A study of security and privacy issues associated with the Amazon Echo

Catherine Jackson* and Angela Orebaugh

School of Continuing and Professional Studies,
University of Virginia,
Charlottesville, VA, USA
Email: caj5rh@virginia.edu
Email: angelaorebaugh@virginia.edu
*Corresponding author

Abstract: More than 11 million US consumers have an Amazon Echo installed in their homes (Gonzales, 2017). While many consumers view the Amazon Echo as a useful helper in the home to provide information, play music, and order items online, consumers underestimate the device's security and privacy impacts. Additionally, law enforcement officials are beginning to see how consumer internet of things (IoT) devices can provide crucial evidence in cases. This paper presents security and privacy issues with the Amazon Echo and recent cases in which law enforcement officials have employed the Amazon Echo in an investigation. Due to the Amazon Echo's privacy issues and potential uses in court, this paper analyses the fourth amendment in regard to the Amazon Echo. This paper concludes with suggested recommendations that Amazon Echo owners should employ for greater security and privacy.

Keywords: smart speaker; intelligent personal assistant; virtual assistant; Amazon Echo; Alexa; information security; privacy; law enforcement; internet of things; IoT.

Reference to this paper should be made as follows: Jackson, C. and Orebaugh, A. (2018) 'A study of security and privacy issues associated with the Amazon Echo', *Int. J. Internet of Things and Cyber-Assurance*, Vol. 1, No. 1, pp.91–100.

Biographical notes: Catherine Jackson graduated from the University of Virginia in May 2017 with a dual major in English Literature and American Government as well as a graduate certificate in Cybersecurity Management from the UVA's School of Continuing and Professional Studies. She currently works as a Technology Analyst at the Accenture Federal Services, specialising in cybersecurity strategy.

Angela Orebaugh is an Assistant Professor and Director of Cybersecurity and IT Programs at the University of Virginia where she provides academic leadership and direction to the cybersecurity and IT programs, its students, and alumni. Prior to moving in to academia, she spent over 20 years consulting in information technology and cybersecurity. She is currently performing research in the security of cyber physical systems and the internet of things.

1 Introduction

On 23 June 2015, Amazon released the Amazon Echo, the first smart speaker with integrated intelligent personal assistant, to the general public in the USA (Callaham, 2015). Amazon sold over 11 million echo devices from the time of its release through 1 December 2016 (Gonzales, 2017). The Amazon Echo's hands-free speaker connects to the Alexa voice service app, enabling the device to play music, read the news, answer questions posed by the user, and order items online. The Echo's seven microphones and beamforming technology allow the device to listen to requests from the user (Amazon, 2017a). The echo's voice, Alexa, awakes when the user says the wake word, 'Alexa'. Since Alexa lives in the cloud with large storage capacity, the device becomes increasingly smarter with repeated use, learning and storing speech patterns, vocabulary, and personal preferences.

2 Amazon Echo features and vulnerabilities

While 'Hey, Alexa turn the lights on' and similar requests have made users' lives easier and even fulfilled personal dreams of futuristic living, the Amazon Echo creates many security and privacy concerns for its users. Many of the security and privacy concerns for Amazon Echo and other intelligent cognitive assistants (ICA) revolve around mutual trust. "Trust requires attenuation to interaction patterns and accurate fulfillment of requests and system tasks, an attention to coordination of tasks and resources. But it also requires thoughtful care as to how and where data about such requests travels, how ICAs track or log user interactions, and intersections with IoT security and data protections" (NSF, 2016). Trust semantics research for Amazon Echo must focus on the following:

- *Accuracy.* Is the output provided by Alexa sufficiently accurate to ensure human trust? This includes information offered, decisions made, and actions taken. Is the input provided to Alexa sufficiently accurate to ensure ICA trust? This includes speaker recognition and requests and commands.
- *Fairness.* Is the output provided by Alexa free or bias and manipulation? This include social and ethical considerations as well as data integrity attacks.
- *Privacy.* Is the data gathered by Alexa and stored locally or in the Amazon cloud kept private? If the data is used to improve the ICA and its overall functionality, is this done in a sufficiently anonymised way? (NSF, 2016)

Specific vulnerabilities and security and privacy concerns for Amazon Echo include the following:

