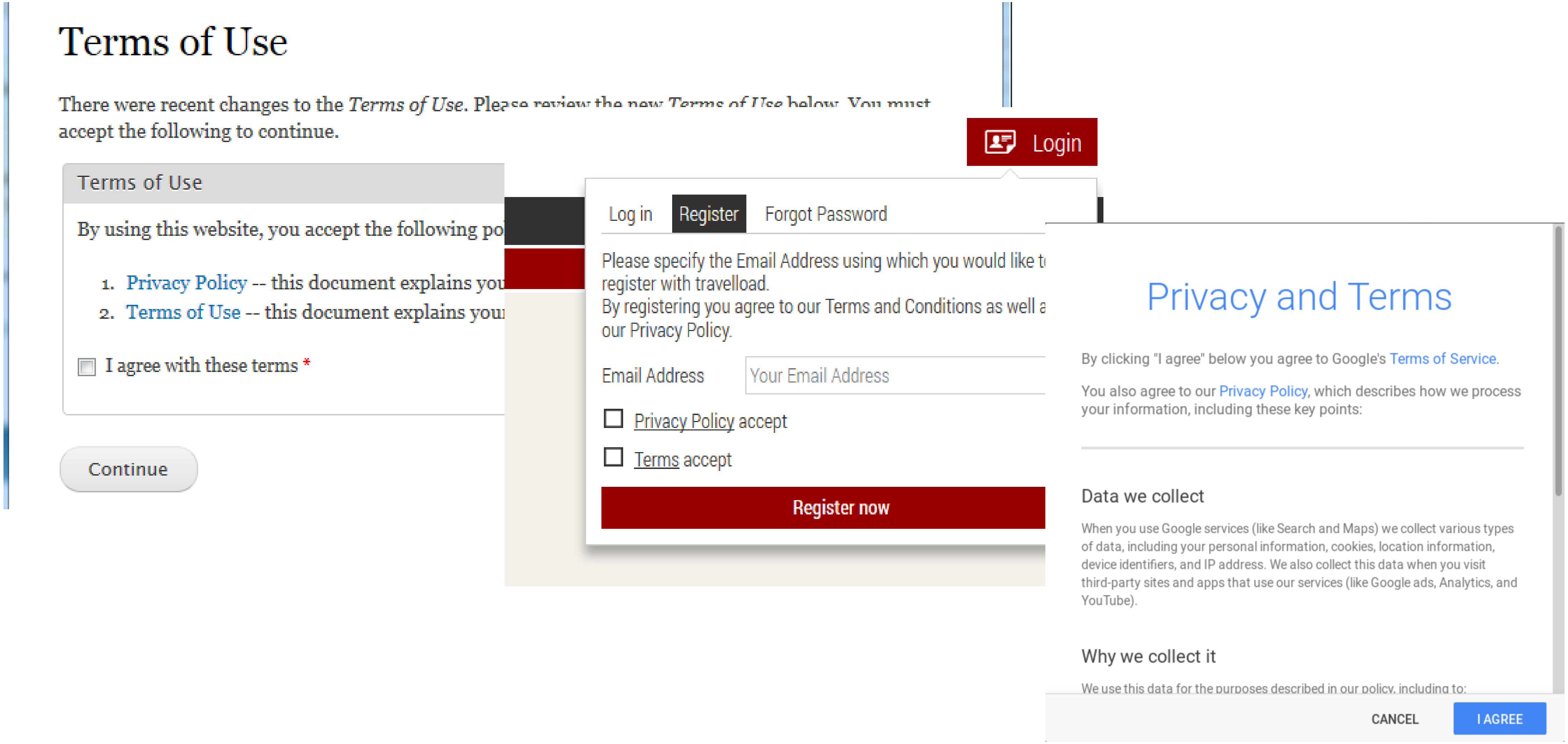
An Automated Negotiation Agent for Permission Management

Tim Baarslag, Centrum Wiskunde & Informatica (CWI)
Alper T. Alan, University of Southampton
Richard Gomer, University of Southampton
Muddasser Alam, University of Oxford
Charith Perera, The Open University
Enrico H. Gerding, University of Southampton
M.C. Schraefel, University of Southampton

AAMAS, Sao Paolo, May 2017



Terms of Use

There were recent changes to the *Terms of Use*. Please review the new *Terms of Use* below. You must accept the following to continue.

