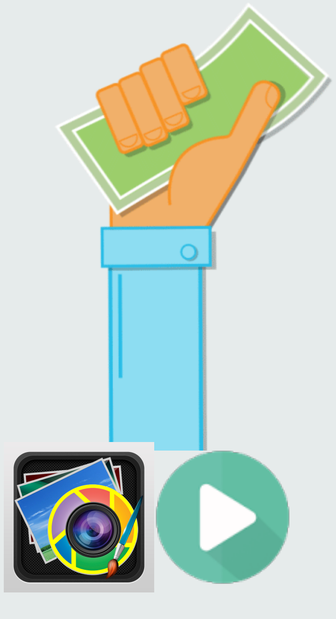
Company 6



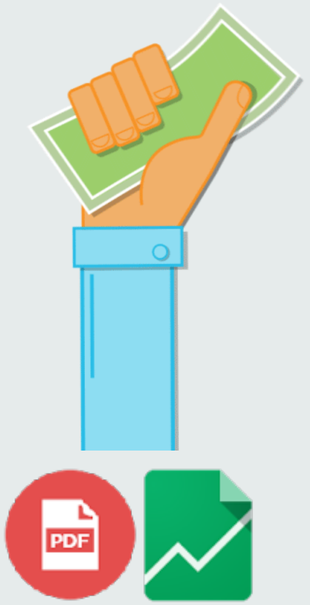
Too Many Shareholders → Larger Attack Surface



