Addressing the Digital Address Books' (Interdependent) Privacy Issues


Kavous S. Niksirat
UNIL / MPI-SP


Lev Velykoivanenko
UNIL


Samuel Mätzler
UZH


Stephan Mulders
UM


Aurelia Tamò-Larrieux
UNIL


Marc-Olivier Boldi
UNIL


Mathias Humbert
UNIL


Kévin Huguenin
UNIL

UNIL | Université de Lausanne

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

Universität Zürich[UZH]

Maastricht University

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Interdependent Privacy

Situations where an individual's privacy is compromised by others (i.e., actions of some individuals affect the privacy of other individuals)

- Online Social Networks
- (Co-) Location-based Services
- Genomics data
- Smartphone app permission
- Voice Assistants*
- Smart Homes*
- Augmented Reality

*also known as *bystander privacy* in some contexts

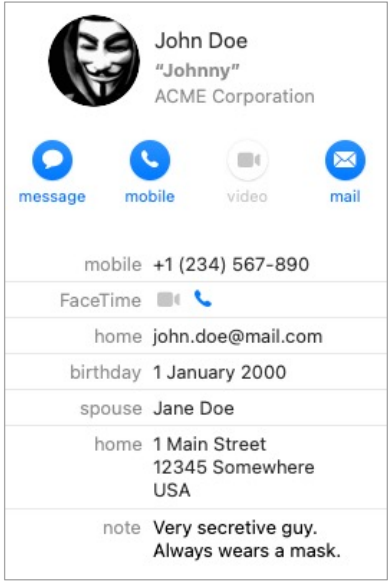
Digital Address Books, or phone book, or contact → **DABs**

DABs

Individuals store PII of *other* individuals in a structured way in their DABs, which they often sync with online services.

This often happens without data subjects' consent or even their awareness!

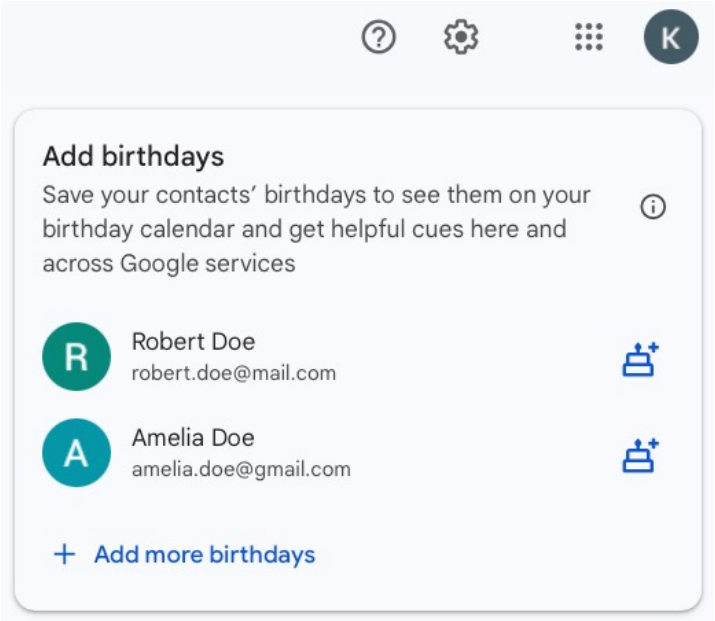
DABs are a simple, yet fundamental, example of interdependent privacy.



DABs

In some cases, DAB service providers even actively encourage their users to input more PII about their contacts.

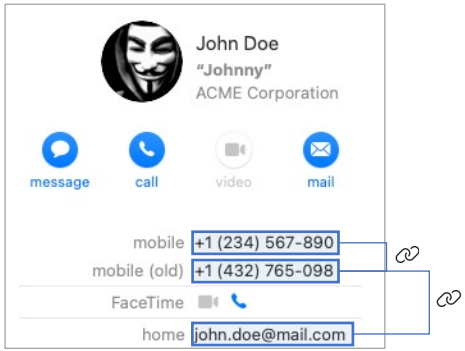
For example, Google does so for birthdays.



DABs

⚠ The privacy risk is straightforward!

Profiling (possibly non-users, cf. shadow profiles)!