Terms of Use

By using this website, you accept the following po

1. Privacy Policy -- this document explains you
2. Terms of Use -- this document explains you

□ I agree with these terms *

Continue

Please specify the Email Address using which you would like t register with travelload.
By registering you agree to our Terms and Conditions as well a our Privacy Policy.

Email Address: Your Email Address

□ Privacy Policy accept

□ Terms accept

Register now

Privacy and Terms

By clicking "I agree" below you agree to Google's Terms of Service.

You also agree to our Privacy Policy, which describes how we process your information, including these key points:

Data we collect

When you use Google services (like Search and Maps) we collect various types of data, including your personal information, cookies, location information, device identifiers, and IP address. We also collect this data when you visit third-party sites and apps that use our services (like Google ads, Analytics, and YouTube).

Why we collect it

We use this data for the purposes described in our policy, including to:

Meaningless consent

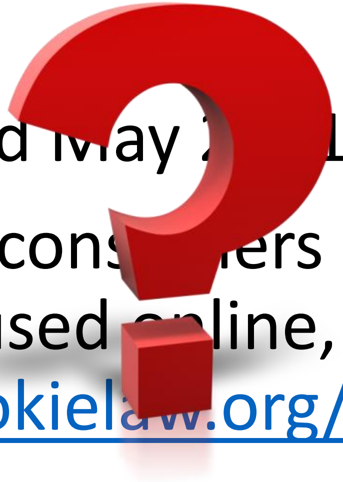
Despite being asked to "agree" constantly to terms of service, consent is not currently "meaningful.”

- It is **impossible** to read all the terms and conditions
- Even if we read them, they are clouded in legal language and **difficult to understand** what it means in practice for most people
- Privacy policies are often high level and do not specify exactly **who** receives our personal data **how** it is being used
- There is often **no real choice**: it is a take-it-or-leave-it proposition

Why is this important?

- Increasing amount information is being collected
  - Browsing
  - Social media
  - Mobile devices
  - *Internet of Things*
- Potential *privacy* issues
  - Many apps collect personally identifiable information (PII) such as voice, contacts, browsing history, text messages, location, etc
  - Information is in some cases sold to third parties
- Leads to mistrust and loss of revenue, and e.g. ad blockers

Current Legal Solutions



- EU Cookie Law, adopted May 2 1
- The goal was to `make cons ers aware of how information about them is collected and used online, and give them a choice to allow it or not' http://www.cookielaw.org/the-cookie-law/
- Issues:
  - Not many people ur kies are
  - Still not clear how ir used
  - Often there is no ch

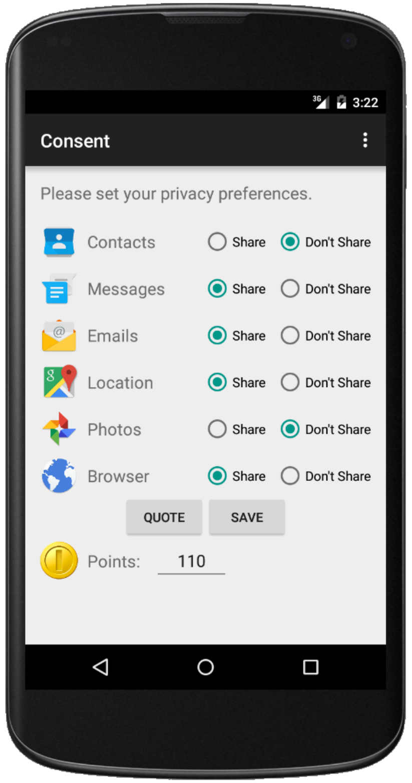
Opportunities for Agent-Based Research

In the age of big data and the Internet of Things, one can no longer rely on making all decisions manually. Agents can:

- Elicit privacy preferences
- Make privacy setting recommendations
- Automate privacy decisions
- Negotiate privacy agreements

Negotiating App Permissions

- We developed an Android App with no intrinsic functionality
- Negotiate access to data in return for “points”
  - Represents level of service obtained
- Mined from users’ smartphones: access to all
  - Contacts
  - Messages
  - Apps
  - Photos
  - Browsing history



