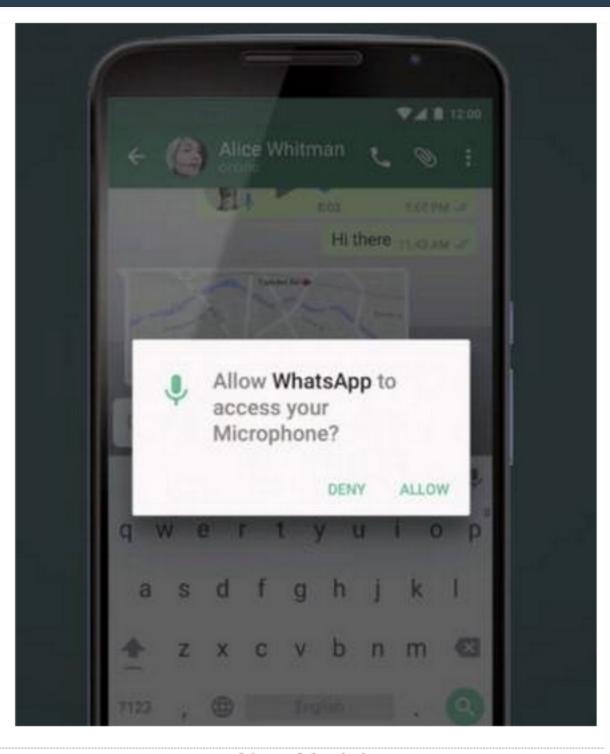
Data-Driven Privacy Indicators

Hamza Harkous, Rameez Rahman, Karl Aberer EPFL, Switzerland

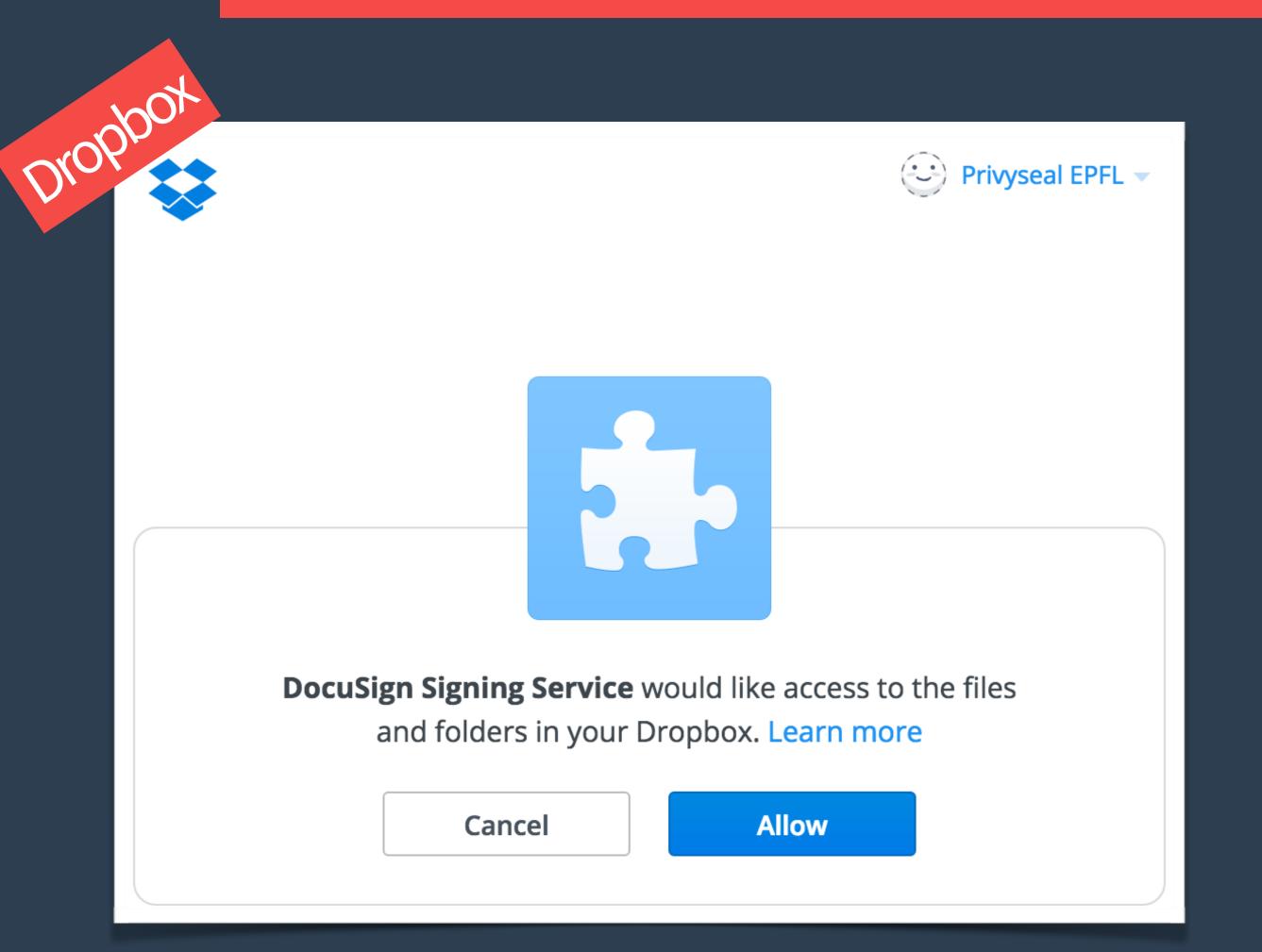
* 🛜 🔏 77% 📋 1:36 PM App permissions Facebook needs access to additional permissions (marked as NEW): Your messages NEW: Read your text messages (SMS or MMS) Your personal information NEW: Add or modify calendar events and send emails to guests without host's knowledge, read calendar events plus confidential information, read your own contact card Network communication NEW: Connect and disconnect from Wi-Fi Full network access Com.sec.android.provider.badge.permission.R com.sec.android.provider.badge.permission.W Other Application UI Draw over other apps System tools Read hattery statistics ACCEPT