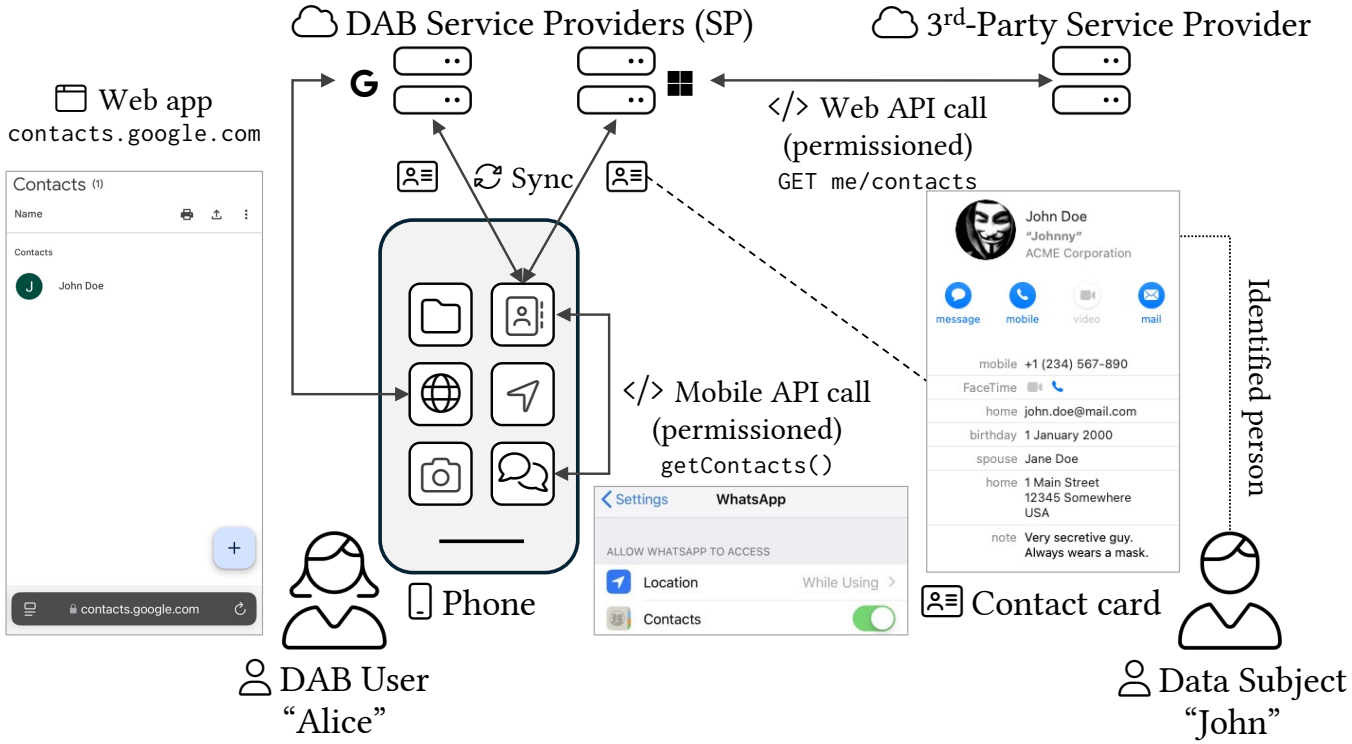


Profile of +1 (234) 567-890

Profile of +1 (432) 765-098

Profile of john.doe@mail.com

Ecosystem


DAB Service Providers (SP)
3rd-Party Service Provider
Web app
contacts.google.com
Contacts (1)
Name
Contacts
John Doe
contacts.google.com
Sync
</> Web API call
(permissioned)
GET me/contacts
John Doe
"Johnny"
ACME Corporation
message
mobile
video
mail
mobile +1 (234) 567-890
FaceTime
home john.doe@mail.com
birthday 1 January 2000
spouse Jane Doe
home 1 Main Street
12345 Somewhere
USA
note Very secretive guy.
Always wears a mask.
Identified person
</> Mobile API call
(permissioned)
getContacts()
Settings
WhatsApp
ALLOW WHATSAPP TO ACCESS
Location
While Using
Contacts
Phone
Contact card
DAB User
"Alice"
Data Subject
"John"

Research Questions

RQ1. How do users interact with their DABs, what contact data do they store, and how complete are their DABs?