- *Listening and recording:* because the device is voice activated, it is always listening for the user to say the wake word. While it is listening, the Amazon Echo remains "in an inert state of buffering and re-recording, allowing the microphone to passively listen for a key word without recording or transmitting information" (Gray, 2016). When the user issues the wake word and a request, Alexa records an audio file of the request and sends that file to the cloud to process the request and create a response (Moynihan, 2016). According to Amazon (2017b), "the audio stream includes a fraction of a second of audio before the wake word, and closes once your question or

request has been processed". All requests to Alexa are stored as audio clips in the user's Amazon account. The audio clips are encrypted via secure sockets layer (SSL) when sent to the cloud, making it challenging for an attacker to capture a user's conversations with Alexa even if the home network is compromised. However, a network-level attacker can identify the encrypted SSL traffic between the Amazon Echo and Amazon.com to detect when a user is interacting with Alexa (Apthorp et al., 2017).

- *Voice activation:* Amazon Echo's voice recognition feature cannot differentiate between different voices. Anyone within microphone range can make requests to Alexa. This concept has been demonstrated repeatedly, most notably by making erroneous dollhouse purchases after a television news story triggered Alexa (Hackett, 2017). Other instances have been movies or television shows with characters named Alexa, such as 50 first dates (Sony Pictures, 2004), and the cartoon South Park purposely triggering Alexa with a series of profanities (Warren, 2017). Some research is making progress in trust semantics that would facilitate trustworthiness of sources in Alexa voice activation (Kotis and Vouros, 2016).
- *High frequency attacks:* Chinese researchers at the Zhejiang University have exploited an Amazon Echo vulnerability through what they call a DolphinAttack (Zhang et al., 2017). This attack translates vocal commands into ultrasonic frequencies too high for the human ear to hear (> 20 KhZ), but easily detected by Amazon Echo's microphones and Alexa assistant. Using low cost, low tech equipment, the researchers were able to invoke any command with the high frequency attack.
- *Physical root access attacks:* on a more nefarious level, attackers can gain root level access to the Amazon Echo's underlying Linux operating system through physical access to the device (Barnes, 2017). The vulnerability is exploited through the easily accessible exposed debug pads on the base of the device and the device's ability to boot from an external SD card. Once root level access is obtained, attackers can gain remote access to eavesdrop, insert comments, and install malware with no evidence of tampering. This may not be a concern for Amazon Echo home users who have tight physical security around their device, but many hotel chains are beginning to deploy the Echo in hotel rooms including the Wynn in Las Vegas (Welch, 2016) and Marriott (Crothers, 2017). The Amazon Echo deployment in hotel rooms is leading to big privacy concerns for hotel guests.
- *Cameras and Drop-In:* Amazon released the echo show in late June 2017. The echo show incorporates a display screen and camera to the smart speaker and Alexa technology. While a detailed review of the Echo Show is beyond the scope of this paper and will be included in future research, the inclusion of a camera and the new drop-in feature is causing privacy concerns for users. The drop-in features works like an intercom for instant communication between Echo devices. On the echo show, the video camera will activate, leading to a frosted glass screen for ten seconds before the caller can see anything. The recipient will hear a chime and see the green light on their echo to indicate an incoming drop-in. The drop-in feature has also been released as an upgrade on older echo models for audio only (Heater, 2017).

- *Cloud data storage:* another privacy concern is that Amazon is able to view user dialogues with Alexa and use them to the company's advantage. Every hour, Amazon uploads gigabytes of Alexa voice recordings to its vast data centre. Amazon uses these recordings to feed Alexa's neural network, the form of artificial intelligence that allows a device to "learn" by absorbing a large and diverse amount of data, instead of being manually programmed (Cao and Bass, 2016). The more speech recognition that a device intakes, the better it becomes at understanding and carrying on a normal conversation. While this seems beneficial to the user, Amazon also learns the user's daily routine of interacting with Alexa, including morning news updates, traffic and weather checks, music tastes, item preferences, and random queries. The use of this data by others, including law enforcement, presents the largest potential threat to user privacy.

3 Law enforcement and the internet of things (IoT)

Everyday household items are becoming increasingly interconnected as part of the IoT to perform tasks and increase productivity and efficiency. These IoT devices collect data and closely monitor the lives of their owners, leaving behind a digital trail for law enforcement investigations. Mark Stokes, head of Scotland Yard's digital, forensics, and cyber communications unit asserted that police officers are being trained to look for the digital footprints provided by IoT

> "Wireless cameras within a device such as the fridge may record the movement of suspects and owners. Doorbells that connect directly to apps on a user's phone can show who has rung the door and the owner or others may then remotely, if they choose to, give controlled access to the premises while away from the property. All these leave a log and a trace of activity". (Smith, 2017a)

In the future, investigators will be able to use a digital forensics toolkit to download and scan data from the crime scene including devices such as smart speakers and intelligent personal assistants. Already, law enforcement has enlisted the help of Amazon's Alexa during an investigation.

