Seminar on Internet-of-Things, privacy and integrity

Case - IOT and health

Per Gunningberg
IoT and sensors

• Vision - everything that can connect to the Internet will do so.

• Scope - 100 Billions devices on the Internet. Soon.

• For you - up to 100 devices around You or carried by You or worn by You or inside You.
INTERNET of THINGS
• https://www.youtube.com/watch?v=kq8wcjQYW90
WIRELESS IMPLANTABLE MEDICAL DEVICES

- Deep Brain Neurostimulators
- Cochlear Implants
- Gastric Stimulators
- Cardiac Defibrillators/Pacemakers
- Foot Drop Implants
- Insulin Pumps
INTERNET OF THINGS
Privacy (/prɪvəsi/ or /praɪvəsi/; from Latin: privatus) is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.
Privacy in Mobile Technology for Personal Healthcare

SASI KANTH AVANCHA and AMIT BAXI, Intel Labs Bangalore
DAVID KOTZ, Dartmouth College

Information technology can improve the quality, efficiency, and cost of healthcare. In this survey, the privacy requirements of mobile computing technologies that have the potential to transform healthcare. Such mHealth technology enables physicians to remotely monitor patients’ health and enable patients to manage their own health more easily. Despite these advantages, privacy is essential for any monitoring technology. Through an extensive survey of the literature, we develop a conceptual privacy framework for mHealth, itemize the privacy properties needed in mHealth systems, and discuss the role of accountability for supporting privacy-sensitive mHealth systems. We end with a list of open research questions.

Categories and Subject Descriptors: A.1 [Introductory and Survey]; J.3 [Life and Medical Sciences]; K.4.1 [Computers and Society]: Public Policy Issues

General Terms: Security, Legal Aspects, Human Factors

Additional Key Words and Phrases: Privacy framework, medicine, electronic health record, medical information systems, health; K.4.1 [Computers and Society]: Public Policy Issues

ACM Reference Format:
mHealth

*mHealth* technology appears promising in many ways: enabling physicians to remotely monitor their patients’ health and improve the quality of healthcare, enabling patients to manage their health more easily, and reducing the cost of care by allowing patients to spend less time in the hospital or make fewer visits to their doctor.

Mobile Internet Devices (MIDs), connected wirelessly to wearable, portable, and even embeddable sensors, will enable long-term continuous medical monitoring for many purposes.
• “Health information privacy” is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.

• Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

• Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.”
mHealth privacy

• mHealth allows for the collection of far more medical data about the Patient. (For example, it is possible to record ECG data continuously for weeks, throughout daily life)

• mHealth allows much broader range. Many mHealth applications will collect information about Patient lifestyle and activities (such as food habits and diet details, location tracks, physical activity, or social interactions).

• mHealth will enable sharing data with your health provider, as in a traditional doctor relationship, but also sharing data with an insurance company, with lifestyle coaches, with athletic coaches, or with family (e.g., to support a relative’s recovery from surgery).
a supportive ecosystem

- **Policymakers** establish laws, regulations, and standards regarding the protection of Patient privacy in mHealth technology;

- **Certification bodies** attest to whether particular products and services meet the policies and standards.

- **Manufacturers** produce hardware and software products and services.

- **Distribution & Management services** distribute the hardware and software to Patients and Consumers, and provide remote-management capabilities such as secure, automatic software updates and remote deletion of data and keys on lost devices.

- **Key-Management Infrastructure** provides the key-distribution and certificate authorities to support the crypto-systems used for verification.
Activity Tracking

The simplest way to get credit for your steps, exercise and overall calories burned throughout the day. Knowing is the first step to get more active and stay motivated.

Smart Coach

Smart Coach gives you the motivation and personalized insights you need to reach your goals, no matter where your day takes you. Plus, it gets smarter over time—as Smart Coach gets to know you, insights and tips get better and better. And you will too.

Sleep Tracking

Easily track hours slept and quality of sleep. Smart Coach learns your habits and gives you personalized suggestions to help you get to bed on time. Smart Alarm™ silently wakes you up at the optimal moment in your sleep cycle—so you feel refreshed.

Food Logging

Log your meals and track calories in no time with the UP® barcode scanner, restaurant menu search and food database. Smart Coach helps guide you to healthy habits and gives your meal a Food Score—because there’s more to eating well than just counting calories.
Go to bed by 10:20pm tonight...

Try this today

Anne moved 10,832 steps today

Try this today

Try this today
Authorize this connection?

Allow Uplt Widget to:

- Read your basic info
- Read you cardiac data
- Read your extended info
- Read your generic events
- Read your meals
- Read your mood
- Read your moves
- Read your sleep
- Read your weight

Allow my UP teammates to see Uplt Widget posts.

CANCEL  AGREE
Averages based on UP users. The National Sleep Foundation recommends between 7-9 hours of sleep per night, and experts recommend 10,000 steps a day for an active, healthy lifestyle.