Consent

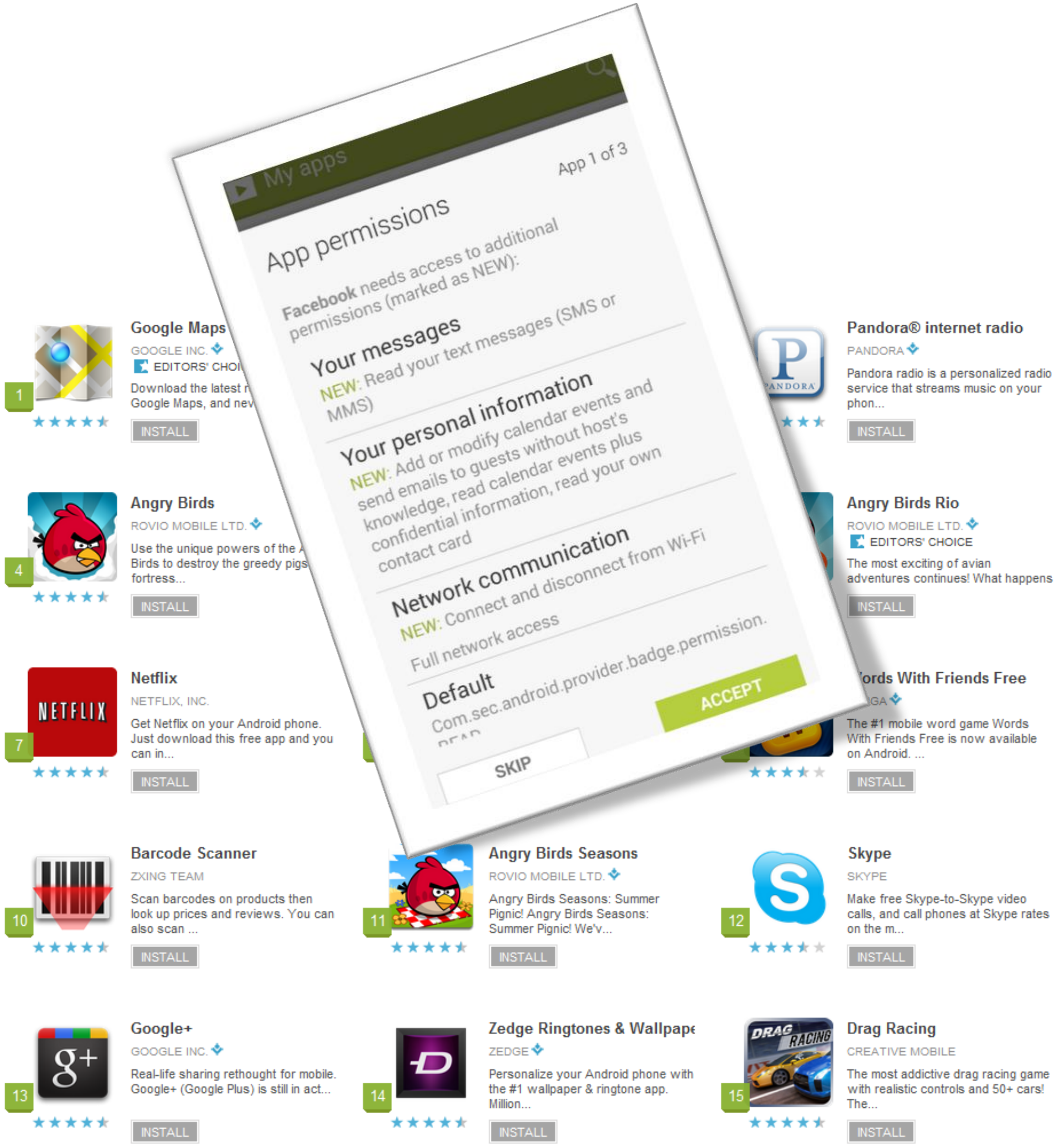
Please set your privacy preferences.

Contacts	○ Share	● Don't Share
Messages	● Share	○ Don't Share
Emails	● Share	○ Don't Share
Location	● Share	○ Don't Share
Photos	○ Share	● Don't Share
Browser	● Share	○ Don't Share

Points: 110

Why app permissions?

- Access to very privacy sensitive content
- Permissions give no understanding of how information is used
- Clearly defined domain (compared to terms and conditions)
- Users are already familiar with this domain
- Easy to do controlled experiments



My apps

App permissions

App 1 of 3

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

Default

Com.sec.android.provider.badge.permission.

