BIM and the Internet of Things

Carl G. Roberts
Learning objectives:
- Scope of IoT
- Legal responsibilities for information custodians
- Ownership
- Cybersecurity
- Privacy
<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2010</th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Devices</td>
<td>500 million</td>
<td>12.5 billion</td>
<td>25 billion</td>
<td>50 billion*</td>
</tr>
<tr>
<td>World Population</td>
<td>6.3 billion</td>
<td>6.8 billion</td>
<td>7.2 billion</td>
<td>7.6 billion</td>
</tr>
<tr>
<td>Devices Per Person</td>
<td>.8</td>
<td>1.84</td>
<td>3.47</td>
<td>6.58</td>
</tr>
</tbody>
</table>

* Intel estimate – 200 billion

Source: Cisco April 2011
Smart Buildings and Smart Cities
  – Energy
  – Water Distribution
  – Transportation
  – Public Safety
  – Digital Services

10^6 | MB
10^9 | GB
10^{12} | TB
10^{15} | PB
10^{18} | EB
10^{21} | ZB
10^{24} | YB
10^{27} | BB
Evidence
Ownership

May be multiple rights
  – Perspective
License
  – Scope
Notice and Consent
  – Scope/Repurposing
Breaches

783 reported breaches in 2014

27.5% increase from 2013

18.3% increase from 2010

Data provided by Identity Theft Resource Center
Authorities and Agencies

White House
FTC    DOE    FCC

FAA
NHTSA
States
EU
Cybersecurity

Devices - low margin, low cost, low quality, generally insecure

Many points of access
  – To data
  – To systems

Multiple organizations – collaboration

Protection schema have not kept up with attack technologies
Data Privacy

Present focus - predominantly consumer rights

Today’s consumer issue is tomorrow’s business issue

– HIPAA

What    How    Why    For How Long
Best Practices

Access control and user authentication
  Audit trails
  Prompt attention to vulnerabilities
  Data minimization
  Obfuscate PII
Encrypt – both in transit and at rest
  Backups
  Test

Encourage culture of security
Implement security by design
Implement defense-in-depth

Provide Notice – Choice – Consent
Cyber-insurance
Carl G. Roberts, Ballard Spahr LLP

cgroberts@ballardspahr.com