IOT PRIVACY CONCERNS WITH VOICE FIRST DEVICES

ANEESH KULKARNI

CS – 578
“A VOICE-FIRST DEVICE IS AN ALWAYS-ON, INTELLIGENT PIECE OF HARDWARE WHERE THE PRIMARY INTERFACE IS VOICE, BOTH INPUT AND OUTPUT.”

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.7mil</td>
<td>6.5mil</td>
<td>24.5mil</td>
</tr>
</tbody>
</table>
• People are no longer *users* of an IoT service but rather *subjects* of the service.
  ▪ Public WiFi connectivity
  ▪ The Echo & Mini at every household
• One major privacy concern with such devices is that users aren’t always aware when a device is collecting personal data.
• IoT privacy notifications on Mobile Example.
Voice First Device might some day be extended to support privacy notifications. Where every new device in hearing range be given notification about its presence.

All This must be done silently and explicitly.

The Last Mile for IoT Privacy


Fair Information-Practice Principles (ACPSR)
TOWARDS PRIVACY NOTICES

• Companies are obliged to have privacy policies in place to notify the users about their privacy practices.

• The privacy policy challenges get worse when dealing with such devices have access to very sensitive data about users.

• The numbers of which are said to be 25 billion and by 2020 they reach up to 50 billion.

• These collect sensitive and insensitive personal data such as location, physical conditions, habits and the way these data are used or shared are huge privacy concerns for IoT.
OECD FAIR INFORMATION PRINCIPLES

• One of the main privacy risks is unsolicited marketing.

• *Can user be informed about their personal information which are collected, used or shared with IoT devices?*

• *Can we use Limitation Principle?*

• How to notify users about changes in privacy policies?

• *Notice Timing is a Challenge.*

• *How frequently should this notice be given?*
OTHER IMPORTANT CONCERNS:

• *Decoupled Notices: Like in Alexa and Google home which have no screens where privacy policy can be shown.*

• *Identifying audience: like the Owner, Family Member and Guest.*

• *Relevant and Irrelevant notices*

• *Establishing a medium for notice.*

• “*take-it-or-leave-it choice*”
SOLUTION

• Collect verbs in the privacy document like store, save, listen, record, process, send, sell, share, control and permit.
• Other key words like Vendor, third party and service provider.
• All these words must be highlighted.
WITH YOUR CONSENT ON SUCH PRIVACY DOCUMENTS:

- We may collect and store information (including personal information) locally on your device using mechanisms such as application data caches.
- We will share personal information with companies, organizations or individuals outside of Google.
- Amazon will periodically import and store your contacts to improve your Alexa Calling and Messaging experience.
- Certain Alexa Calling and Messaging services are provided by our third party service providers, and we may provide them with information, such as telephone numbers, to provide those services.
- If you do not accept the third party terms applicable to a Third Party Service, do not use that Third Party Service.
CONCLUSION:

• Best practice is to integrate privacy Notice in every IoT device.
• Considering the standardization for a protocol stack for communication between users and devices.
• Enforcing key word highlight in privacy documents.
• Giving the choice of not sharing information for development of services.
• Limit use of third party service vendors.
• Considering each communication as a transaction which can be encrypted.
• Limit information storage time period.
REFERENCES:

• “Is there a Room for security and Privacy in IoT?”, Elias Tabane, ©2016 IEEE

• www.EandTmagazine.com April 2017 Engineering & Technology

• Miguel C. An analysis of M2M platforms: challenges and opportunities for the Internet of Things. 2012.


• Amazon. Alexa terms of use, 2017. [Online; accessed Dec 2017].

• Google terms of use, 2017. [Online; accessed Dec 2017].