RQ2. How do users perceive the privacy risks associated with storing others' personal data, and what is their level of awareness and support for enforcing the data protection rights (e.g., access) of those individuals?

RQ3. What kinds of privacy-preserving remedies do users envision to mitigate these risks and support these rights?

Study Overview

- **Study 1**
  - Large-scale online survey (463)
  - Focus: Self-reported use of DABs, perceived privacy risks, and data rights
- **Study 2**
  - Large-scale online survey (459)
  - Focus: Actual DAB data collection + behavioral choices about data sharing

Study #1 - Methods

Understand DAB users' (self-reported) usage and (privacy) perceptions

2024 | Prolific | 20 min | 3.5€ | 463

Screener survey: + +

Main survey

- Two roles for respondents (subject, i.e., John, and user, i.e., Alice) with specific phrasings

"Please rate how concerning you find it, from a privacy perspective, when the following personal information about you is stored in someone else's digital address book."

vs.

"Please rate how concerning you find it, from a privacy perspective, when you store the following personal information of someone else in your digital address book."

Study #1 - Methods

DAB Practices: Frequency of use and completeness of contact entries

Data Sharing & Awareness: Access granted to third-party apps and awareness of DAB service providers accessing contact data

Privacy Concerns: Concerns about storing others' data and others storing theirs

Privacy Preferences: Opinions on access, deletion, and correction rights, and perspective-switching between "user" and "subject"

Dashboard Design: Ideas for interfaces to manage one's data in others' DABs

Study #1 – Findings

99.1% reported accessing their DAB from their phone!

41.7% reported never accessing their DAB from a web browser

29.4% reported accessing their DAB from a single platform (their phones)

→ E2E should not be a problem ✓

90.5% reported having at least one app with permission to access their contacts.

Among these, 33.4% had **10+**

#199 Apps, #23 Categories

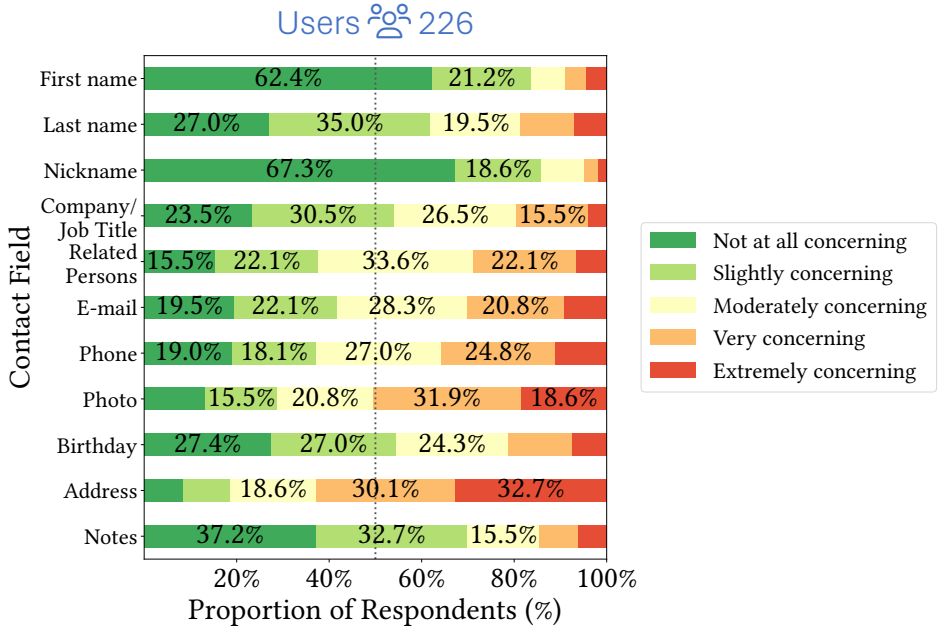
Communication, Social networking, Productivity, Finance, and Travel