ACCEPT

SKIP

1 Google Maps — GOOGLE INC. — EDITORS' CHOI — Download the latest r Google Maps, and nev — INSTALL

Pandora® internet radio — PANDORA — Pandora radio is a personalized radio service that streams music on your phon... — INSTALL

4 Angry Birds — ROVIO MOBILE LTD. — Use the unique powers of the Birds to destroy the greedy pigs fortress... — INSTALL

Angry Birds Rio — ROVIO MOBILE LTD. — EDITORS' CHOICE — The most exciting of avian adventures continues! What happens — INSTALL

7 Netflix — NETFLIX, INC. — Get Netflix on your Android phone. Just download this free app and you can in... — INSTALL

ords With Friends Free — The #1 mobile word game Words With Friends Free is now available on Android. ... — INSTALL

10 Barcode Scanner — ZXING TEAM — Scan barcodes on products then look up prices and reviews. You can also scan ... — INSTALL

11 Angry Birds Seasons — ROVIO MOBILE LTD. — Angry Birds Seasons: Summer Pignic! Angry Birds Seasons: Summer Pignic! We'v... — INSTALL

12 Skype — SKYPE — Make free Skype-to-Skype video calls, and call phones at Skype rates on the m... — INSTALL

13 Google+ — GOOGLE INC. — Real-life sharing rethought for mobile. Google+ (Google Plus) is still in act... — INSTALL

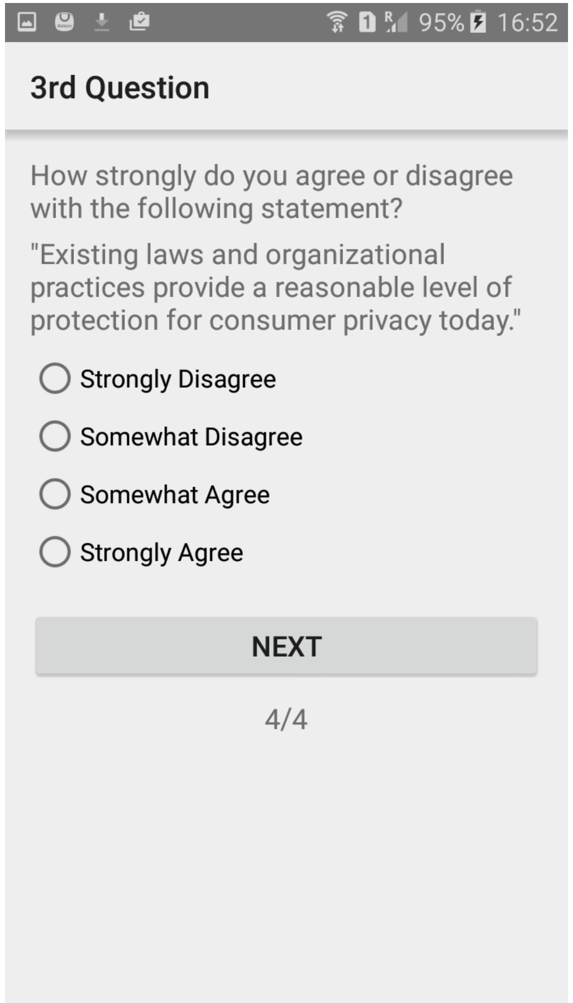
14 Zedge Ringtones & Wallpape — ZEDGE — Personalize your Android phone with the #1 wallpaper & ringtone app. Million... — INSTALL

15 Drag Racing — CREATIVE MOBILE — The most addictive drag racing game with realistic controls and 50+ cars! The... — INSTALL

Pre-Study Questionnaire

Users are asked demographics questions and 3 questions for deriving of a user's *privacy type* using *Weston's Privacy Segmentation Index*:

- **Fundamentalists** (15%): most protective of privacy
- **Pragmatists** (79%): weigh the potential pros and cons
- **Unconcerned** (6%)



3rd Question

How strongly do you agree or disagree with the following statement?

"Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today."