In November 2017, James Bates invited a few friends over to watch a football game and stay the night at his home in Bentonville, Arkansas. The following morning, one of these friends, Victor Collins, was found strangled in Bates' hot tub. Bates was charged with murdering Victor Collins, but pled innocent.

During the investigation, the police found an Amazon Echo located in Bates' home. Due to the echo's ever-present ear listening for its wake word, the police thought that the echo could potentially shed some light on Collins' murder. Even if Bates had not submitted any requests directly to Alexa, the television or anyone accidentally saying the word 'Alexa' could have prompted the device to record an audio file of its surroundings. An Arkansas state judge signed a search warrant for the Amazon Echo, but the seizure yielded minimal results due to the data storage on Amazon's cloud. Amazon released the customer's subscriber and purchase information but refused to offer any recordings or data related to Bates' conversations with Alexa.

Amazon contended that the prosecutors provided insufficient evidence to compel giving this data to the Arkansas police and doing so would violate the customer's privacy rights. Amazon demanded that the prosecutors prove that this information was not

available elsewhere and that the court listens to the recordings first in order to determine their relevance to this case. Amazon publicly stated in the court documents: "Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials" (Mukunyadzi, 2017). In its motion to quash the subpoena of echo recordings, Amazon based its argument on its original nature as an online bookseller, likening echo recordings to book purchase records. Amazon's lawyers at Davis Wright Tremaine cite case law stating that the First Amendment protects people's right to receive information and forbids the government from being privy to this information without a compelling need (Hancock, 2017). However, there is already another case, Zurcher v. The Stanford Daily, which set precedent that a warrant is sufficient to override first amendment rights (Atherton, 2017). While Amazon continued to refuse to supply the Echo voice recordings, the defendant and his attorney gave permission to voluntarily release the recordings. Amazon provided the data to prosecutors later that same day (McLaughlin, 2017).

Although Amazon was adamant in protecting consumer data privacy in the *Arkansas vs. Bates* case, it may not be successful in the future. Various legal interpretations and rulings could create precedent to allow devices such as the Amazon Echo and Alexa interactions to be used in an investigation and court of law. Additionally, laws could be passed to "allow the police to remotely activate these devices and eavesdrop on suspects" (Cranz, 2016). The *Arkansas vs. Bates* case is pivotal in the area of consumer privacy because it has sparked a much wider debate regarding the Fourth Amendment, IoT devices, and the data they store.[1]

4 Analysis of the fourth amendment in the technology age

With Amazon Echo and other IoT devices increasingly taking residence in consumer homes and collecting information about the user, conflicts between law enforcement and consumer privacy will continue to arise. The *Arkansas vs. Bates* case and many to come, illuminate the issue of consumer privacy rights protected under the fourth amendment that provides "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and person or things to be seized". The Founders specifically oriented this Amendment to the citizens' demand for protection against general searches of their private property, particularly focusing on material things, by the Government. The Founders could not have imagined the new technology available today and increasing connectivity of IoT devices in our daily lives, which instigate debate regarding protection from government searches.

The earliest Supreme Court case to discuss the fourth amendment protection of personal privacy occurred in 1886 in *Boyd v. United States*. Customs officers confiscated several cases of plate glass from the defendants because they believed the shipment paperwork had been falsified (Boyd v. United States, 2016). In court, the judge ordered the defendants to produce records for the quantity and value of the shipments. The defendants argued that they could not be compelled to produce evidence against themselves. The Supreme Court declared this statute in which the government required

individuals to produce private papers to be unconstitutional. This decision paved the way for a more liberal interpretation of the fourth amendment's protection of personal privacy. In this interpretation, 'search and seizure' under the Fourth Amendment was not restricted only to government officials physically entering, searching, and taking illegal contraband, but instead, compelling a person to hand over incriminating personal papers was determined to be equivalent to a 'search and seizure'. Having these two circumstances be equally unconstitutional points to an underlying concept of a person's dignity that the founders created the fourth amendment to protect. In the court's opinion, Justice Joseph Bradley explains this broader definition of privacy which encompasses not only protecting a person's property, but also a person's dignity. On the illegality of general warrants, Justice Bradley proclaimed:

> "They apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence, – it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment." (O'Brien, 2014)

Justice Bradley describes personal security as an 'indefeasible right' and a 'sacred right,' arguing that the invasion of this personal privacy is what makes general searches unconstitutional. Citizens have a right to privacy in their own home and as a result of this case, the fourth amendment extends beyond 'persons, houses, papers, and effects' to include other 'constitutionally protected areas' such as business offices, stores, hotel rooms, apartments, automobiles, and taxis. This case remains particularly relevant in the age of electronic communication and IoT devices in which there is no physical trespass to search and seize a person's private papers (often in the form of email or electronic file) but rather the files are viewed remotely. The decision to equate this offense to a 'search and seizure' allows modern judges to interpret the Fourth Amendment more loosely to defend a person's 'sacred right' of personal security from governmental intrusion.

In Amazon's brief, Amazon lawyers reference *Riley v. California (2011)*, arguably a watershed case in terms of upholding the privacy rights of citizens against law enforcement searches. In this case, the police pulled over David Leon Riley for driving a car with expired license registration tags. Because Riley's license was suspended, the police impounded the vehicle; first, performing an inventory search of the car to appertain all of the items located within the vehicle at the time of the impoundment. During this search, the police found two firearms and arrested Riley for possession. Since Riley had his cell phone in his pocket at the time of his arrest, the police confiscated it. A gang unit detective analysed the photos and messages on the phone linking Riley to a known gang and a recent shooting confirmed by ballistics tests.

Before trial, Riley moved to suppress the evidence the police had collected from his phone linking him to the gang. This case moved to the Supreme Court to determine whether the evidence admitted at trial from a warrantless search of Riley's phone violated Riley's fourth amendment rights. Writing the unanimous opinion for the Court, Chief Justice John Roberts stated that the warrantless search exception following an arrest exists only to protect the police officers from harm and preserve evidence. Neither of these issues is at play with digital data as the data cannot cause physical harm to the officers and the phone may be stored safely in a 'Faraday bag' until a warrant is obtained

(IIT, 2017). The Court differentiated cell phones from other items that could be seized such as a wallet, describing smartphones as mini computers known for their vast storage capacity: "the sum of an individual's life can be reconstructed from a thousand photographs, labeled with dates, times, locations, and descriptions; the same cannot be said of a photograph of one or two loved ones tucked into a wallet" (Riley V. California, 2014). In addition, the Court held that information accessible on the phone but stored in cloud computing does not even constitute information that is on the person's being. The Court ruled in favour of individual privacy, concluding that a warrant is generally required before this type of search. In some emergencies where the Government's interests are compelling, warrantless cell phone searches may be permitted.

In *Arkansas vs. Bates*, Amazon's lawyers likened the cell phone's capability to display an individual's life to the Amazon Alexa recordings of its owner's daily life. While this comparison holds weight, the key difference in the *Arkansas vs. Bates* case is that the Arkansas police were granted a warrant to access these recordings during the specified hours of the murder. Without further law created to prevent warranted searches of IoT devices like the Amazon Echo, Amazon possesses limited legal footing to resist complying with law enforcement. While general searches of IoT devices by law enforcement will not be permitted, law enforcement officials will increasingly look to IoT devices to assist investigations.

5 Conclusions and recommendations

Although, the Amazon Echo and other IoT devices have simplified home automation, they can also invoke numerous security and privacy concerns related to unauthorised use, surveillance, and access to private data. Although some research looks promising for creating mutual trust in human-ICA interactions (Kotis and Vouros, 2016), more research is needed to facilitate trust in the areas of accuracy, fairness, and privacy (NSF, 2016).

Our analysis of the security and privacy concerns for the Amazon Echo have resulted in the following recommendations:

1 *Voice activation.* Alexa trusts and responds to requests from anyone, including those on TV or passing by an open window. Without proper security measures, unauthorised users can order items on Amazon, unlock the doors of the house, control thermostats, locate phones, and control GE devices such as ovens and laundry machines.

   Recommendation: change the wake word for the Amazon Echo in the Alexa app. In addition to 'Alexa', the Amazon Echo enables users to change the wake word to 'Amazon', 'echo', and 'computer'. This will keep commercials (Witwam, 2017), news stories (Hackett, 2017), and movies with characters named Alexa (Sony Pictures, 2004) from activating the device.