Study #1 – Findings

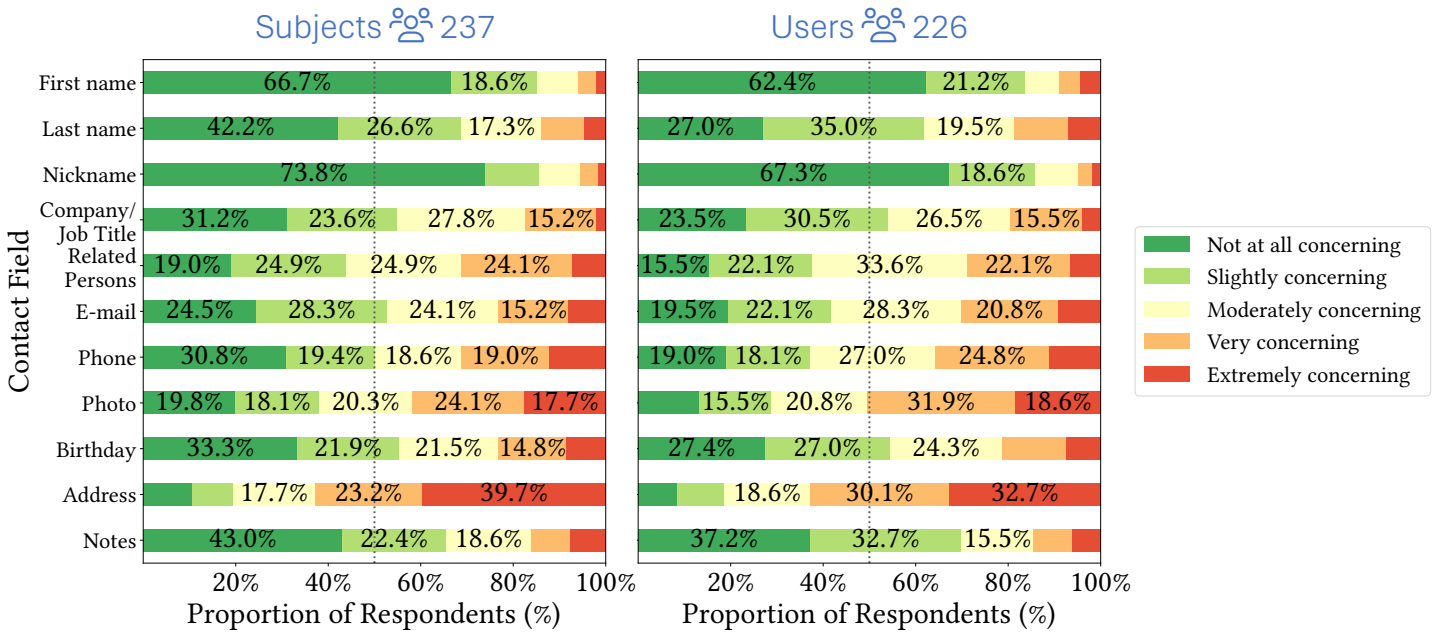
80.8% expressed some agreement (i.e., at least *"somewhat agree"*) when asked whether the DAB Service provider could technically access (in the clear) the data users store in their DABs

