Google/Apple Exposure Notification framework

October 2020
Exposure Notification is a multi-step process

1. Measure
   
   Keep track of all the persons (phones) in your proximity

2. Announce
   
   Later, if you are infected with Covid-19 virus, announce your infection status

3. Warn
   
   So that others can be warned and act themselves
Schematically

Every phone transmits a “unique code”…

… that is received by all phones nearby
“Random Codes”

- TEK=3cbfe7a73a673ac122
  - Random
    - RPI=a720b69e89
    - Derived, only look random
    - RPI=aec458d230
    - RPI=5347c88650
    - RPI=226816e3a2
    - ...
    - RPI=e512caa813
“Random Codes”

- TEK=3cbfe7a73a673ac122
  - RPI=a720b69e89
  - RPI=aec458d230
  - RPI=5347c88650
  - RPI=226816e3a2
  - RPI=...
“Random Codes”

TEK=3cbfe7a73a673ac122

- RPI=a720b69e89
- RPI=aec458d230
- RPI=5347c88650
- RPI=226816e3a2
- ... 
- RPI=e512caa813

TEK=3cbfe7a73a673ac122

- RPI=a720b69e89
- RPI=aec458d230
- RPI=5347c88650
- RPI=226816e3a2
- ... 
- RPI=e512caa813

Reconstructed
Personal data involved

<table>
<thead>
<tr>
<th>Data</th>
<th>Pseudonymous Identifier?</th>
<th>Health Data?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary Exposure Keys</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Rolling Proximity Identifiers</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Diagnosis Keys</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exposure Risk</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

As outlined by the EDPB in the interoperability statement.
Privacy by Design

- The proximity identifiers rotate every 10-20 minutes
- Calculating the *Exposure Risk Score* is done on the phone, not in the cloud
- The app cannot be used as a “Covid Passport” to prove one’s infection status (NL-specific)
Not so Private by Design

• TEK’s don’t change often enough

• Exposure Notification is a framework that tracks who meets who in real life, on an unprecedented scale, embedded in closed-source operating systems/middleware
[Do you spend time with your spouse? Are you risk aversive?]

• The calculation of the Exposure Risk Score happens inside the framework, not in the app. Thus the framework learns all health data involved (telemetry?!)
[The threat model of Google/Apple is “don’t trust the app”]
Forward

As soon as possible: go into detail
• Better explain: DPbD ≠ anonimity
• Telemetry? Legal safeguards necessary? On European level?
• Can GA change the API boundary between framework and app? Will they?
• Is Exposure Notification “just another API”? How about phase II?

For the bold:
• Address governance

Next time:
• invite Health Authorities and Data Protection Authorities to design phase