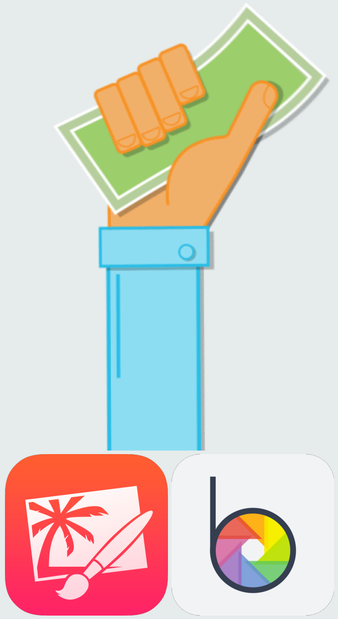
Company 1



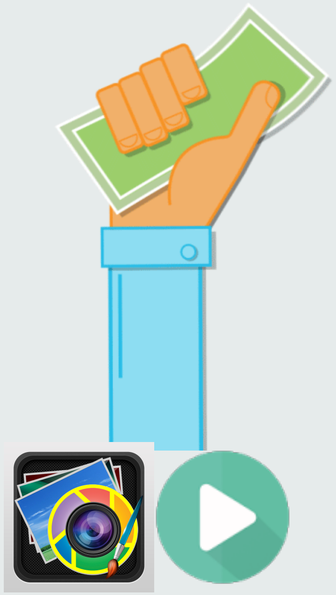
Company 2



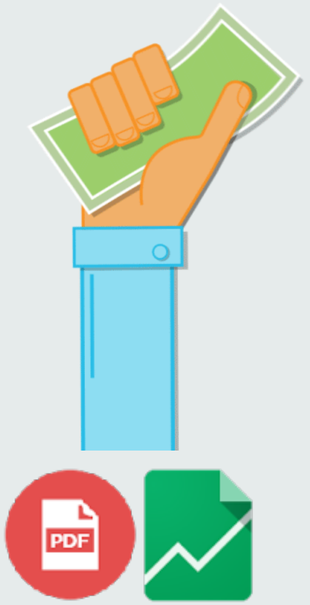
Company 3



Company 1



Company 2



Company 3

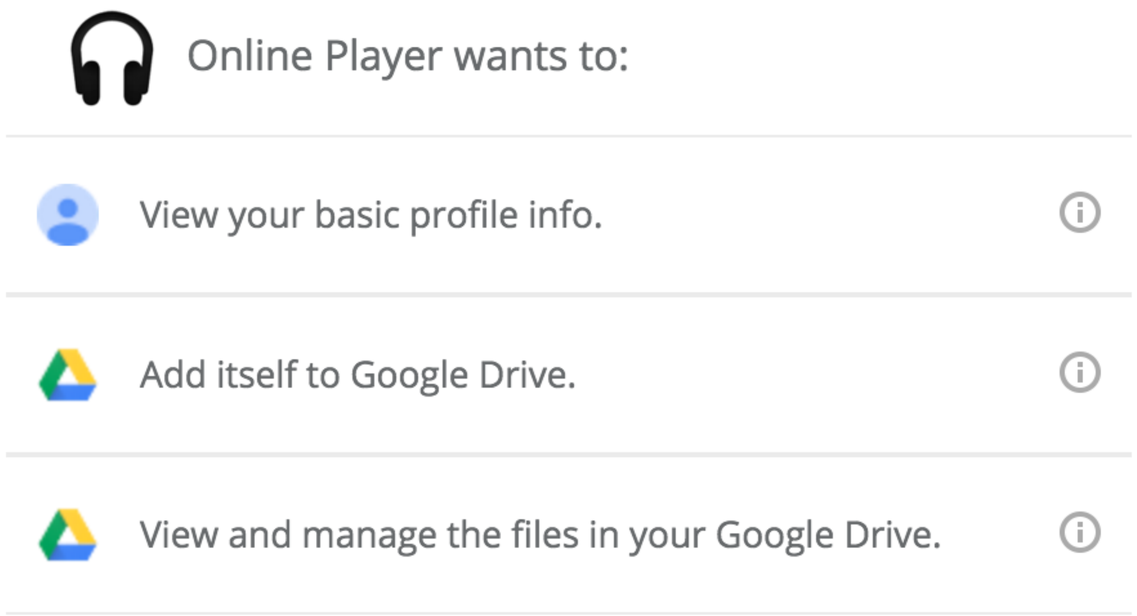
Fewer Shareholders →

Better Privacy

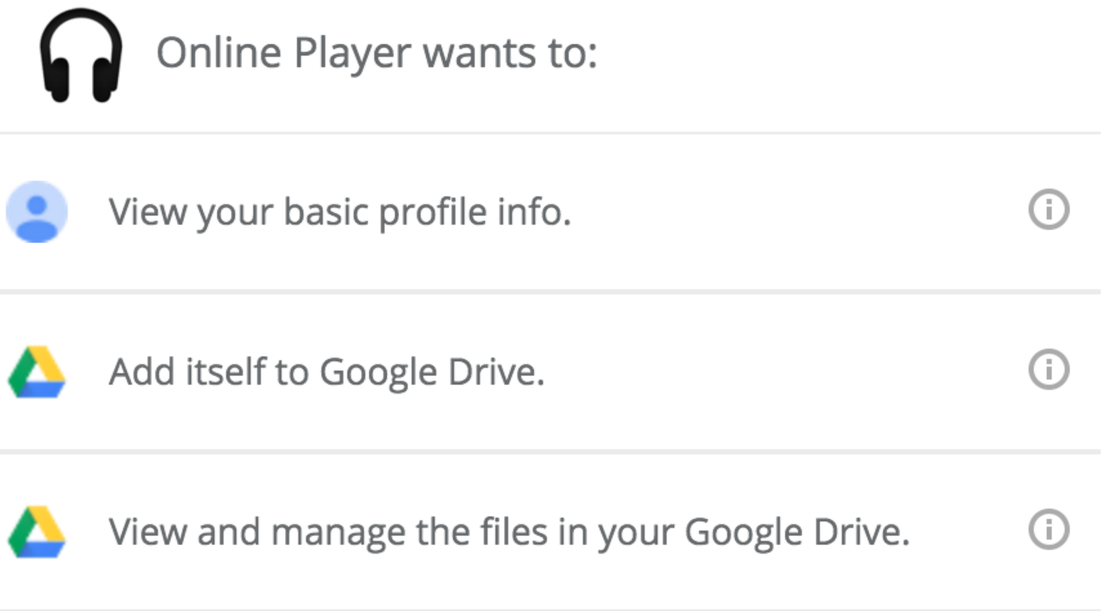
History-based Insights

- Keep data with a minimum number of vendors
- When possible, install apps from vendors that already have access to your data, either directly or from collaborators.

