Privacy and Multi-modal Sensing

John Heidemann
USC/Information Sciences Institute
8 August 2006
Sensornet Privacy Needs Grow

• military surveillance
  – the bad guys
• habitat monitoring
  – plants and animals
• elder-care and urban sensing
  – you and your family
=> apps increasingly require privacy
Threat Models and Tools

• possible threat models
  – external
    • sophisticated malicious attacker
    • naïve malicious attacker
    • casual browser
  – internal
    • sophisticated
    • opportunist
    • browser

• what tools do we have?
  – technical
  – process and policy
  – legal
Threat Models and Tools

• possible threat models
  – external
    • sophisticated malicious attacker
    • naïve malicious attacker
    • casual browser
  – internal
    • sophisticated
    • opportunist
    • browser

• what tools do we have?
  – technical
  – process and policy
  – legal
One Technical Approach


• can we balance privacy and security?
  – limit use of cameras
  – but correlate events with images when necessary

• use multi-modal sensing and intelligence
Principles

• match sensor invasiveness to environment
  – cameras only in *public areas* (lobbies)
    • often already have cameras or guards
  – PIR sensors in private areas (halls, offices)
• what happens at the sensor stays at the sensor
  – queries are explicit
  – only when required
System Architecture

- example office deployment
  - camera in lobby
  - PIR sensors in halls
    - at each office door
- each sensor records events (image or detection) to local flash memory
- queries happen only on demand
  - easy to audit
  - can be visible to office occupants
    - queries could trigger light at sensor

Motion sensors
Camera
theft detected in office A. who?

security officer initiates spatio-temporal query to establish chain of events from A to camera

Query

Negative response

Positive response

relate theft at location A and given time with detections in hall and to image taken in lobby
Observations

- not perfect!
- definite limitations
  - abuse possible (e.g., repeated queries)
  - requires dense PIR sensors
  - spatio-temporal search can be confused by crossed targets
- but combination of techniques help
  - no cameras in offices
    - pervasive watching impossible, even if office nodes compromised or reprogrammed
  - no central database
    - reduces ability to browse or mine data
Do People Really Care?

- survey 60 people to verify assumption
  - rate privacy from 0 to 5, not to very concerned
  - 30 men and 30 women
  - mix of 20 questions about privacy issues (for perspective)

<table>
<thead>
<tr>
<th></th>
<th>motion sensors</th>
<th>cameras</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>2.1 (1.7-2.5)</td>
<td>3.1 (2.6-3.5)</td>
</tr>
<tr>
<td>men</td>
<td>2.5 (1.9-3.1)</td>
<td>2.8 (2.1-2.5)</td>
</tr>
<tr>
<td>women</td>
<td>1.7 (1.1-2.3)</td>
<td>3.3 (2.7-3.8)</td>
</tr>
</tbody>
</table>

*yes, but there is a significant difference by gender*
Generalizations

• simple, physically obvious evidence of privacy is important (not just software)
  – door on the camera
  – physical switch on WiFi
  – sleeve over RFID badge

• distinguish public from private areas

• decentralized data

• augment technical solutions with policy and legal