→ Good understanding ✓

Privacy Concerns



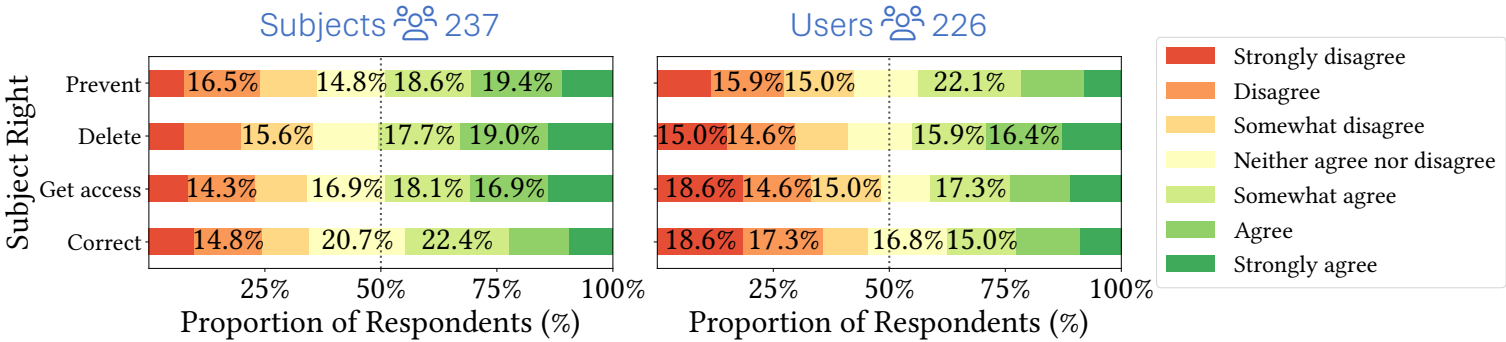
Study #1 – Findings 👁 ☹



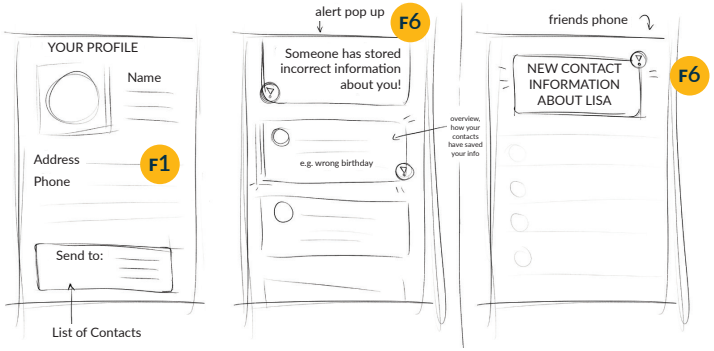
Study #1 – Findings

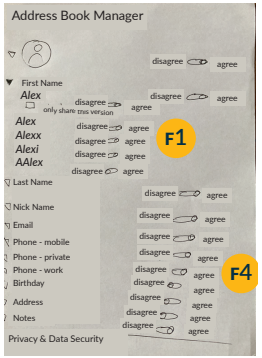
Respondents were mostly in favor of granting data subject rights:

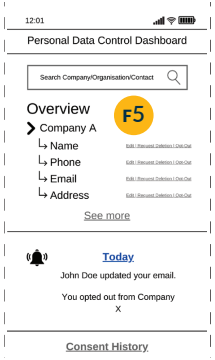
The ability to prevent, delete, access, or correct that data.

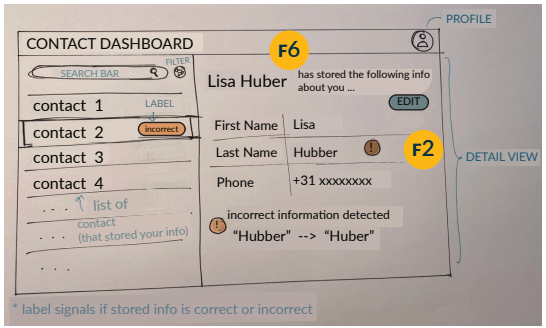


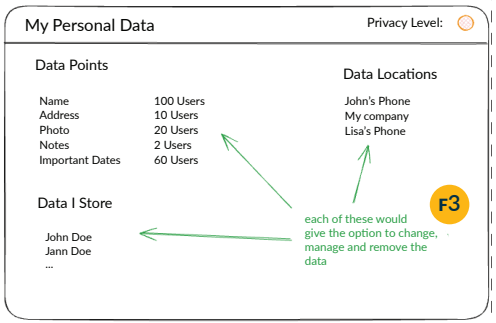
Study #1 – Findings

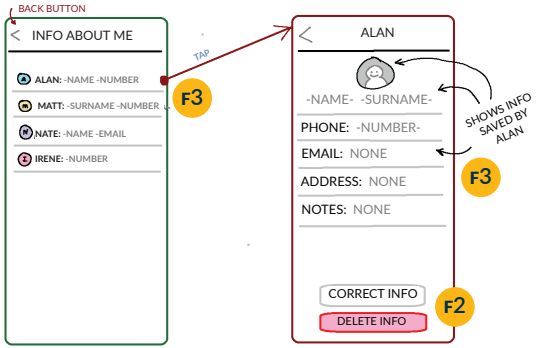












F1: Accurate Information | **F2: Edit & Delete** | **F3: Visualization** | **F4: Access Control** | **F5: Transparency** | **F6: Notifications**

Study #2 - Methods

Collect actual user data and understand their willingness to share their DAB data

2024 | Prolific | 100.0% | 2-5 min | 1$ | 459

Screener survey: + +

AB Main survey: Choose between

(1) granting access to their Google contacts data (incentivized)