   Recommendation: Enable request notification sounds at the start and end of a request to know when Alexa is triggered.

   Recommendation: place the Amazon Echo away from windows, doors, and answering machines.

2 *Listening and recording.* The benefit of an intelligent digital assistant is voice activation which requires the device to constantly listen for the wake word. However, there may be times when users want extra privacy and do not want Alexa to be quietly listening in on conversations.

   Recommendation: mute the Amazon Echo by pressing the mute button on top of the device. The LED indicator for the mute button will turn red and Alexa will no longer be listening. The mute button physically disconnects the circuit flow to the microphone hardware. The mute button on the echo show will also deactivate the camera. Some users may want to regularly mute the Amazon Echo when they are not at home. For those who want a more permanent, private solution, keep the Amazon Echo muted and use the Amazon Echo Remote, which is push-for-use and not always on.

   Recommendation: unplug the Amazon Echo and other non-essential IoT devices when you are leaving home for an extended period of time, such as vacation.

3 *Cloud data storage.* Alexa stores a log of requests in the Amazon cloud for the associated Amazon account.

   Recommendation: regularly review Alexa's stored history to ensure there are no unexplained or unauthorised actions. For extra privacy, delete stored recordings as necessary through the Alexa app or through the Amazon account's content and devices portal.

4 *Voice purchasing.* By default, voice purchasing is enabled on the Amazon Echo.

   Recommendation: disable voice purchasing or add a 4-digit PIN for purchases through the Alexa app (McClelland, 2017).

While these recommendations can improve consumer security and privacy for the Amazon Echo, similar actions should be taken for other intelligent personal assistants. Additionally, it is important to raise overall consumer awareness of security and privacy. In an age where individuals have become accustomed to sharing their daily lives with the world on social media, individuals have forgotten the importance of privacy. They assume that their IoT devices such as intelligent personal assistants will be safe from access without taking any security and privacy precautions.

To help raise awareness of security and privacy concerns, IoT device vendors should make clear the security capabilities they provide for their devices and offer suggestions for secure implementation. Just as IoT devices simplify life for the consumer, so, too, should IoT device vendors simplify security and privacy for the consumer? Companies that deliver secure IoT devices will earn trust and respect in the consumer market. Technology vendors and consumers will need to continue to work together to find new security and privacy solutions for operating in an increasingly connected environment.

References

Amazon. (2017a) *Amazon Echo – Amazon Official Site – Alexa-Enabled* [online] https://www.amazon.com/dp/B00X4WHP5E (accessed February 23).

Amazon. (2017b) *Amazon.com Help: Alexa and Alexa Device FAQs* [online] https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (accessed February 23).

Apthorpe, N., Reisman, D. and Feamster, N. (2017) *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*, arXiv preprint arXiv:1705.06805.

Atherton, K. (2017) 'Amazon Echo and the internet of things that spy on you', *Popular Science* [online] http://www.popsci.com/amazon-echo-privacy (accessed 11 October 2017).

Barnes, M. (2017) *Alexa, are you listening?' MWR Labs* [online] https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening/ (accessed 11 October 2017).

Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524, 29 L. Ed. 746, 1886 U.S. LEXIS 1806, 3 A.F.T.R. (P-H) 2488, 1 February 1886, US.

Callaham, J. (2015) *Amazon Echo Is Now Available for Everyone to Buy for $179.99, Shipments Start on July 14*, 23 June, Android Central [online] http://www.androidcentral.com/amazon-echo-now-available-everyone-buy-17999-shipments-start-july-14 (accessed 11 October 2017).

Cao, J. and Bass, D. (2016) *Why Google, Microsoft and Amazon Love the Sound of Your Voice – Bloomberg*, 13 December, Bloomberg Technology [online] https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice (accessed 11 October 2017).

Cranz, A. (2016) *Amazon's Alexa Is Not Even Remotely Secure and I Really Don't Care*, Gizmodo [online] https://gizmodo.com/alexa-is-not-even-remotely-secure-and-really-i-dont-car-1764761117 (accessed 11 October 2017).