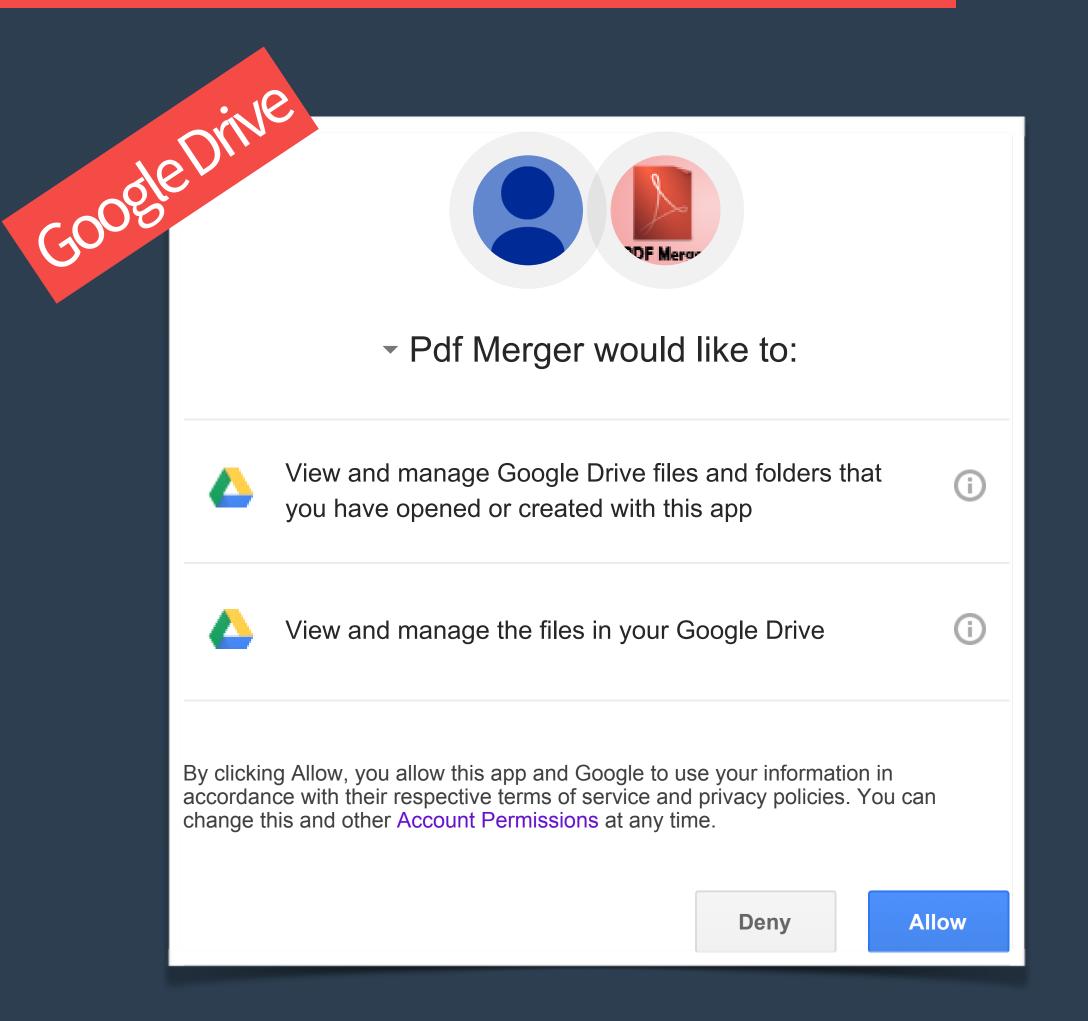
Old Model

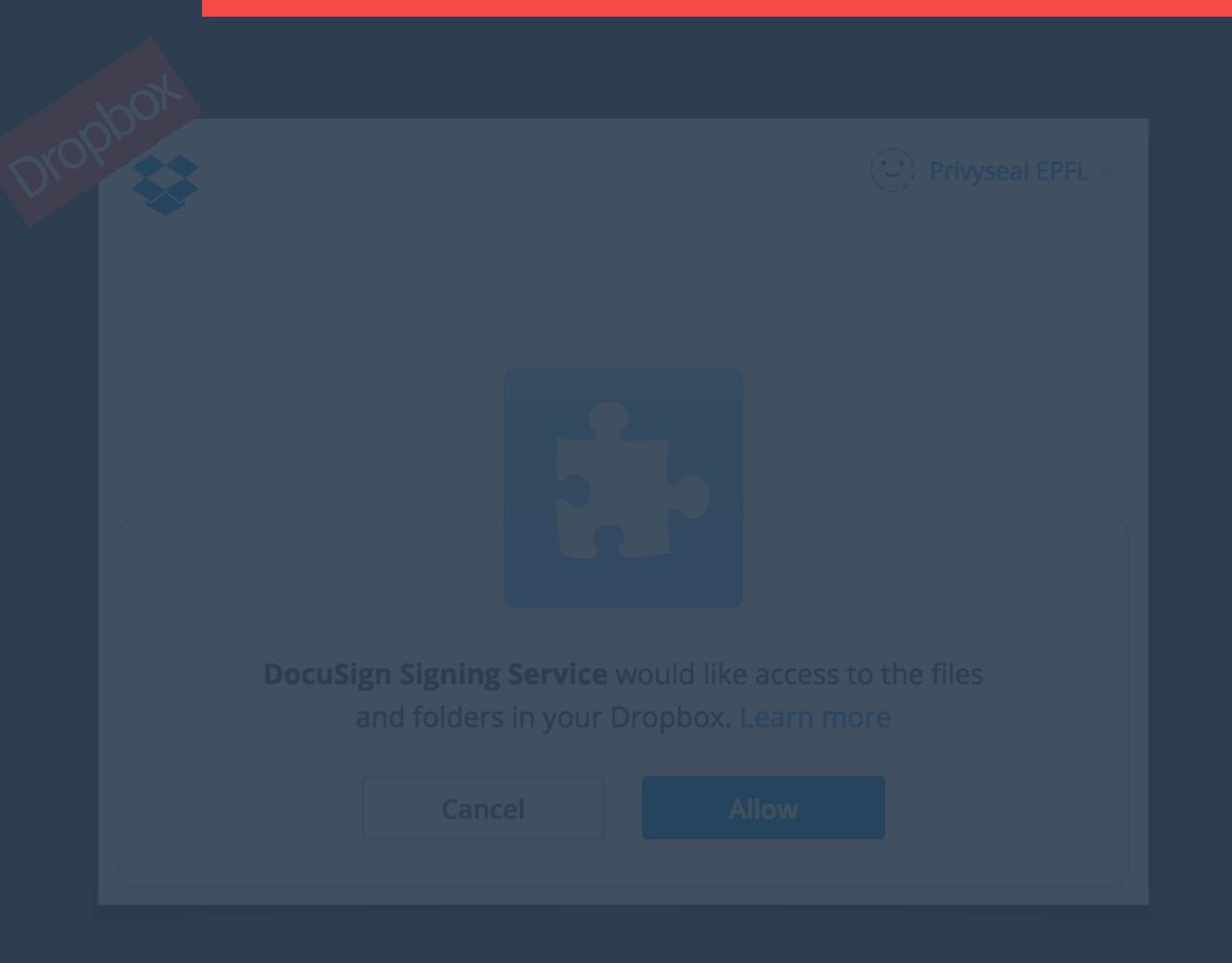


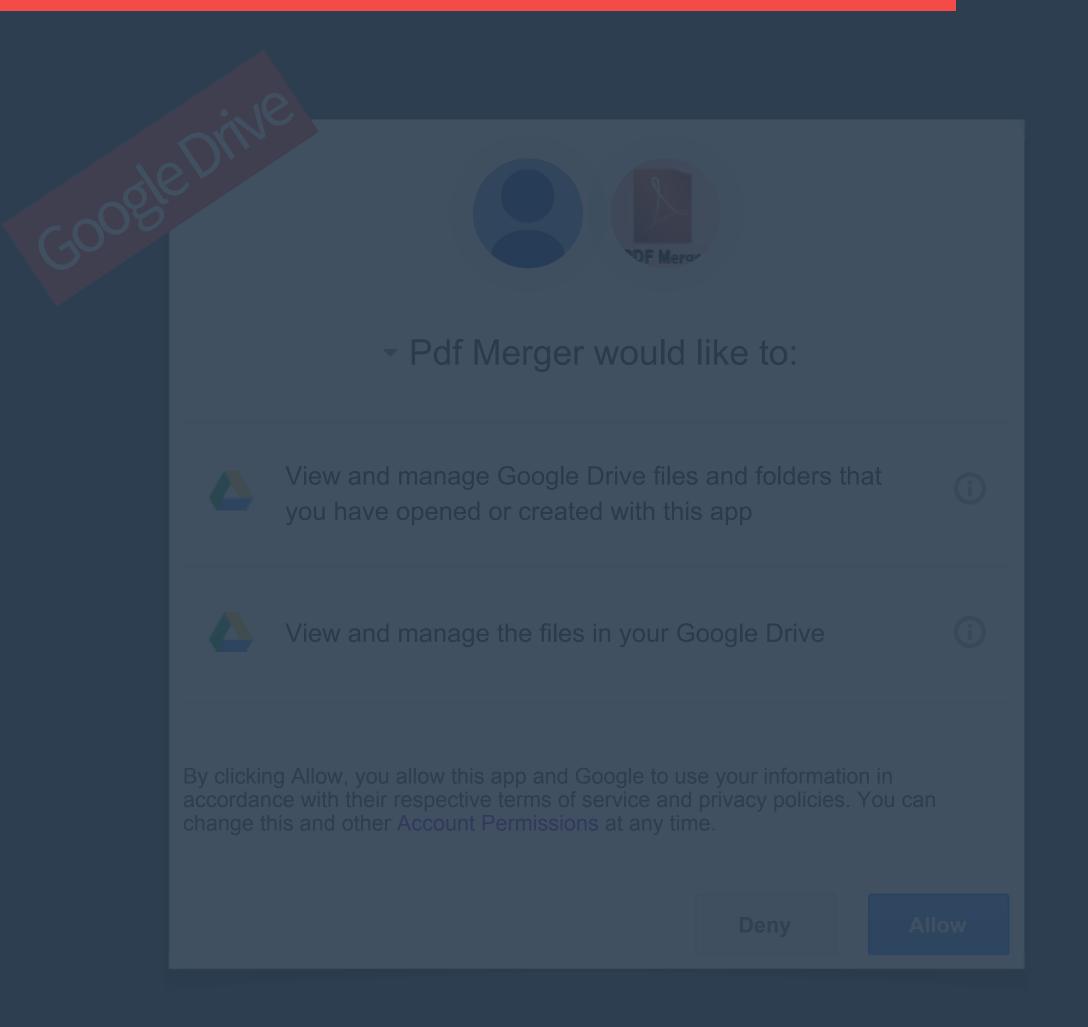
New Model

Log in with Facebook Get Satisfaction will receive the following info: your public profile. Review the info you provide A This does not let the app post to Facebook. Okay App Terms · Privacy Policy Cancel











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













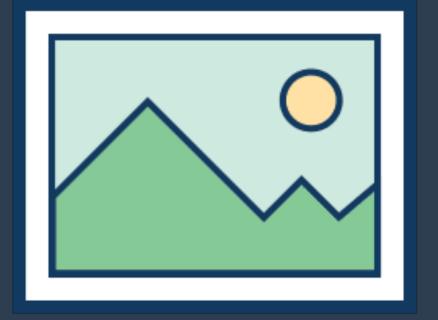


CSPs





Your Files



Problem 1: Dealing with App Over-privilege

Dealing with App Over-privilege



of 3rd party apps request more data than needed*

Current Interface

ZIP Extractor wants to:

- View your basic profile info
- View your email address

per-file access

full access