○ Strongly Disagree

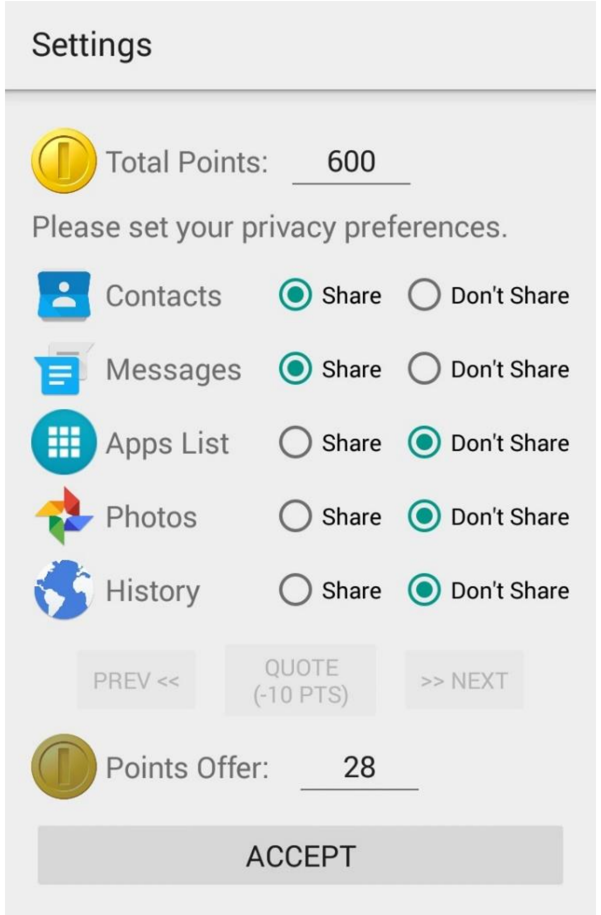
○ Somewhat Disagree

○ Somewhat Agree

○ Strongly Agree

Negotiation Process

- User gets a “default” setting with a given set of permission and number of points
- Users can choose what permissions to share and press “quote” to receive an offer in terms of points
- Each quote has a small quoting cost, representing effort when users do this in real settings
- The user can then accept, press a new quote, or revisit a previous offer. They can also turn all permissions off and receive no points.



Settings

Total Points: 600

Please set your privacy preferences.

Contacts	● Share	○ Don't Share
Messages	● Share	○ Don't Share
Apps List	○ Share	● Don't Share
Photos	○ Share	● Don't Share
History	○ Share	● Don't Share

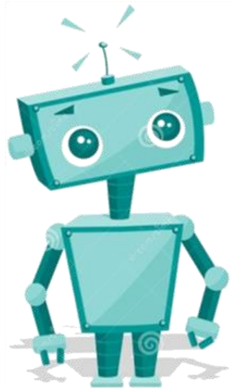
Points Offer: 28

The Negotiation Agent

- The agent learns the preferences of the user (more about it on the next slide)
- Agent negotiates behind the scene by requesting quotes
  - Uses Pandora's algorithm to find optimal negotiation strategy
- Shows the result through as the default setting
- User can accept or continue to negotiation manually

(users are not aware of the agent)

- Treatment 2: randomly chosen default settings.