(2) manually answering questions about it

(3) quitting

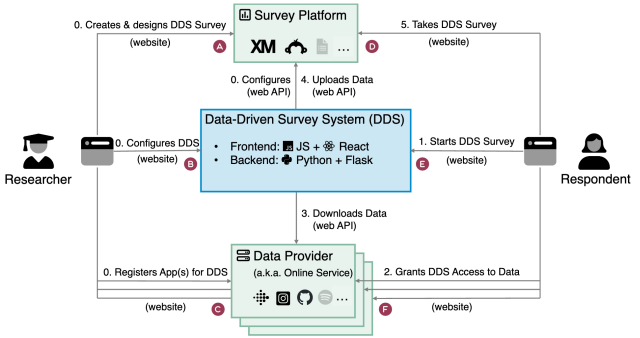
Study #2 - Methods

💰 Incentive variation: multiple batches (~120 each) | 4 waves with different incentives ($0, $1, $2, $5)

🔓 Granted access via DDS*

✋ Manual response: Asked why they preferred not to share

🚫 Never share scenario: Asked why they trusted Google but not researchers



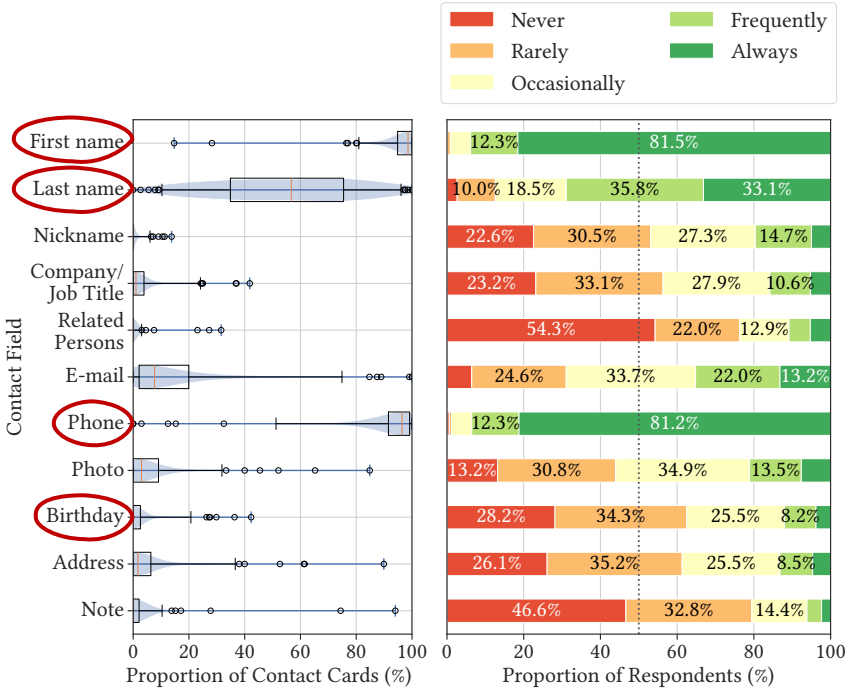
https://github.com/DataDrivenSurveys/DataDrivenSurveys

**Velykoivanenko, L., et al. Designing a data-driven survey system: leveraging participants' online data to personalize surveys. CHI'24.*

Study #2 – Findings 🔁

- Half of the respondents had a birthday in around 3.6% of their contact cards.
- But even 3.6% is meaningful!
- Even with 3.6% chance that a user includes the birthday, if an individual appears in the DABs of 50 users, then there is an **86%** chance that the service provider has their birthday!

