Internet of Things: Pepper's Privacy Risks

By: Muhammad Jamal and Benita Lalani
Faculty Mentor: Alison Leland
Smithsonian Mentor: Danee Adams

UNIVERSITY of HOUSTON

Smithsonian

Background Information

- Pepper robots is the world's first social humanoid robot that can recognize human faces and emotions.
- Pepper was created to interact with humans and was introduced to the public in 2014
- Softbank Robotics, creators of the robot, gifted 24 Pepper robots to the Smithsonian Institution:
- Details:
  - 4-feet tall
  - 62 pounds
  - Exchanges are pre-scripted
- Pepper also has audio sensors, video sensors, and special abilities
  - Dancing
  - Posing for selfies
  - Explanation to individual how he views them

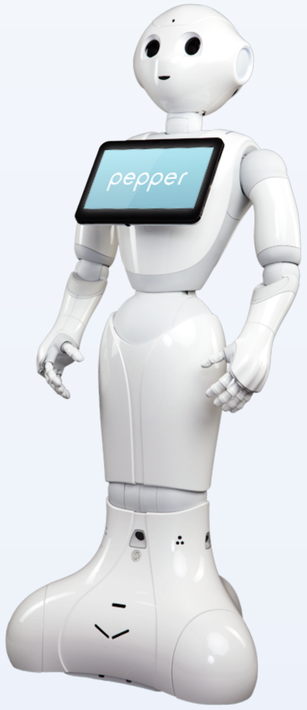
SoftBank

Privacy Implications For Pepper Robots

- As an emotionally intelligent robot, Pepper has been designed to not only recognize emotions but also gather data over the course of conversations and relay the information back to its processing system.
- Researchers claim that Pepper was commercialized before it was ready
  - "… the manufacturer extensively neglected any sort of security assessments before commercializing their product."
  - Experiments show that login credentials can easily be compromised, allowing an individual to steal data and command the robot without authentication to spy and potentially even directly harm them.
- Unsecured administrative page with no "log off" function in administrative panel
- New upgrade allows Pepper to remember faces and details of previous orders

Effects

- Through the ability to record and store conversations, Pepper robots, if not configured correctly, could be sorting information without consent of the individual.
- Hacking Concerns
- Pepper to be used as a way to break into the Smithsonian network
- Human Error
- Softbank Low Communication



Solutions

- Minimize utilization of Pepper's capabilities
  - Limit conversational ability, audio/video recording, and ability to recognize human features
- Gain more knowledge of what Pepper can do before utilizing him and having it in Smithsonian Museums
  - More intensive research should be performed in order to learn full capabilities of Pepper
- Mandatory change of public password to a private password with time-sensitive changing standards
  - Public password allows for easy access for hacking; private password increases security and defers from being able to hack easily
- Retention plan
  - What is the purpose of retaining data?
  - Data should be purged daily if not being used for informational purposes
- Software update
  - More security updates to Pepper software are necessary so hacking isn't as easy
- Add "log off" function in the admin panel
  - Without a "log off" button, Pepper is prone to easily being hacked if a hacker can log on to an admin computer
- Until privacy risks are resolved, limit Pepper's interaction with children under a certain age
  - Age limit should be set to at least 13 years of age
  - Goes back to Pepper's ability to determine age (should not be able to perform this)
- Pepper needs to have a privacy notice
  - Due to the lack of information about Pepper, a privacy notice explaining the "who's" and "what's" of Pepper should be provided

Pepper with a Dash of Salt! - Summary

Below is a summary of an article written by Muhammad Jamal and Benita Lalani and presented to the Smithsonian Privacy Council

Why So Salty?

As the future of AI technology slowly becomes mass-produced consumer product (because let's be honest, who doesn't want their own personal butler… er, robot), we need to be careful about what issues this progress may cause. We or someone we know has seen movies where highly intelligent robots take over the world; although fiction, they bring up good questions. So, let's slow down a minute and talk about the future of Pepper in relation to the Smithsonian.

As an emotionally intelligent robot, Pepper has been designed to not only recognize emotions, but also gather data over the course of a conversation. During these conversations, Pepper gathers data on the individual's tastes, traits, preferences, and habits to personalize responses and better address needs. A remarkable feat, however, it's easy to see the security and privacy concerns…

Pepper with a Dash of Salt! – Summary Continued

…within this trick. In addition, the most recent update in this humanoid robot allows it to remember customers' faces and the details of their previous orders: an alarming addition as it only increases risk.

Solutions

One solution is to develop an information retention plan for Pepper in order to dispose of collected information as soon as the information is no longer needed. But first and foremost, why is Pepper collecting information such as recording encounters with humans and being able to determine age, sex, and emotions? If Pepper was not able to collect all of this information, then there would be no need for a retention plan. However, this robot was human-made, and as humans, we are all prone to error. Thus, the need for a retention plan is imminent, and the data collected should be purged daily, unless it is being used for informational/research purposes.

….For the full article, please see the handout on the desk.

References

Chirgwin, Richard. "Softbank's 'Pepper' Robot Is a Security Joke." • *The Register*, The Register, 1 June 2018, www.theregister.co.uk/2018/05/29/softbank_pepper_robot_multiple_basic_security_flaws/.

Giaretta, Alberto, et al. *Adding Salt to Pepper*. 4 July 2018.

Middleton, Chris. "SoftBank Pepper Robot 'Astonishingly Insecure', Potential 'Cyber Weapon.'" *Internet of Business*, 20 June 2018, internetofbusiness.com/softbank-pepper-robot-astonishingly-insecure-and-a-cyber-weapon/.

"Pepper the Humanoid and Programmable Robot: SoftBank Robotics." *SoftBank Robotics - Group*, www.softbankrobotics.com/emea/en/pepper.

Sanders, James. "SoftBank Invested 'Almost Nothing' in Pepper Robot Security, Creating Huge Business Risk." *TechRepublic*, TechRepublic, 26 Jan. 2019, www.techrepublic.com/article/softbank-invested-almost-nothing-in-pepper-robot-security-creating-huge-business-risk/.