Privacy in Personal Life

2018 was a big year for privacy issues. There were social media scandals, data breaches, and testimony given by some of the largest data companies in front of the Senate. The EU General Data Protection Regulation became enforceable in early 2018, bringing with it the onslaught of privacy policy update and consent emails. With all these high-profile privacy events and incidents, it's easy to forget how we all face issues of privacy in our daily lives. We'll be looking at the smartphone and smart speaker in this post, devices that we carry with us everywhere or that have found a place as permanent fixtures in our homes.

Smartphone Location Tracking

A recent investigation published by the New York Times in December 2018 details how apps installed on smartphones can track a person's movements and location with surprising accuracy. The New York Times reviewed the database of one company containing more than 1 million smartphone devices, and found that they could track and identify an individual (a Lisa Magrin) even though her identity was not initially disclosed in the raw data. The investigators were able to track when she traveled to her dermatologist's office and ex-boyfriend's house, updating her data as often as once every 2 seconds.

Ms. Magrin's location data found its way into this database when her data was sold without her knowledge through an app on her smartphone. A mobile analysis firm called MightySignal found that 1,200 apps on the Google Android system and 200 apps on Apple's iOS had location sharing code, and the Times' own research found 17 out of 20 examined apps sent exact longitude and latitude data to around 70 companies.

One might wonder if consumers have any control over when apps on their smartphones record and send such detailed location information. Typically, location services must be enabled by the user for an app on a smartphone to acquire location data. The Times found that consumers were confused or uninformed, however, about what they were agreeing to when prompted to turn on these location services: "An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold. That disclosure is often buried in a vague privacy policy." A user may unwittingly give permissions to an app by granting it access to send personal data to other companies for uses far beyond what was imagined.

Once this location data is sold to companies, it is used for a variety of purposes such as market analysis. Access to this type of data has also opened new opportunities and avenues in the advertising space, allowing for more targeted, geographically based advertisements. For example, NPR reported on a

phenomenon where marketing companies target ads for law firms on individuals who have recently visited emergency rooms. Wholefoods has similarly taken advantage of customer location data. The grocery chain ran an advertising campaign using location data by placing geofences, or virtual geographical boundaries, near the stores of its competitors to target ads at nearby shoppers.

Smart Speakers and Virtual Assistants

Smart Speaker and virtual assistant devices, such as the Google Home or Amazon Echo, were a popular gift this past holiday season. The recipients made up 8% of the US population according to a report by NPR and Edison Research. Overall, 53 million people in the United States over the age of 18 own a Smart Speaker (21% of the United States population).

Although Smart Speakers enjoy such wide popularity, ever present is the question of "are they listening?" A survey of 3,000 people by the research firm MusicWatch found that 48% of those surveyed had privacy concerns regarding these devices. This distrust of Smart Speakers may stem from the voice activated interface used to interact with these devices.

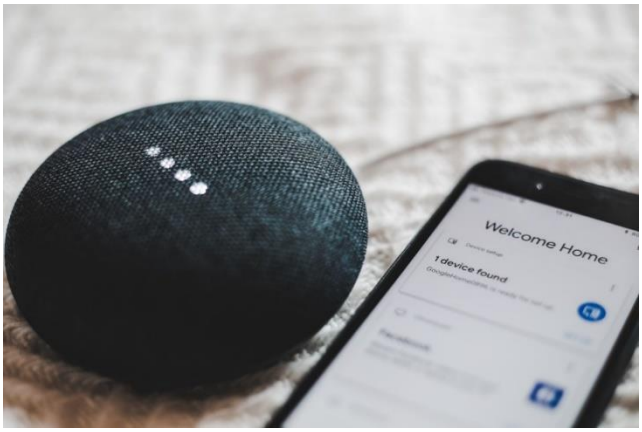
Products like the Google Home or Amazon Echo passively listen for "wake-up" or "hot" words, such as "Alexa" or "OK Google," that alert the device that it is about to receive additional voice commands from the user. While waiting for these keywords, devices such as the Echo are only *passively* listening (not actively recording). Once activated, however, these devices record, transcribe, and send what they hear to the cloud where the files are stored and processed.

For Google and Amazon Smart Speakers, the recordings stay in the cloud until deleted by the user. Google specifies that it saves this data "to make our services faster, smarter, and more useful to you, and also to help us protect you from malware, phishing, and other suspicious activity." Amazon states that it keeps the transcriptions and recordings "to improve the accuracy of the results provided to you and to improve our services." Google and Amazon give users access to these recording libraries and a way to delete those files. Apple (for Siri), however, does not.

While the Google Home and Amazon Echo do not actively record conversations before they detect a hotword, there have been incidents where a device has been unintentionally activated, triggering a recording. On an interview with a local radio station, the owner of an Amazon Echo relayed how her device activated after mistakenly picking up the word "Alexa" in the background. The device then recorded a conversation she was having with her husband before sending it to her husband's colleague. Other users of Smart Speakers have reported that upon review of their files, their devices have made similar recordings as the result of hotword word false positives.

Recently, a novel use for these recordings has emerged within our judicial system. There have been at least two instances where a court has requested the release of Amazon Echo recordings and data pertaining to criminal cases. In a 2015 murder case, Amazon released data from its servers after receiving consent. More recently, a judge ordered Amazon to produce "any recordings made by an Echo smart speaker with Alexa voice command capability… as well as any information identifying cellular devices that were paired to that smart speaker" for the time period surrounding the murder.

Protecting Our Privacy



Both smartphones and smart speakers have become integral parts of daily life for people living in the United States. Beneath of the promise of ease and efficiency, however, lie serious threats to one's privacy. One might wonder how they may maintain a level of confidentiality without giving up the devices we use everyday. The New York Times has outlined the steps to disable location tracking on your phone. Similar instructions have been provided by theVerge on how to delete recordings off of your Google Home and Amazon Alexa devices. While not perfect solutions to all of the privacy issues in our daily lives, these methods will at least keep our smartphone location data and Smart Speaker audio recordings out of reach.

Happy Data Privacy Day,

PRIVACY GROUP