Agenda

- Background on the Internet of Things
- Smart speakers and privacy
- What’s in store for the future?
- Privacy and security steps to consider
Background

- Background on the Internet of Things
- Smart speakers and privacy
- What’s in store for the future?
- Privacy and security steps to consider
What is the IoT?

- Networked devices that can collect information
- Fitbits, Fuelbands, etc. that can track the steps you take in a day, calories burned, and minutes asleep
- Baby monitors, thermometers, scales, that are connected to a network
- Nest Thermostat; connected ovens, refrigerators, and other appliances; and home electricity and water-usage tracker
- “Smart speakers” such as Amazon Alexa and Google Home
- Additional devices, sensors, data points considered in the future
Numerous devices bring benefits and questions

- 200 billion connected sensor devices will be in use by 2020, with a market size of roughly $2.7 trillion to $6.2 trillion per year by 2025.

- A 2017 Gallup poll found that 20 percent of Americans used smart home devices like thermostats and lighting.

- **Benefits**: Can be very useful, they are fun, they are convenient.

- **Questions**: Who owns the data these sensors generate? How can such data be used? Are such devices, and the data they produce, secure?
Smart speakers and privacy

Background on the Internet of Things

Smart speakers and privacy

What’s in store for the future?

Privacy and security steps to consider
What are smart speakers?

“A smart speaker is a type of wireless speaker and voice command device with an integrated virtual assistant that offers interactive actions and hands-free activation with the help of one ‘hot word’ (or several ‘hot words’).”* 

How do they work...

Device monitors for the ‘wake word’ or ‘hot word.’

Once activated, information is sent to company servers for processing.

Third parties can also obtain access, for example, where “skills” or additional functionality is involved.
Where are they and what can they “hear”? 

**Home**: the canonical private space

**Conversations**: from silly to intimate and everything in between

**Society**: from workplace and shopping to business uses and transportation
Where else might they be used and what can they “hear”?  

Other sensitive locations, such as hospitals

Could be deployed potentially anywhere

Could be used to listen to anything
How do people feel about them?

- **Value**
  - 53 percent of respondents feel that IoT makes their lives more convenient.
  - 47 percent say IoT makes them more efficient, and 34 percent say IoT increases their safety.

- **Trust**
  - Only **9 percent** of respondents say that they trust that their data collected and shared through IoT is secure.
  - Only **14 percent** feel that companies do a good job of informing them what data is being collected and how it is used.
What are the privacy implications?

“Privacy”: An essentially contested concept, like art, freedom, or democracy

Legalistic approach: 4\textsuperscript{th} Amendment – “reasonable expectation of privacy”

Sociological approach:
• “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” – Alan Westin
• Privacy states: solitude, intimacy, anonymity, reserve.

These states are all aspects of being inside a home, and thus smart speakers have the potential to impact all of these states.
How IoT Devices Sometimes do not Work

CNN

Google admits its new smart speaker was eavesdropping on users
by Samuel Burke @CNNTech
October 12, 2017, 7:28 AM ET

Washington Post

How Nest, designed to keep intruders out of people’s homes, effectively allowed hackers to get in

NPR

Amazon Echo Recorded And Sent Couple’s Conversation — All Without Their Knowledge
May 25, 2018, 3:16 PM ET

Mercury News

“5 minutes of sheer terror”: Hackers infiltrate East Bay family’s Nest surveillance camera, send warning of incoming North Korea missile attack
Fake ICBM missile warning over Nest system sends East Bay family into panic
## Legal frameworks

| Constitutional                                                                 | • Applies to government  
|• 3d party doctrine |
|---|---|
| 4th Amendment: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ... .” | |

<table>
<thead>
<tr>
<th>Statutes related to electronic communications</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal: ECPA: Wiretap Act, Stored Communications Act</td>
<td>All deal with transmitting and storing voice recording</td>
</tr>
<tr>
<td>State: California Wiretapping Law (Cal. Penal Code s. 632)</td>
<td>California makes it a crime to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation.</td>
</tr>
</tbody>
</table>
## Legal frameworks

<table>
<thead>
<tr>
<th>Consumer Protection</th>
<th>Requires companies to abide by their terms of service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal and state consumer protection statutes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Children</th>
<th>Requires verifiable parental consent before collecting a child’s personal information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Children’s Online Privacy Protection Act (COPPA)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposed</th>
<th>Would change preference for storage and exchange of recordings from <strong>opt-out</strong> to <strong>opt-in</strong>. Consumers would have to affirmatively consent to storing their recordings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB-1395: Smart Speaker Privacy Act</td>
<td>- Scheduled for a hearing on April 30 in the CA Assembly Privacy and Consumer Protection Committee</td>
</tr>
</tbody>
</table>
What’s in store for the future?

Background on the Internet of Things

Smart speakers and privacy

What’s in store for the future?

Privacy and security steps to consider
• **Patent applications**
  • Amazon envisions the next wave of Alexa-enabled devices using information collected to build profiles on anyone in the room to sell them goods.

  • Amazon describes how a “voice sniffer algorithm” could be used on an array of devices, like tablets and e-book readers, to analyze audio almost in real-time when it hears words like “love,” “bought” or “dislike.”

• **Targeted ads based on IoT information**
  • E.g. smart thermometers
• **Mischief**
  • One application details how audio monitoring could help detect that a child is engaging in “mischief” at home by first using speech patterns and pitch to identify a child’s presence, one filing said. A device could then try to sense movement while listening for whispers or silence, and even program a smart speaker to “provide a verbal warning.”*

• **Mood**
  • Voices could be used to determine a speaker’s mood using the “volume of the user’s voice, detected breathing rate, crying and so forth,” and medical condition “based on detected coughing, sneezing and so forth.”*

*New York Times*
### Additional issues to consider

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Oversharing</strong></td>
<td>Some fitness trackers/wristbands share large amounts of data by default.</td>
</tr>
<tr>
<td><strong>Subject to hacking/hacked passwords</strong></td>
<td>Home security cameras accessed using hacked passwords allowed intruders to warn homeowners of a fake missile attack or threaten to kidnap a child.</td>
</tr>
<tr>
<td><strong>Potential for abuse</strong></td>
<td>Improper or unexpected internal access to personal information.</td>
</tr>
<tr>
<td><strong>Secondary uses of information</strong></td>
<td>Fitness tracker data shared with/sold to insurers?</td>
</tr>
</tbody>
</table>
Privacy and security steps to consider

- Background on the Internet of Things
- Smart speakers and privacy
- What’s in store for the future?
- Privacy and security steps to consider
If you own a smart speaker or other IoT device – privacy and security steps to consider (1 of 2)

• Use different passwords for different accounts.

• Enable two-factor authentication.

• Make sure devices are running the latest software updates.

• Make sure your WiFi network is secure and be sure to protect it with a strong password (e.g., passphrase or eight character alpha-numeric with at least one special character).
If you own a smart speaker or other IoT device – privacy and security steps to consider (2 of 2)

• Review recordings and consider deleting them.

• Require a PIN for purchases (if an option).

• Consider using it for things that are unlikely to be risky. “Play me some jazz” is less problematic than “let my sister know we’re away for a week and don’t need the car back.”

• Review privacy settings and set them in ways that align with your expectations.
Questions & Answers (open)

Privacy Office Contact

Email: PrivacyOffice@ceo.sccgov.org
Internal website: https://sccconnect.sharepoint.com/sites/cpo
External website for constituents: https://www.sccgov.org/sites/cpo