A Curious Case of “Consent Button”
[... neither do I want to accept, nor decline ...]

Nurul Momen & Lothar Fritsch

Karlstad University

HotPETs, KTH, Stockholm
I want to find an app to wash my hands ...
What happens next?

- Personal data access: a lot more than a user can observe.
- Partial identities can be extracted from privilege usage data.
Good and bad behavior of apps

1. Requirement types (price): what does it ask for & how much of the privilege is being used?
2. Legal requirements: does it comply with the regulations?
3. Crowd-sourced user feedback: what do other users think?
Let's judge an apps' behavior ...


Legend
- Permission-groups requested in Manifest.
- Clarification missing in privacy policy.
- Permission access without user interaction during runtime.
Let's compare with other apps ...

i. Lifesum: 13 (5/3/4/T) [Threat count, T=1]

ii. Endomondo: 9 (5/0/2/T) [Threat count, T=2]

iii. 30dayFitnessChal.: 6 (2/2/0/T) [Threat count, T=2]


v. Pedometer: 13 (6/3/2/T) [Threat count, T=2]

vi. MyFitnessPal: 9 (6/2/0/T) [Threat count, T=1]


viii. 7minsWorkout: 6 (2/2/0/T) [Threat count, T=2]

ix. Fitbit: 20 (8/3/5/T) [Threat count, T=5]

x. GoogleFit: 10 (5/0/3/T) [Threat count, T=2]

Permission-groups requested in Manifest.
Clarification missing in privacy policy.
Permission access without user interaction during runtime.

But, apps change requirements!

Overview of data collection periods.

### Change of privilege-requirements

<table>
<thead>
<tr>
<th></th>
<th>Communication apps</th>
<th>Social apps</th>
<th>Fitness apps</th>
<th>Weather apps</th>
<th>Music apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telegram</td>
<td>A</td>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viber</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsApp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instagram</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whatsapp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Change of privilege usage pattern

<table>
<thead>
<tr>
<th>Communication apps</th>
<th>Social apps</th>
<th>Fitness apps</th>
<th>Weather apps</th>
<th>Music apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tango (8)</td>
<td>Lyft (7)</td>
<td>7 minWorkout (23)</td>
<td>Yandex Weather (14)</td>
<td>Imo (45)</td>
</tr>
<tr>
<td>LinkedIn (33)</td>
<td>MyFitnessPal (22)</td>
<td>71.05</td>
<td>Yandex Weather (14)</td>
<td>SoundCloud (9)</td>
</tr>
<tr>
<td>Pedometer (29)</td>
<td>Endomondo (26)</td>
<td>83.33</td>
<td>WeatherBug (16)</td>
<td>Shazam (8)</td>
</tr>
<tr>
<td>Tango (8)</td>
<td>MyFitnessPal (22)</td>
<td>43.72</td>
<td>WeatherBug (16)</td>
<td>Tidal (7)</td>
</tr>
<tr>
<td>LinkedIn (33)</td>
<td>Endomondo (26)</td>
<td>37.5</td>
<td>WeatherBug (16)</td>
<td>SongFlip (6)</td>
</tr>
<tr>
<td>Pedometer (29)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>BBCiPlayer (5)</td>
</tr>
<tr>
<td>Tango (8)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>Deezer (4)</td>
</tr>
<tr>
<td>LinkedIn (33)</td>
<td>Endomondo (26)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>PlayMusic (3)</td>
</tr>
<tr>
<td>Pedometer (29)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>JangoRadio (2)</td>
</tr>
<tr>
<td>Tango (8)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>iHeartRadio (1)</td>
</tr>
<tr>
<td>LinkedIn (33)</td>
<td>Endomondo (26)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>BBCiPlayer (5)</td>
</tr>
<tr>
<td>Pedometer (29)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>Deezer (4)</td>
</tr>
<tr>
<td>Tango (8)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>PlayMusic (3)</td>
</tr>
<tr>
<td>LinkedIn (33)</td>
<td>Endomondo (26)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>JangoRadio (2)</td>
</tr>
<tr>
<td>Pedometer (29)</td>
<td>MyFitnessPal (22)</td>
<td>100</td>
<td>WeatherBug (16)</td>
<td>iHeartRadio (1)</td>
</tr>
</tbody>
</table>

Wait, wait ... That's a lot to consider!

How can a user re-evaluate decisions taken earlier with ease?
Confused?

I don’t know!
Confused?

I don’t know!
So, maybe?

Accept     Maybe     Decline

Paper V: Partial Commitment—“Try Before You Buy” and “Buyer’s Remorse” for Personal Data in Big Data Machine Learning; L Fritsch; IFIP International Conference on Trust Management, page 3-11.
Partial commitment

Consent with an expiry date.
Consent for a subset of data.
Consent for limited access.
At expiration?

Decision to continue or revoke access.
Intervenability.
Wrapping up ...

Problems:

▶ Leaving the *data-tap* open.
▶ Poor means for monitoring.
▶ Consent for eternity.

Looking ahead:

▶ Methods to determine privacy-impact assessment cues.
▶ Burdensome responsibility to assess the cues.
▶ Starting a discussion about *partial commitment*. 
Questions & discussion

Contacts:
1. Nurul Momen, PhD Candidate, PriSec, Computer Science Dept. Karlstad University.
   email: nurul.momen@kau.se
2. Lothar Fritsch, Associate Professor, PriSec, Computer Science Dept. Karlstad University.
   email: lothar.fritsch@kau.se

References:
Paper V: Partial Commitment—“Try Before You Buy” and “Buyer’s Remorse” for Personal Data in Big Data Machine Learning; L Fritsch; IFIP International Conference on Trust Management, page 3-11.