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

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

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?

Immediate
Insights
(examples)
from your
Data

10

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
- Let 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

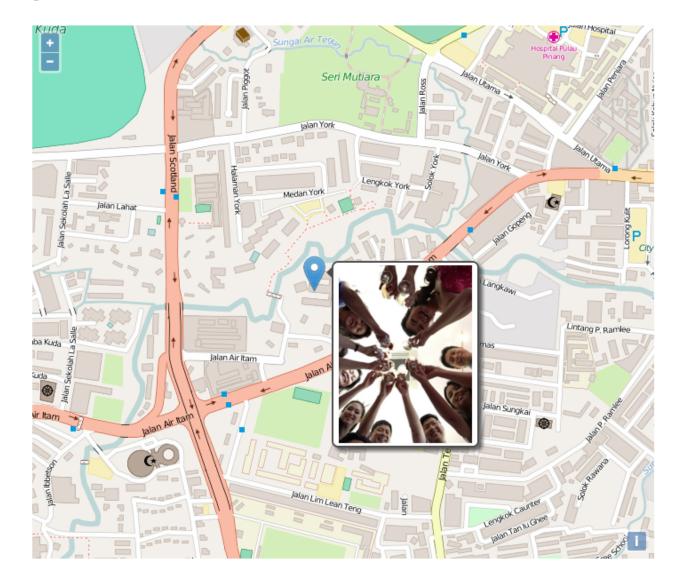
View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- Let 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:



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
- Let 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

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

13

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
- Let 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?