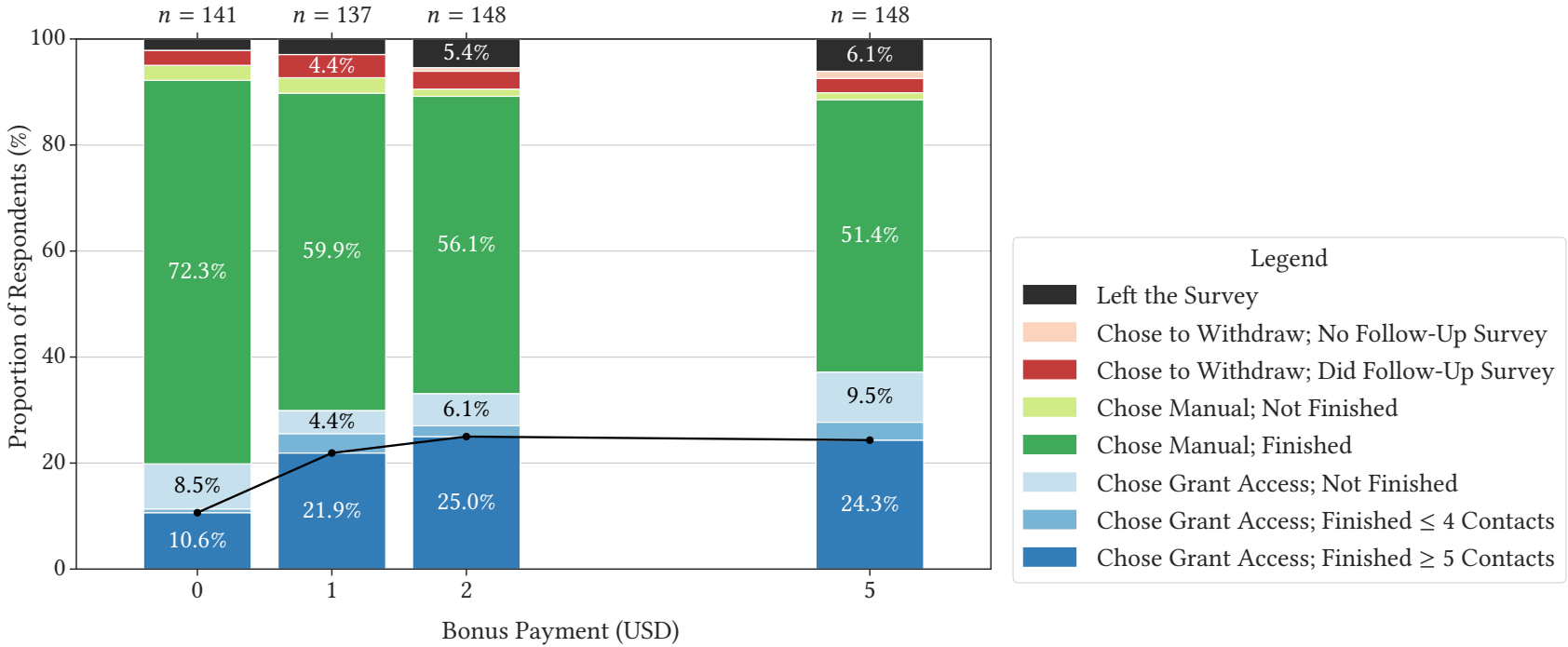
$$100\%-(100\%-3.6\%)^{50} = 86\%$$



Actual data
118

Self-reported data
341

Study #2 – Findings



Study #2 – Findings ⚖ 66

Chose Grant Access	Chose Manual	Chose to Withdraw
• Convenience • Financial Compensation • Lack of Privacy Concerns	• Privacy Concerns • Interdependent Privacy Concerns	• Privacy Concerns

"I know the data is safe in your hands." [NB, 36 y.o.]

"I wasn't really worried about it. I don't have any secret contacts." [W, 66 y.o.]

"I like to keep my privacy." [W, 43 y.o.]

"I don't want to reveal other people's private contact information without their permission." [M, 45 y.o.]

Study #2 – Findings 66

Would you share for money?

- ~1/3 of (manual) respondents would consider granting access if compensated
- Median request: $15 (range: $12.5 to $35)

Why Google, Not Researcher?

"Google has a reputation for safeguarding user information and is a well-known and established company." [W, 65 y.o.]

"Because Google is Google. You are a random researcher on the Internet." [M, 44 y.o.]

"It is more or less a necessary evil to have functionality and ease of use." [W, 37 y.o.]

Interdependent Privacy Risks Are Real!
Respondents expressed moderate concern.
Yet ~25% would still share these for a few dollars.

Non-Users Lack Control
People who don't use DAB services are still affected.
Their data ends up stored and potentially processed—without consent.

Utility Justifies Broad Access, but at a Cost
Third-party apps use DABs for functionality, but this overshadows interdependent privacy risks.

Design Leverage: Single-Device Use
Most users access DABs from only one device.
This makes E2EE more feasible.

Users Support Shared Rights!
Many support giving contacts rights over shared data.
Raises a need for rethinking consent and balancing user vs. subject rights.

Link to the full paper