THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

July 14, 2017

Alexa, Can You Help Me Solve This Murder?

Police want access to data from the Amazon Echo speaker found in the home of a Bentonville, Ark. man who is charged with first-degree murder. Since the Echo speaker is always listening for Alexa voice commands, the audio it recorded could provide clues about what happened at the crime scene.

While investigating, police noticed the Echo in the kitchen and pointed out that the music playing in the home could have been voice activated through the device. While the Echo records only after hearing the wake word, police are hoping that ambient noise or background chatter could have accidentally triggered the device, leading to some more clues. Amazon stores all the voice recordings on its servers, in the hopes of using the data to improve its voice assistant services. While you can delete your personal voice data, Amazon reserves the right to store that information on its servers, and promises to handle it in accordance with its main privacy policy.

A key issue in the Arkansas case is whether or not Amazon servers have information that the police can't otherwise access. The company did provide Bates account details and purchases, but court records show that Amazon twice declined to give the actual voice search queries to local police.

You have the right to remain silent, but does your smart device?

Police access to user data stored on consumer technology devices was fodder for national debate last year when Apple refused to help the FBI access an encrypted iPhone. The FBI eventually gained access on its own, effectively pushing the issue of whether or not tech companies should be required to aid an investigation. The Electronic Privacy Information Center has long been concerned about "always on" devices and wrote in a July 2015 letter to the US Justice Department that such machines are "increasingly prevalent in the Internet of Things". Along with the Amazon Echo, other technology cited in EPIC's letter was smart televisions, Microsoft Kinect for the Xbox, and various home security devices. How much privacy do our smart devices really provide?

"Americans do not expect that the devices in their homes will persistently record everything they say"; EPIC warned the Justice Department. By introducing ";always on"; voice recording into ordinary consumer products such as computers, televisions and toys, companies are listening to consumers in their most private spaces. EPIC stated that "it is unreasonable to expect consumers to monitor every word in front of their home electronics. It is also genuinely creepy."

If you're an Alexa user concerned that Amazon might be storing your personal conversations, the company provides some options to manage voice recordings and review what you've asked Alexa. The simplest is to delete all voice recordings associated with your Amazon account for each of your Alexa-enabled products. To do so, visit www.amazon.com/mycd or contact customer service.

Read full articles here:

http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html

http://www.msn.com/en-us/news/technology/police-request-echo-recordings-for-homicide-investigation/ar-BBxCB9u?OCID=ansmsnnews11

Foreign Travel

Foreign travel increases the risk of foreign intelligence targeting. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you, and their actions are not restricted within their own country's borders.

Collection techniques include:

- Bugged hotel rooms or airline cabins
- Intercepts of fax and email transmissions
- Recording of telephone calls/conversations
- Unauthorized access and downloading, including outright theft of hardware and software
- Installation of malicious software, intrusions into or searches of hotel rooms, briefcases, luggage, etc
- Recruitment or substitution of flight attendant

Some commonsense security countermeasures should include:

- Do not publicize travel plans and limit sharing of this information to people who need to know.
- Conduct pre-travel security briefings.
- Maintain control of sensitive information, media, and equipment. Do not pack these types of articles in checked baggage; carry them with you at all times. Do not leave them unattended in hotel rooms or stored in hotel safes.
- Keep hotel room doors locked. Note how the room looks when you leave.
- Limit sensitive discussions. Public areas are rarely suitable for discussion of sensitive information.
- Do not use computer or fax equipment at foreign hotels or business centers for sensitive matters.
- Ignore or deflect intrusive or suspect inquiries or conversations about professional or personal matters.
- Keep unwanted sensitive material until it can be disposed of securely.

"If money is your hope for independence, you will never have it. The only real security that a man can have in this world is a reserve of knowledge, experience and ability." Henry Ford