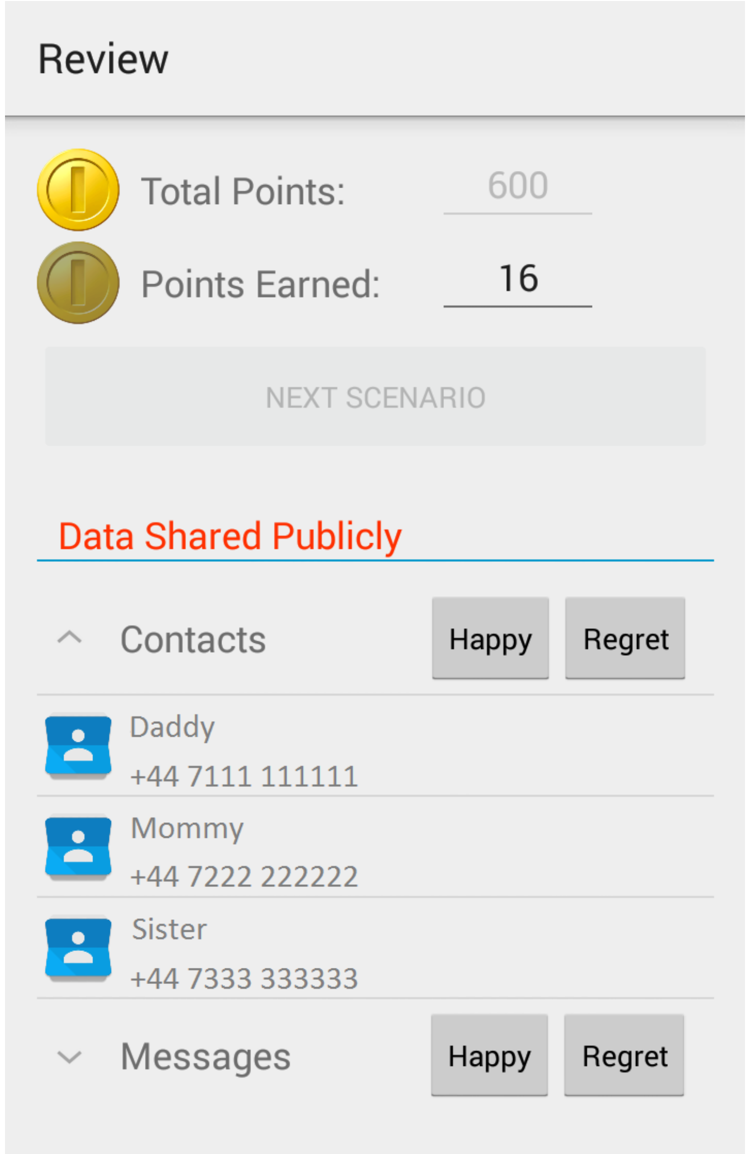


Learning User Preferences

- Results from previous experiments are used to derive preferences for each **privacy type**
- Each negotiation interaction results in a set of linear constraints: e.g.
  - If user agrees to share Contacts and Messages for 28 points, we know that:
    $$U(Contacts + Messages) \leq 28$$
  - If users declined such an offer, we derive that:
    $$U(Contacts + Messages) \geq 28$$
- People of the same type (and even individuals) are not necessarily consistent, and so we find the utility function which *maximises the number of constraints satisfied*
- A user’s privacy type in round 1 is based on “declared” privacy type (from pre-study questionnaire), and in subsequent rounds is updated based on how much users actually share

Review Screen

- 3 randomly-selected items of each category were “shared”
- Users can see exactly what data was shared
- Users can express whether they regret their sharing decision for each of the permissions