**Move**
- 15,000 steps

**Sleep**
- 7h 30m

**Weight**
- Set goal

---

**myfitnesspal**
Calorie Counter

**The Breakfast Challenge**
Log a breakfast every morning and Quaker will donate a meal to Feeding America.

**IFTTT**
IFTTT puts the internet to work for you.

---

**Last Workout** • 06/20/14 05:26 AM

Quickstart • Workout

Home • Results • Health • Settings
Privacy IT technology

- Authentication
- Patient, Provider, and Devices
- Anonymity (data may be used for research)
- Location privacy
- Consent management (e.g. to medical records)
- Access control
- Auditing (held accountable when handling patient data)
- Data integrity (data is not changed)
- Confidentiality and secure transmission
- Device presence
- Device compromise, Theft, and Loss
Discussion Topic

• Discuss the design of the JawBone UP24 technology (or any other activity band) with respect to the privacy issues:

  • Access control
  
  • Anonymity (social, location)
  
  • Confidentiality
  
  • Consent management. How and what? Fine and complicated or course - like all or nothing?
Discussion topics

• How owns the data from a medical device, like an Activity Band?

• Are there cultural, generation and gender with respect differences to what is considered Privacy?

• What (ethical) responsibility do you have as a researcher and developer when designing new devices with respect to privacy?
FitBit focus group study

Acceptance of sharing Activity Band data with Friends, Family and Public

<table>
<thead>
<tr>
<th>TABLE 30.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants</td>
</tr>
<tr>
<td>Male</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Students</td>
</tr>
<tr>
<td>Working</td>
</tr>
<tr>
<td>Retired</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>
## TABLE 30.3

Final Normalized Sharing Scores for Family versus Friends, Family versus Public, and Public versus TP

<table>
<thead>
<tr>
<th></th>
<th>Family</th>
<th>Friends</th>
<th>Family</th>
<th>Public</th>
<th>Public</th>
<th>TP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steps</td>
<td>0.96</td>
<td>0.94</td>
<td>0.96</td>
<td>0.91(^a)</td>
<td>0.89</td>
<td>0.89</td>
</tr>
<tr>
<td></td>
<td>(0.19)</td>
<td>(0.14)</td>
<td>(0.19)</td>
<td>(0.22)</td>
<td>(0.27)</td>
<td>(0.25)</td>
</tr>
<tr>
<td>Calories</td>
<td>0.96</td>
<td>0.94</td>
<td>0.96</td>
<td>0.89(^a)</td>
<td>0.89</td>
<td>0.89</td>
</tr>
<tr>
<td></td>
<td>(0.19)</td>
<td>(0.17)</td>
<td>(0.19)</td>
<td>(0.25)</td>
<td>(0.27)</td>
<td>(0.25)</td>
</tr>
<tr>
<td>Sleep</td>
<td>0.96</td>
<td>0.95</td>
<td>0.96</td>
<td>0.87(^a)</td>
<td>0.87</td>
<td>0.87</td>
</tr>
<tr>
<td></td>
<td>(0.19)</td>
<td>(0.14)</td>
<td>(0.19)</td>
<td>(0.30)</td>
<td>(0.30)</td>
<td>(0.29)</td>
</tr>
<tr>
<td>Traits</td>
<td>0.91</td>
<td>0.83</td>
<td>0.91</td>
<td>0.78(^a)</td>
<td>0.80</td>
<td>0.83</td>
</tr>
<tr>
<td></td>
<td>(0.23)</td>
<td>(0.26)</td>
<td>(0.23)</td>
<td>(0.29)</td>
<td>(0.29)</td>
<td>(0.32)</td>
</tr>
<tr>
<td>Goals</td>
<td>0.85</td>
<td>0.73</td>
<td>0.86</td>
<td>0.61(^a)</td>
<td>0.68</td>
<td>0.82(^a)</td>
</tr>
<tr>
<td></td>
<td>(0.36)</td>
<td>(0.42)</td>
<td>(0.36)</td>
<td>(0.50)</td>
<td>(0.48)</td>
<td>(0.38)</td>
</tr>
<tr>
<td>Major</td>
<td>0.94</td>
<td>0.91</td>
<td>0.95</td>
<td>1.00</td>
<td>0.98</td>
<td>0.82(^a)</td>
</tr>
<tr>
<td></td>
<td>(0.21)</td>
<td>(0.25)</td>
<td>(0.21)</td>
<td>(0.00)</td>
<td>(0.16)</td>
<td>(0.38)</td>
</tr>
<tr>
<td>Weight</td>
<td>0.83</td>
<td>0.64(^a)</td>
<td>0.84</td>
<td>0.54(^b)</td>
<td>0.59</td>
<td>0.74(^a)</td>
</tr>
<tr>
<td></td>
<td>(0.37)</td>
<td>(0.46)</td>
<td>(0.36)</td>
<td>(0.51)</td>
<td>(0.50)</td>
<td>(0.43)</td>
</tr>
</tbody>
</table>

\(^a\) Significant at 0.05 level; \(^b\) Significant at 0.01 level.
Some study results

• Weight and health goals most sensitive issue to share.
  • Sometimes more willing to share with public than family.

• Some differences in sharing over gender, demographics and occupational status.
  • Some does not want to share with children or parents.
  • Some concern about sharing with “third parties”, companies.

• Uncertainty to understand what the Activity band captures. “Being watched the whole time”.

• “Could be used against you. I have no control.”
Recommendations from study

• Flexible controls to sharing and privacy
  • Both fine and course grained
  • One-size-fits-all is not enough
  • Flexible design that allow users to visualize how they are sharing with others.
References