...with Entities/Concepts/Topics

ZIP Extractor wants to:

obtain permissions it doesn't need

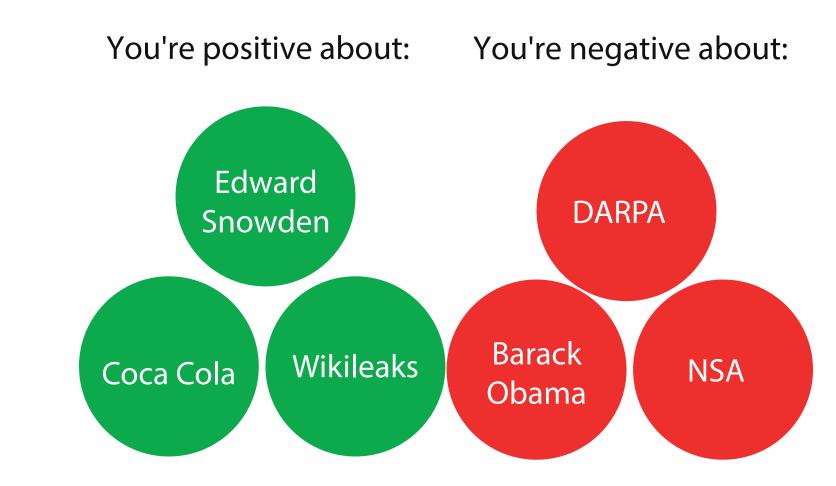
View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- Let 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:



...Sentiments

ZIP Extractor wants to:

obtain permissions it doesn't need

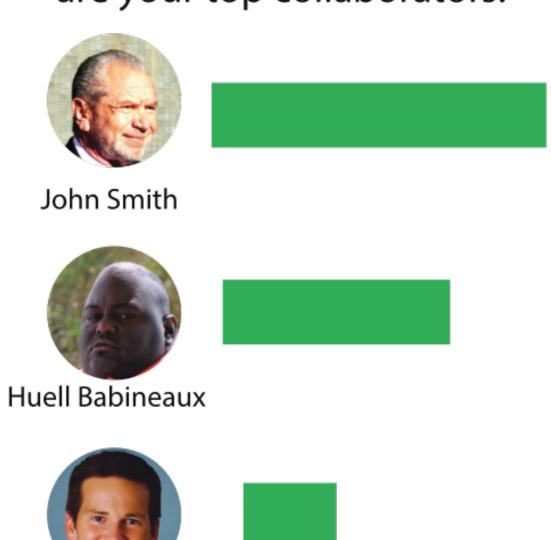
View the files in your Google Drive

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

Adam Kerry

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
- Let 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

ZIP Extractor wants to:

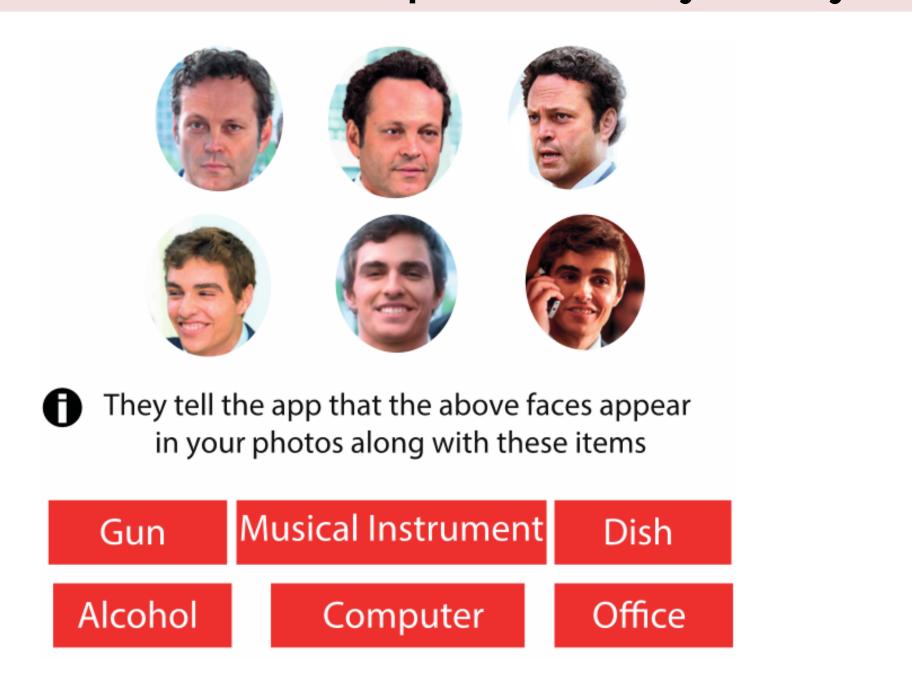
obtain permissions it doesn't need

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?



...Faces with Context

ZIP Extractor wants to:

obtain permissions it doesn't need

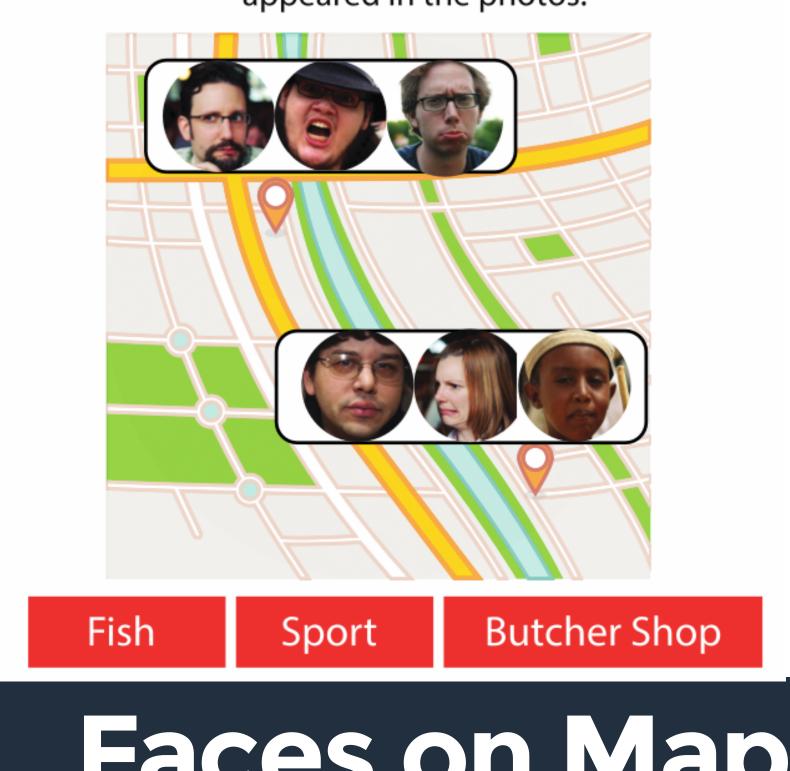
View the files in your Google Drive

obtain permissions it needs to function

- View your basic profile info
- View your email address
- View and manage Google Drive files and fold 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.