Review

Total Points: 600

Points Earned: 16

NEXT SCENARIO

Data Shared Publicly

Contacts Happy Regret

Daddy
+44 7111 111111

Mommy
+44 7222 222222

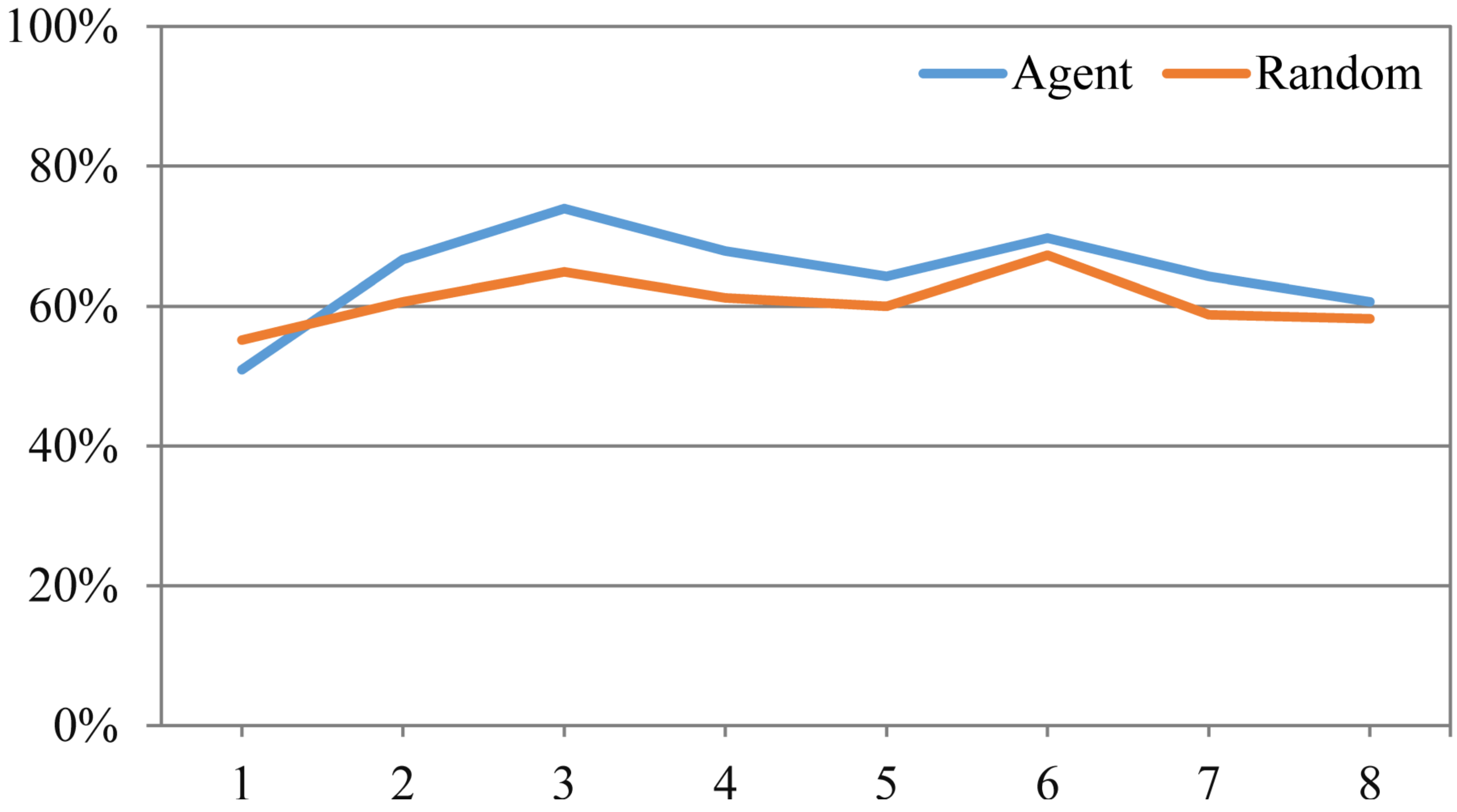
Sister
+44 7333 333333

Messages Happy Regret

Evaluation

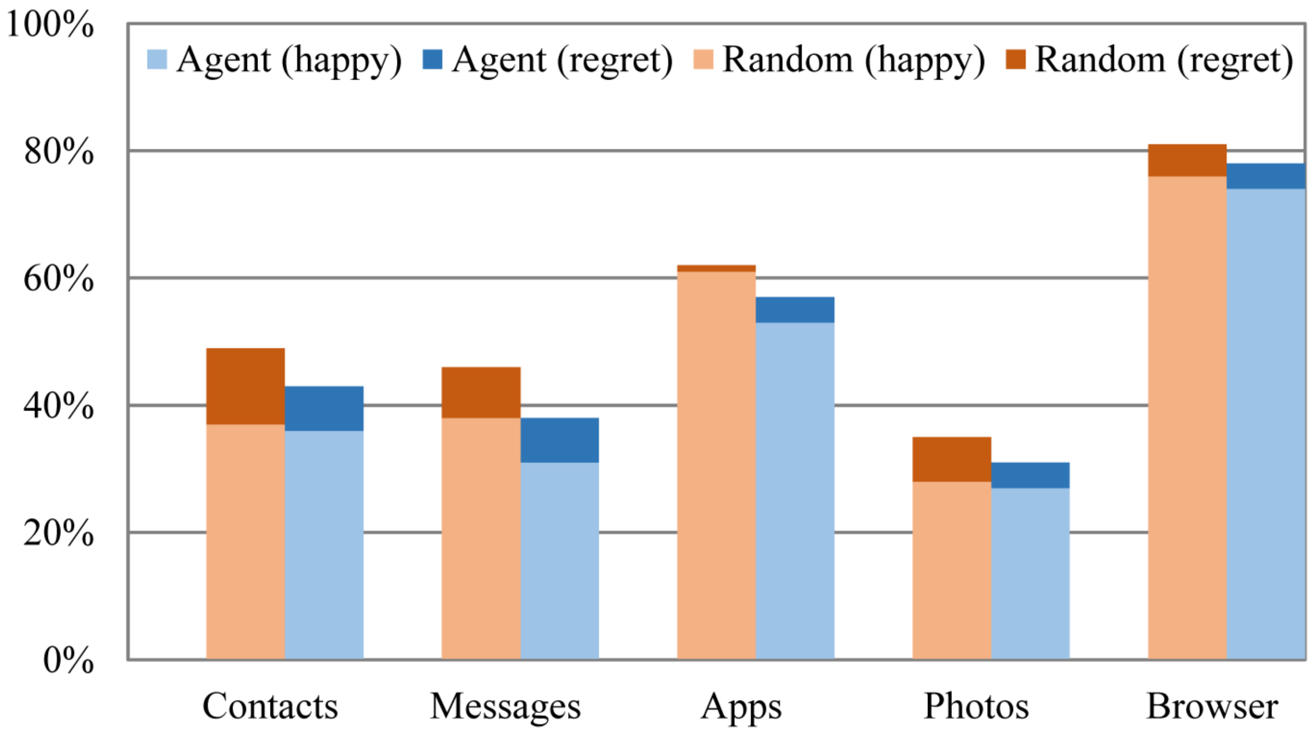
- Lab study in which participants were asked to download the app on their own smartphones
- Deception: any data they shared would be publicly accessible on a website
- Users go through 8 different points scenario.
- Logged user interactions, post-questionnaire and semi-structured interviews
- In total 66 students took part in the study, and received cash between £5 and £10 depending on the overall points earned

