An Amazon Echo may be the key to solving a murder case

Posted Dec 27, 2016 by Sarah Buhr (@sarahbuhr) techcrunch.com

Internet-connected devices may start helping in criminal cases. As first reported in The Information, police in Bentonville, Arkansas have issued a warrant to Amazon, asking the company to hand over data from an Echo device to help prosecute a suspected murderer.

James Andrew Bates, the suspect in the case, was charged with first-degree murder in November of 2015 after authorities found victim Victor Collins strangled and drowned in Mr. Bates' hot tub.

Mr. Bates told police he'd invited Collins and two other friends, Owen McDonald and Sean Henry, over to watch a football game and said he decided to go to bed about 1 a.m., leaving the victim and McDonald to hang out and drink in his hot tub.

According to Bates' affidavit, he found Collins face down in the water when he woke up several hours later. However, McDonald says he left Bates and Collins around 12:30 a.m., which was a story confirmed by McDonald's wife.

According to phone records, Bates was also texting a woman throughout the evening and had placed several calls to his dad, other friends (including McDonald) and the Flying Fish restaurant. None of the calls went through and Bates told police these were accidental butt dials.

Bates has several internet-connected devices in his home, including a Nest thermostat and a Honeywell alarm system, but the key witness in the case may be his Amazon Echo, which, as per The Information, police records say could have controlled the streaming music, which was being wirelessly transmitted throughout the night using Echo's assistant Alexa.

However, it's unclear how much data police could extract from the device or how useful that data would be in the case. Alexa is always listening through a system of seven built-in microphones but waits for you to say the "wake word" to send it commands, like asking for the weather or which music to play, according to the company. The device also streams your audio to the cloud, including a fraction of a second of audio before the wake word.

Amazon has so far declined to hand over information in the case, according to court records, and the company says it will not be releasing customer information "without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."

Police have seized the Echo from Bates home anyway, as material evidence, but the device that might offer a better clue as to what happened that night might be the home's smart water device. According to The Information, court records show Bates' home ran 140 gallons of water between 1 a.m. and 3 a.m. on the night in question.

But the broader takeaway in this instance is just how much these IoT devices could be used for or against us, legally. This appears to be a first-of-its-kind case and we are sure to see many more of these types of inquiries in the future.

It is generally considered inappropriate to record a conversation without permission. When police informants wear a wire, there is usually pre-authorization by a judge. Twelve states in the US require all parties to consent to recording before a conversation can be recorded. The remaining states require at least one party to consent. So, in the US, it is never OK for a third party, such as law enforcement, to record a conversation without consent, or warrant. However, it is generally considered appropriate to record metadata about the conversation: who participated, at what time it took place, how long it lasted, and so on.

Now consider a recent case involving Amazon's Echo: https://techcrunch.com/2016/12/27/an-amazon-echo-may-be-the-key-to-solving-a-murder-case/.

There are multiple parties involved: (1) law enforcement (2) Amazon (3) the owner of the Echo (4) Various people who may have been recorded by the Echo (including the owner).

There are two different types of data involved: (1) The recorded conversations and other sounds, and (2) Metadata about the time, duration, etc. of these conversations.

Reasoning by analogy from the preceding paragraph, argue for who owns what data, and who may have access to what data, WITHOUT a judicial warrant. (Let us assume that if a crime has been committed, such as the murder in this example, that a judge will sign a warrant that can override normal privacy and ownership expectations. So this question is about what you could/should do if no warrant can be obtained).

Extend your analysis of the preceding paragraph to data regarding your interaction with your electronic merchant. There are two parties to this interaction: you and the merchant. Who may record the data, who may publish/share the data? Make sure you also consider scenarios where you, as the customer, may wish to publish a review of your (unsatisfactory) interaction with an online merchant.