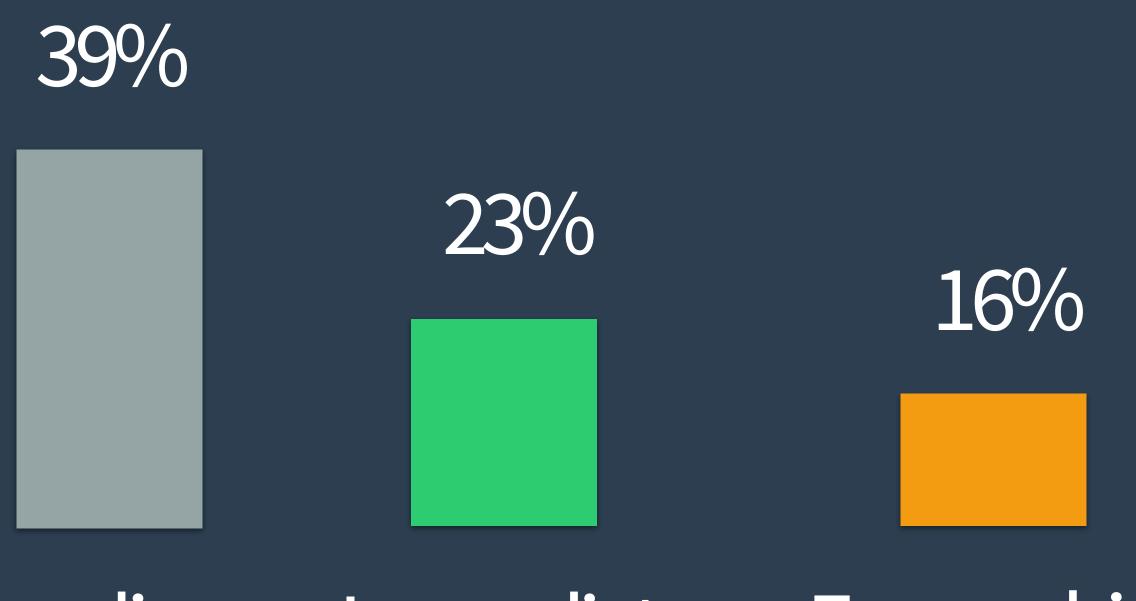


...Faces on Map

Inefficacy of Baseline Permissions

Acceptance Likelihood

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

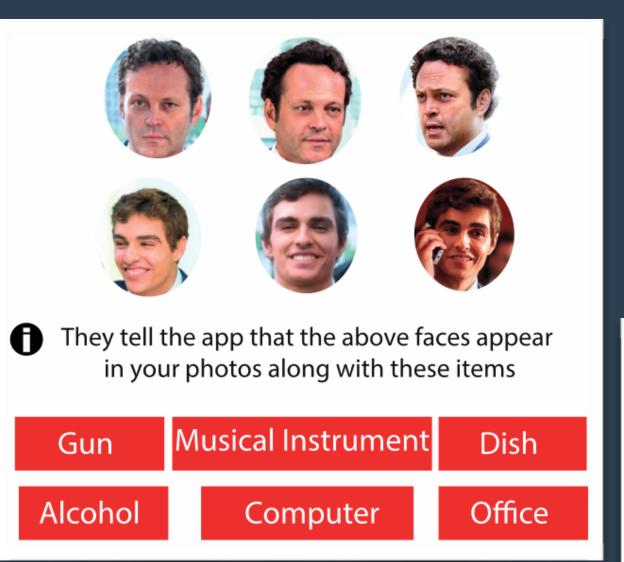


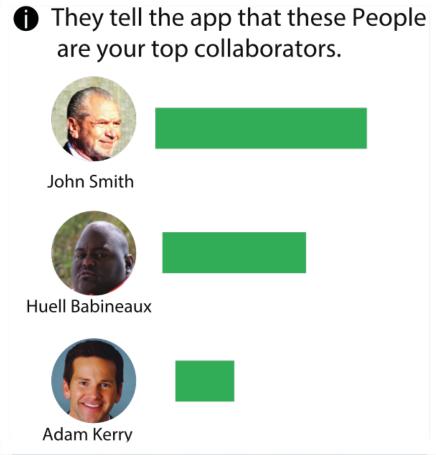
- Online experiment
- Actual user's data
- 160 participants in 3 groups
- GLMMs for significance tests

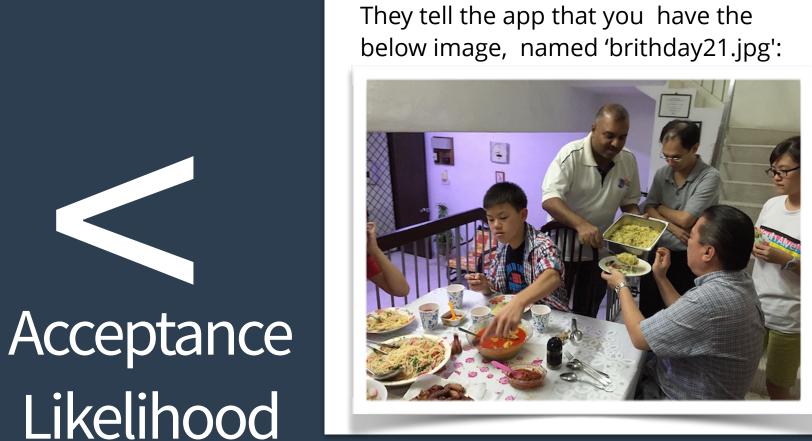
Baseline Immediate Far-reaching

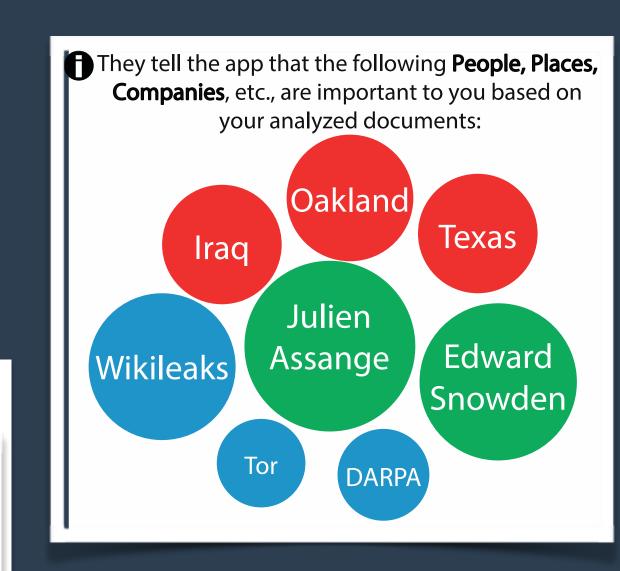
*H. Harkous, R. Rahman, B. Karlas, and K. Aberer.
"The Curious Case of the PDF Converter that Likes Mozart:
Dissecting and Mitigating the Privacy Risk of Personal Cloud Apps", PoPETs