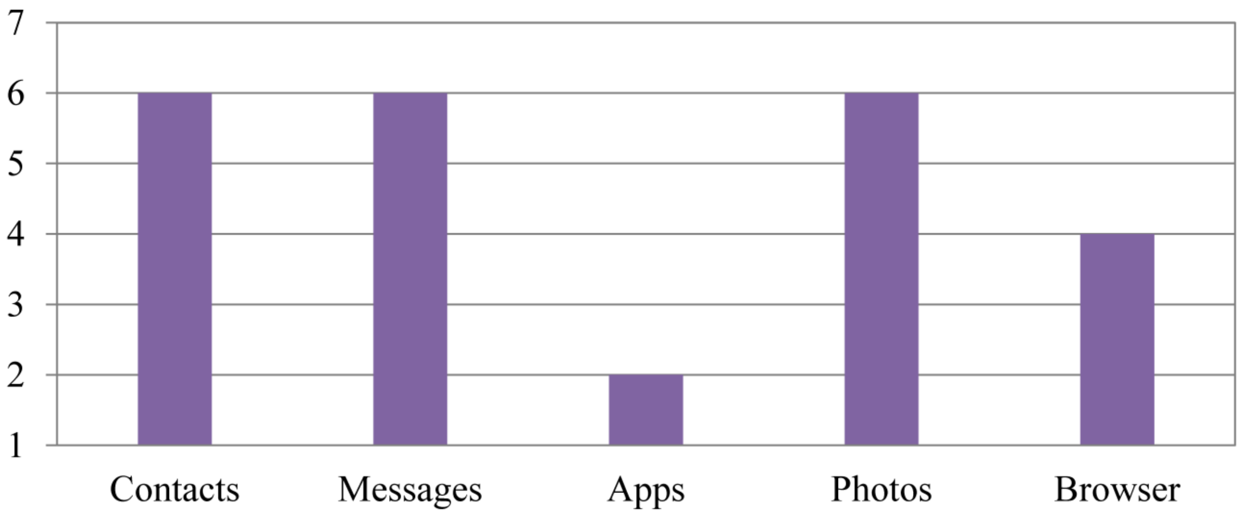
Results: Accuracy



Results: sharing and sensitivity

- Sharing percentages and retrospective feelings are comparable
- User behavior is aligned with their privacy preferences





Main Results

- Our results show that the agent can accurately automate privacy decisions on user behalf in line with normal user behavior
- However, the analysis of NASA TLX show that agent does not cause less overhead
- However, regret is very similar (proportional with amount shared)

Conclusions and Future Work

- Privacy increasingly important in the era of Big Data and the Internet of Things
- Negotiation allows for fine-grained agreements, as opposed to the current take-it-or-leave-it approaches
- This work presents the initial steps towards achieving meaningful consent while minimising user bother
- Future work:
  - Include the uses of data (the recipient, retention period, purpose, quality, and privacy risks) as part of the negotiation domain
  - Include more meaningful classification of data (location, time of day, and relation to other people)
  - Personalized preference models and incremental elicitation
  - Transfer between different applications/devices, e.g. IoT