INTERNET OF BODIES: OUR CONNECTED FUTURE

PRESENTED BY MARY LEE
ART BY GIORGIA LUPI FOR THE RAND CORPORATION

© COPYRIGHT 2022 RAND CORPORATION
What is the Internet of Bodies?

The Internet of Bodies is an ecosystem of internet-connected devices that monitor the human body and collect personal biometric data. Despite its potential to offer revolutionized medical treatments, improved physical performance, convenience, and even fun, the Internet of Bodies is still an inconsistently regulated space that poses cybersecurity and other risks.
Wearable Health Trackers

Bracelets, watches, rings, and smartphone apps that track steps, heart rate, sleep patterns, and other physical data, such as how much alcohol the wearer consumed.

These devices operate by using advanced accelerometers and other sensors that can translate movement into digital measurements.

Many devices also offer data analytics and displays to provide detailed information in accessible forms.
Attention Monitors

Glasses that use brain activity and eye movements to track attention. They are designed to be used in schools or while driving and provide audio or haptic feedback when they sense the user is inattentive.
Implantable Cardiac Devices

Newer cardiac pacemakers, implantable cardioverter defibrillators, and ventricular assist devices can provide real-time and continuous information regarding a patient’s cardiac fluctuations and enable remote device management to automate technical checks, such as battery status, lead impedance, and sensing or pacing thresholds.
In 2017, the FDA approved the first digital pill: aripiprazole tablets with an ingestible sensor embedded in the pill that records that the medication was taken. The system works by sending a message from the pill’s sensor to a wearable patch that transmits the information to a mobile app so that patients can track the ingestion of the medication on their smartphones.

Patients can also permit their caregivers and physician to access the information through a web-based portal. Other ingestible digital pills are now available, including oral oncology drugs with a digital sensor to track adherence, dosing, and patient activity levels to develop better dosing regimens for chemotherapies.
Brain-Computer Interfaces

BCIs use electrodes that connect signals from the brain to a computer. They may be either implanted in the brain or noninvasive (wearable or attached to the skull).

BCIs under development aim to read and type entire words directly from the brain, or control prosthetic limbs from the mind.
The Good: Perceived benefits of the Internet of Bodies

Medical
- Improved disease prevention, treatment, monitoring, prognosis
- Pandemic prevention and detection
- Possible reduction in healthcare costs
- Elective data-sharing may improve research

Performance
- Improved perception
- Improved function
- Improved cognition
- Improved fitness

Convenience
- Improved efficiency
- Monitoring environment for comfort and safety
### The Bad: Understanding some of the risks

#### Global and national security risks
- Security risks
- Data use risks
- Ethical risks
- Policy implementation risks

<table>
<thead>
<tr>
<th>Who might gain access?</th>
<th>What are potential vulnerabilities?</th>
<th>What are possible consequences?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Criminals</td>
<td>• Bodily dependence on device for health or functional purposes</td>
<td>• Death or physical harm from malfunction or hacking</td>
</tr>
<tr>
<td>• Hackers</td>
<td>• Sensitive data collection, possession, or dissemination</td>
<td>• Global and national security challenges</td>
</tr>
<tr>
<td>• Data brokers</td>
<td>• Internet connectivity</td>
<td>• Data breach</td>
</tr>
<tr>
<td>• Data fusion centers</td>
<td>• Regulatory gaps</td>
<td>• Passive collection or sharing of data without informed consent</td>
</tr>
<tr>
<td>• Employers</td>
<td>• Hardware</td>
<td>• Misuse or unexpected uses of data</td>
</tr>
<tr>
<td>• Schools</td>
<td>• Software</td>
<td>• Personal identification</td>
</tr>
<tr>
<td>• Healthcare providers</td>
<td></td>
<td>• Increased health disparities</td>
</tr>
<tr>
<td>• Insurance companies</td>
<td></td>
<td>• Coercion to accept devices</td>
</tr>
<tr>
<td>• Manufacturers</td>
<td></td>
<td>• Infringement on body autonomy</td>
</tr>
<tr>
<td>• Criminal justice system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Governments</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Considering the ethical risks

Inequitable outcomes
• Increased health disparities due to barriers to access (health insurance, internet access)
• Input bias (representativeness of health data across gender, race)

Freedom from IoB
• Privacy for those who may be seen/heard by IoB devices without consent
• Other examples: tracking employee productivity or incarcerated persons

Body autonomy and integrity
• Jailbreaking devices that are integrated in one’s body
• Who has control to modify the device once integrated?

Enforcement of authoritarian regimes?
• China using DNA data to surveil Uighurs
Considering the national security risks

- Purchase of Grindr by Chinese company gave engineers in Beijing access to U.S. user data, including private messages and HIV status
- Threat of Dick Cheney’s remote assassination via his WiFi-enabled defibrillator
- Strava fitness data exposed secret military bases
- Increasing ransomware attacks on hospitals
The Ugly: The patchwork of state and federal policies governing IoB potentially enables regulatory gaps

<table>
<thead>
<tr>
<th>Federal</th>
<th>State</th>
<th>International</th>
<th>Self-Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FDA – regulates medical devices</td>
<td>• California Consumer Privacy Act</td>
<td>• European Union General Data Protection Regulation (GDPR)</td>
<td>• Corporate security and privacy policies</td>
</tr>
<tr>
<td>• FTC – enforces data security and consumer privacy</td>
<td>• California AB-2089 (digital mental health privacy)</td>
<td></td>
<td>• Information-sharing organizations (MedISAO, H-ISAC)</td>
</tr>
<tr>
<td>• HHS – enforces HIPAA</td>
<td>• California IoT law (SB 327)</td>
<td></td>
<td>• Voluntary security standards</td>
</tr>
<tr>
<td>• CPSC – works to reduce the risk of injuries and deaths from consumer products</td>
<td>• Vermont and California data broker laws</td>
<td></td>
<td>• Principles and codes of conduct (e.g., Hippocratic Oath for Medical Devices)</td>
</tr>
<tr>
<td>• IoT Cybersecurity Improvement Act of 2020</td>
<td>• All 50 states – data breach notification laws (scope of each law differs)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Abbreviations: CPSC – Consumer Product Safety Commission; FDA – Food and Drug Administration; FTC – Federal Trade Commission; H-ISAC – Health Information Sharing and Analysis Center; HHS – Health and Human Services; IoT – Internet of Things; MedISAO – Medical Information Sharing and Analysis Organization
Are we ready for the implications of the Internet of Bodies?

**Ohio v. Compton**

In 2016, an Ohio man’s house burned down

Suspecting arson, police issued a warrant for the man’s pacemaker records

Doctors concluded pacemaker data contradicted the man’s version of events, and the man was charged with arson and insurance fraud

Lawyers claimed invasion of privacy and physician-patient privilege, but judge ruled data admissible
Conclusions

• The Internet of Bodies is a relatively nascent, but complex and rapidly evolving ecosystem which may be outpacing policy

• There is a lack of consistency in IoB laws among states and between the state and federal level which enables regulatory gaps

• IoB presents unique challenges that requires balancing between innovation and regulation, while protecting consumers
Questions?