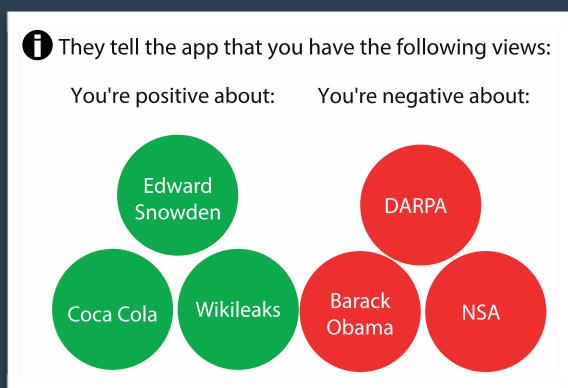
The Power of Relational Insights

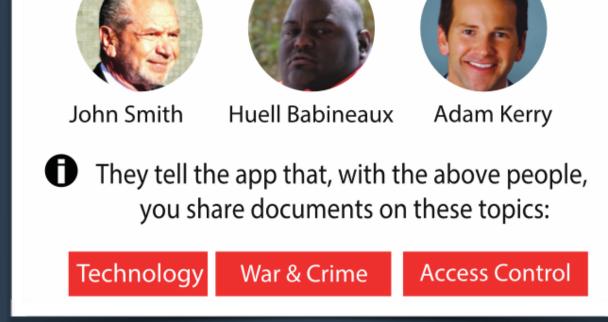




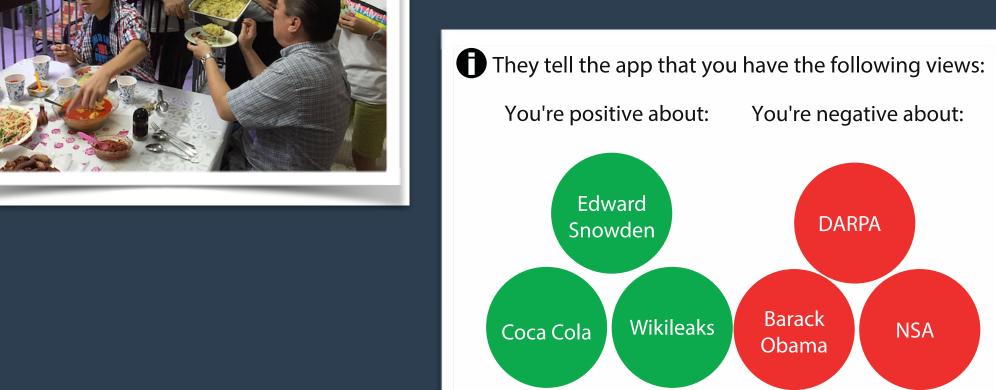




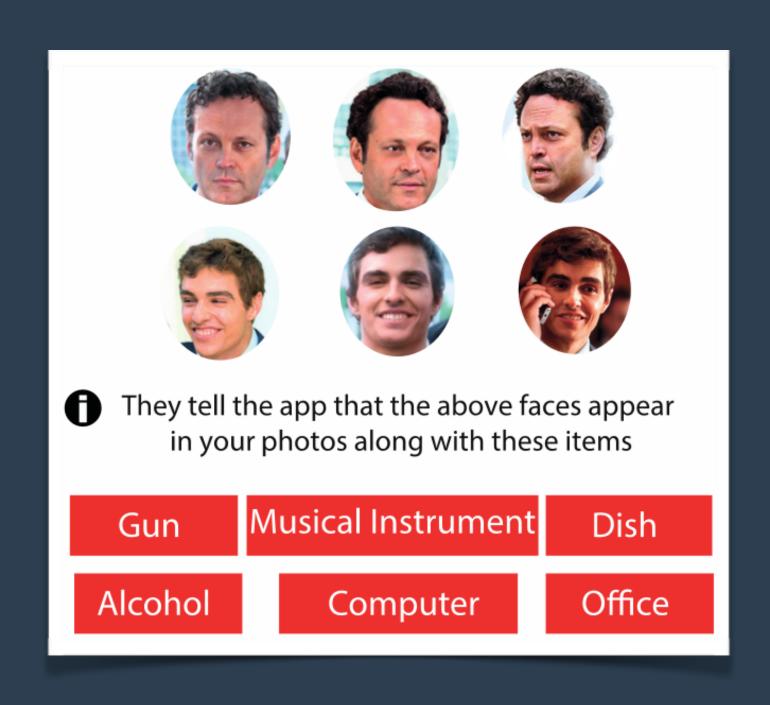








Impact of Face Recognition





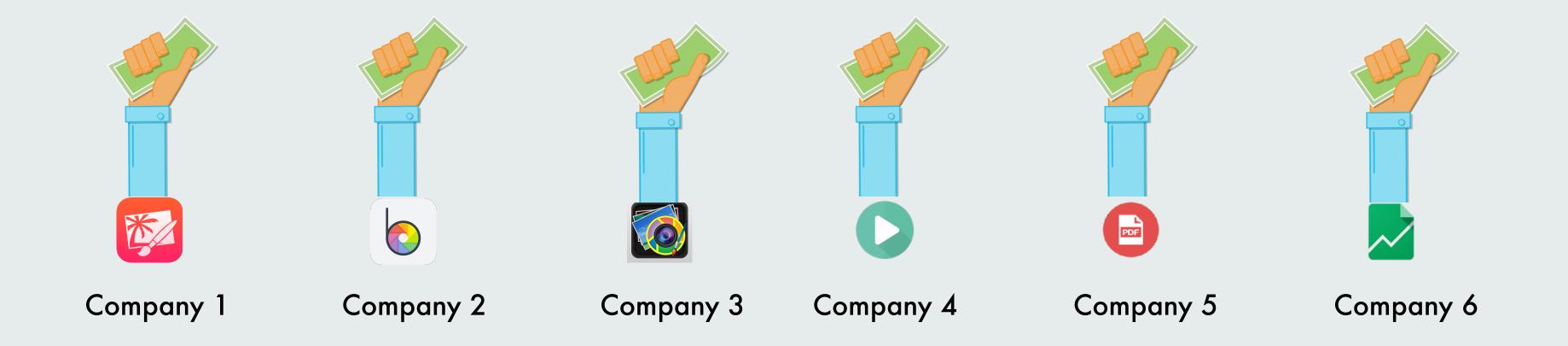


8%

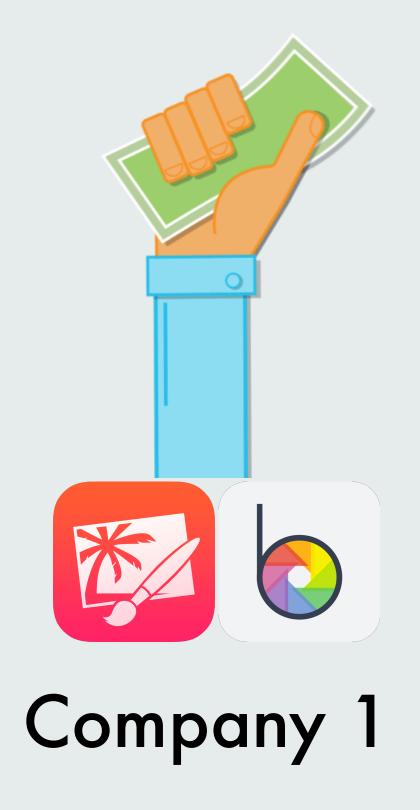
21%

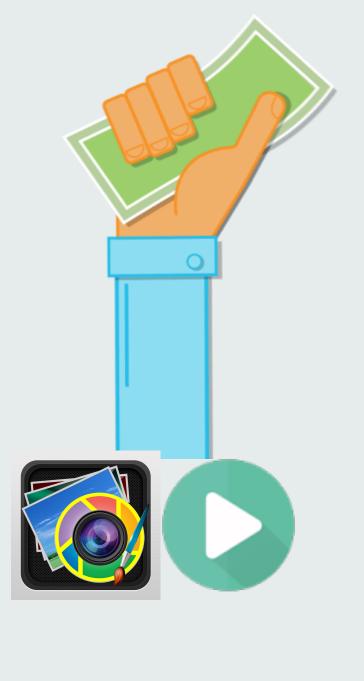
Problem 2: Minimizing Interdependent Privacy