Baseline Permission Model



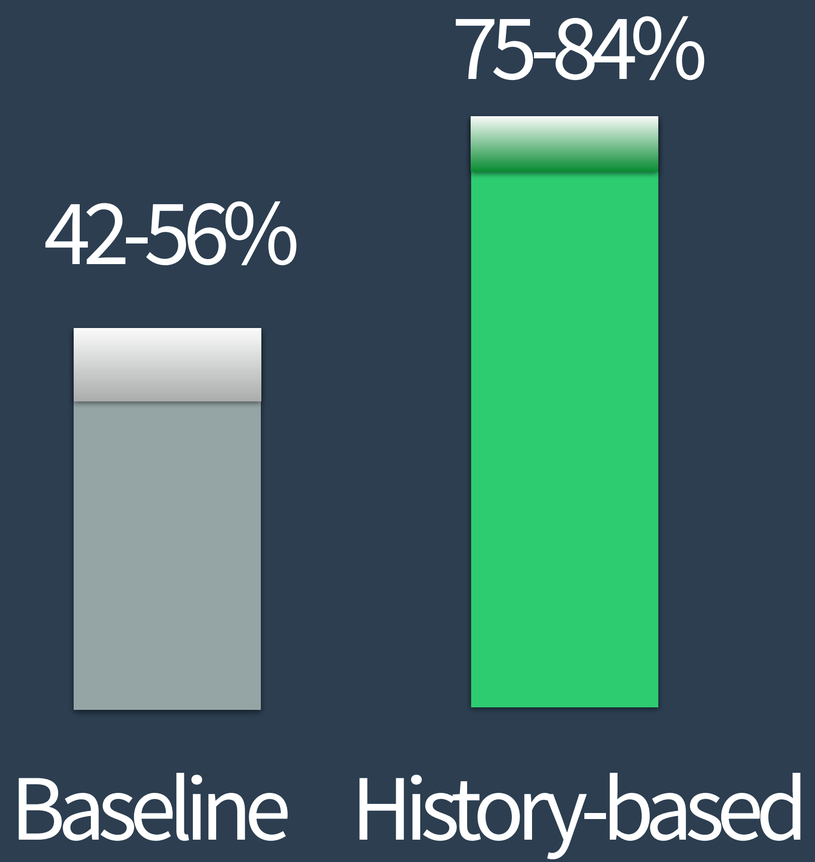
History-based (*HB*) Insights Model



Findings

Superiority of the HB Insights

(Percentage of users who would favor the app with existing access to their data)



- Online experiment (CrowdFlower)
- Role-playing scenario
- 141 participants in 2 groups
- Fisher's test for significance

User Motivations

- cross-app compatibility
- interface familiarity
- satisfaction with the previous vendor

User Motivations

- cross-app compatibility
- interface familiarity
- satisfaction with the previous vendor

Users’ data can be used to highlight the other advantages of taking privacy-aware decisions

Further Applications of DDPIs

Extensions of *FR* and *HB* Insights

- mobile/social networking platforms
- browser extensions (visualize browser history contents)
- visualize the power of 4th party ad providers

New DDPIs

- consequences of privacy settings
- how others view my encrypted data
- visualize which of the user's apps still operate with encryption

Post-installation Scenario

- insights based on downloaded files
- insights based on accessed location*

* H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. CHI 2015

Limitations

The Business Case

- The provider is interested in strengthening the ecosystem
- Could privacy be the selling point?

The Economic Cost

- extra computational cost
- data analysis already run for other purposes (e.g. search)

Usability Challenges

- How to stay minimize information overload?
- How to prioritize messages when multiple optimizations are possible?

What's Next?

DDPIS

Privacy Assistants



Questions/Feedback?

hamza.harkous@gmail.com
hamzaharkous.com

Image/Media Credits

- Markus Magnusson: slide 8
- David Holm: slide 24
- Freepik: slide 23
- Fab Design: slide 41