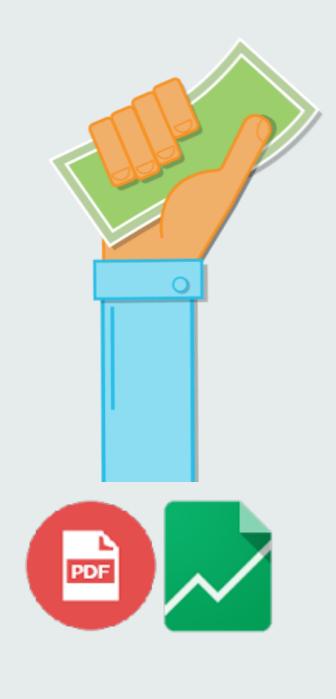




Too Many Shareholders → Larger Attack Surface

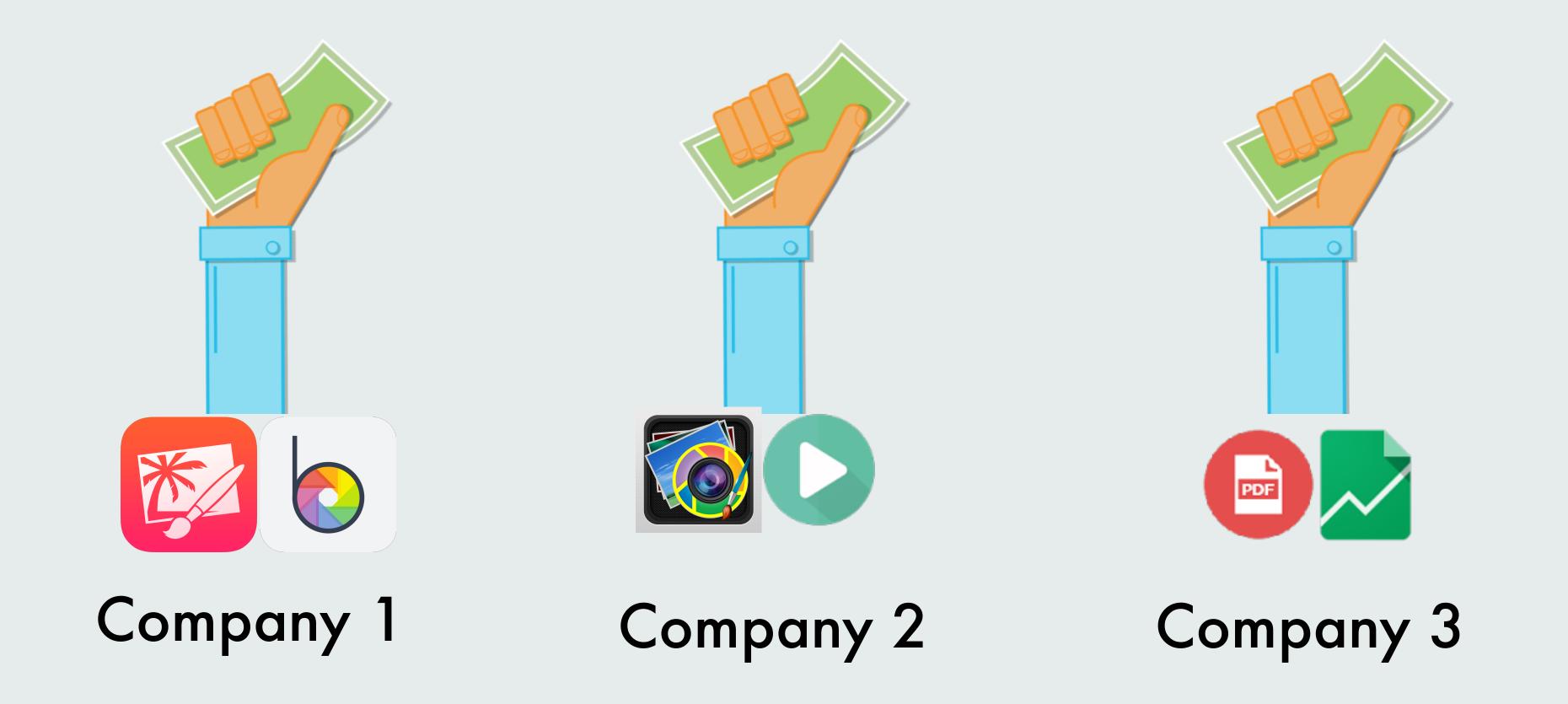






Company 2

Company 3

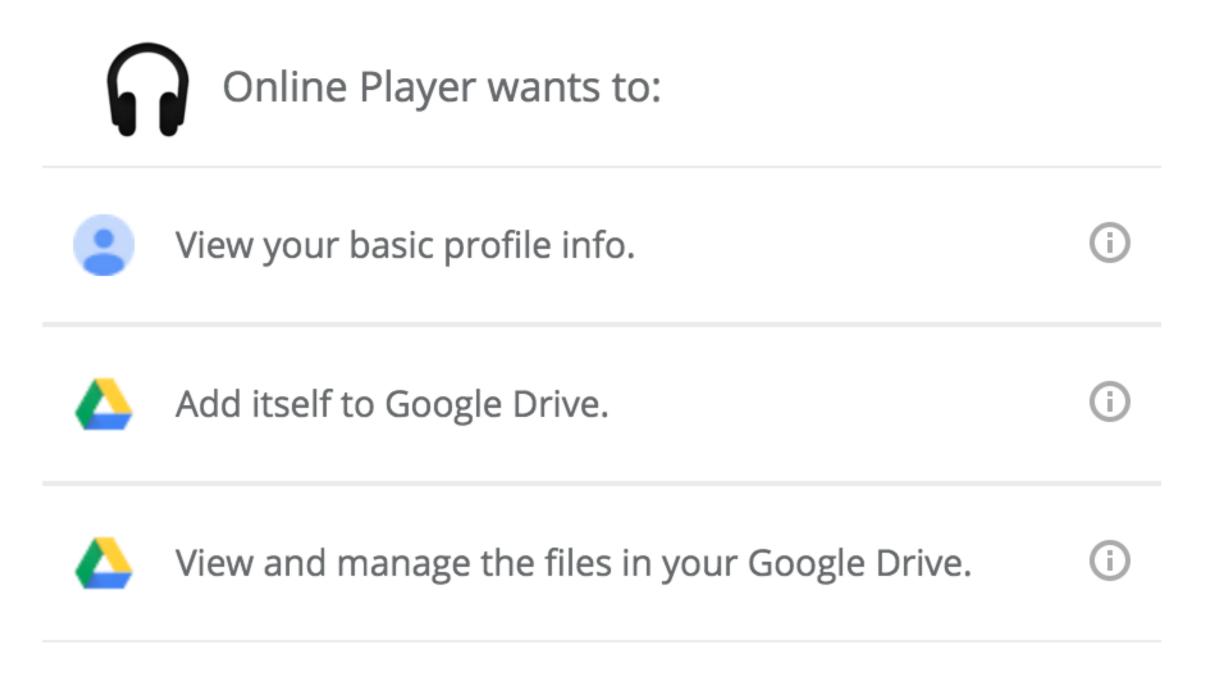


Fewer Shareholders -> Better Privacy

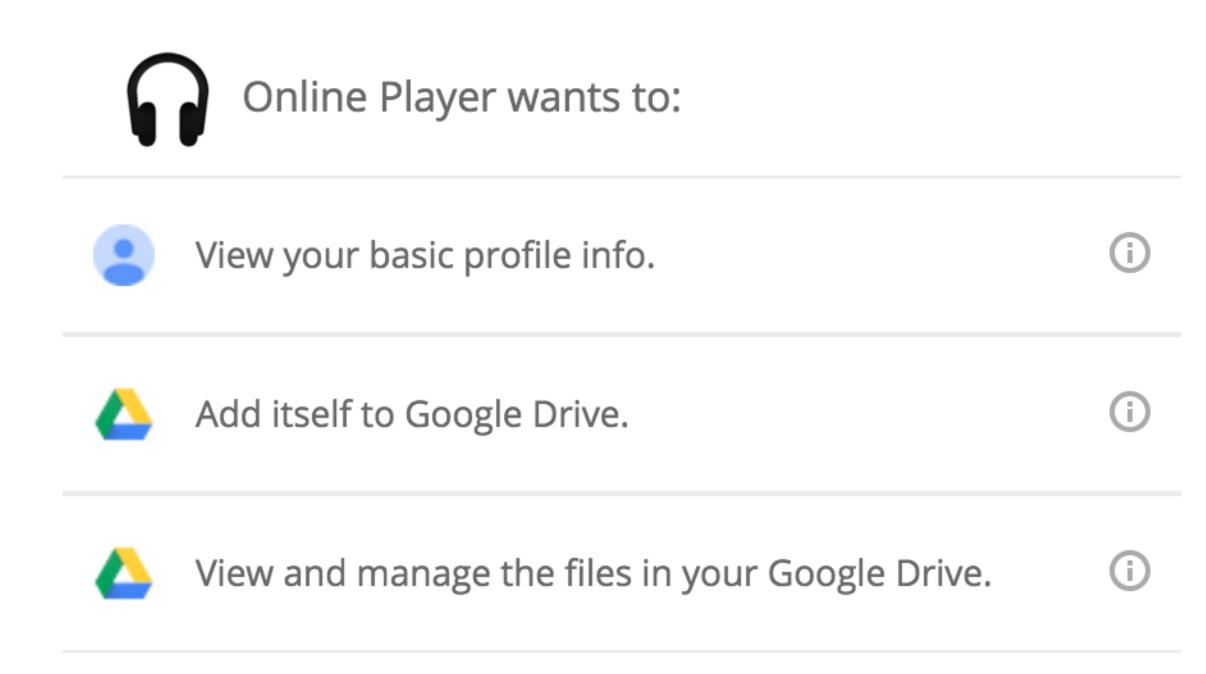
History-based Insights

- 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



The app's company (**driveplayer.com**) already has access to:

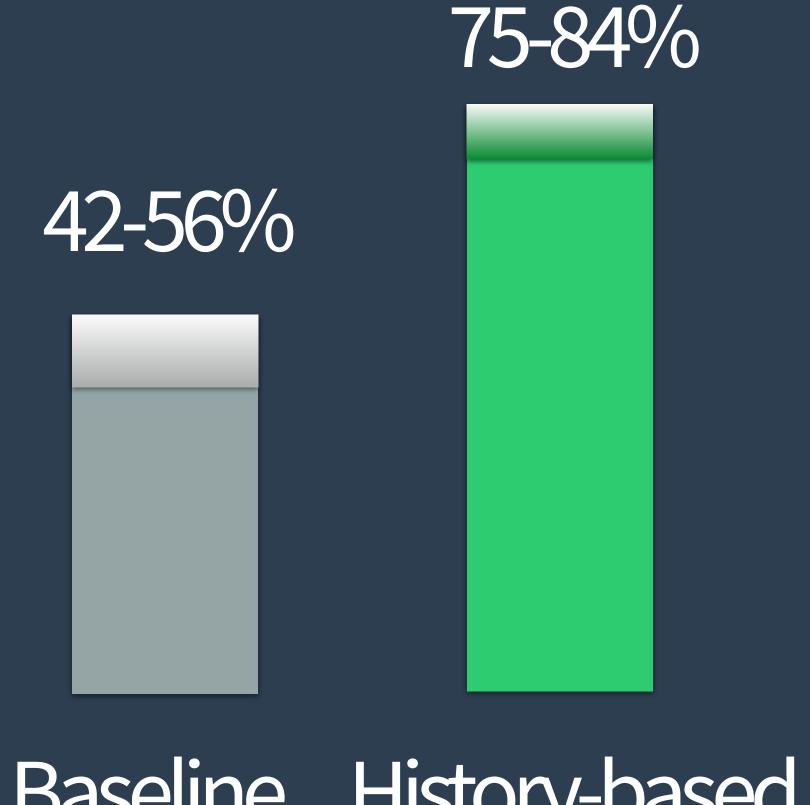
70% of your files

Your friend Lisa has already installed an app from **driveplayer.com**. So this company already has access to the files you share with Lisa.

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

Baseline History-based

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

NewDDPIs

- 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?



3

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