Crothers, B. (2017) *Amazon Alexa, Apple Siri Headed to Hotel Rooms, Report Says*, Fox News [online] http://www.foxnews.com/tech/2017/03/27/amazon-alexa-apple-siri-headed-to-hotel-rooms-report-says.html (accessed 11 October 2017)

Gonzales, A. (2017) *Amazon has Sold more than 11 Million Echo Devices, Morgan Stanley Says*, January, Seattle Times [online] http://www.seattletimes.com/business/amazon/amazon-has-sold-more-than-11-million-echo-devices-morgan-stanley-says/ (accessed 11 October 2017).

Gray, S. (2016) 'Always on: privacy implications of microphone-enabled devices', *Future of Privacy Forum*.

Hackett, R. (2017) *Amazon Echo's Alexa Went Dollhouse Crazy*, Fortune [online] http://fortune.com/2017/01/09/amazon-echo-alexa-dollhouse/ (accessed 5 May 2017).

Hancock, B. (2017) *Fighting Echo Warrant, Amazon Has Scant Law to Draw On*, 1 March, Inside Counsel [online] http://www.insidecounsel.com/2017/03/01/fighting-echo-warrant-amazon-has-scant-law-to-draw (accessed 11 October 2017).

Heater, B. (2017) *Amazon Disputes Claims that Echo Show's Drop-In Feature is a Security Risk*, TechCrunch [online] https://techcrunch.com/2017/06/28/amazon-disputes-claims-that-echo-shows-drop-in-feature-is-a-security-risk/ (accessed 11 October 2017).

IIT Chicago-Kent College of Law (2017) *Riley v. California*, Oyez [online] https://www.oyez.org/cases/2013/13-132 (accessed 15 March).

Kotis, K. and Vouros, G.A. (2016) 'Trust semantics in IoT entities' deployment', *Workshop on Artificial Intelligence and Internet of Things (AI-IoT), 9th Hellenic Conference on Artificial Intelligence (SETN 2016).*

McClelland, D. (2017) *How to Secure Your Amazon Echo*, 17 January, Tech Radar [online] http://www.techradar.com/how-to/how-to-secure-your-amazon-echo (accessed 11 October 2017).

McLaughlin, E. (2017) *Suspect Oks Amazon to hand over Echo Recordings in Murder Case*, CNN [online] http://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/ (accessed 11 October 2017)

Moynihan, T. (2016) *Amazon Echo and Google Home Record What You Say. What Happens to Your Data?*, 5 December, Wired [online] https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ (accessed 11 October 2017).

Mukunyadzi, T. (2017) *Amazon Resists Request for Echo Info in Arkansas Slaying*, 22 February, ABC News [online] http://abcnews.go.com/Technology/wireStory/amazon-resists-request-echo-info-arkansas-slaying-45660945 (accessed 11 October 2017).

National Science Foundation. (2016) *Intelligent Cognitive Assistant Workshop Summary and Recommendations* [online] https://www.nsf.gov/crssprgm/nano/2016-1001_Intelligent CognitiveAssistants_Workshop_2016_Final_Report.pdf (accessed 11 October 2017).

O'Brien, D.M. (2014) *Constitutional Law and Politics: Civil Rights and Civil Liberties*, 9th ed., pp.1003–1004, Vol. 2, W.W. Norton, New York.

Pogue, D. (2017) *Your Echo Is Listening, Which Could Someday Lead to an Invasion of Your Privacy*, March, Scientific American [online] https://www.scientificamerican.com/article/your-echo-is-listening-which-could-someday-lead-to-an-invasion-of-your-privacy/.

Riley v. California (2014) *Supreme Court of the United States*.

Smith, M. (2017a) *Cops to Increasingly Use Digital Footprints from IoT Devices for Investigations*, 2 January, Network World [online] http://www.networkworld.com/article/3154064/security/cops-to-increasingly-use-digital-footprints-from-iot-devices-for-investigations.html (accessed 11 October 2017).

Sony Pictures (2004) *50 First Dates* [online] http://www.imdb.com/title/tt0343660/ (accessed 5 May 2017).

Warren, T. (2017) *South Park Trolls Amazon Alexa Owners in this Week's Episode*, The Verge [online] https://www.theverge.com/2017/9/16/16318694/south-park-amazon-alexa-google-home (accessed 11 October 2017).

Welch, C. (2016) *The Wynn Las Vegas is Putting an Amazon Echo in Every Hotel Room*, The Verge [online] https://www.theverge.com/circuitbreaker/2016/12/14/13955878/wynn-las-vegas-amazon-echo-hotel-room-privacy (accessed 11 October 2017).

Witwam, R. (2017) *Burger King Created a Commercial that Hijacks your Google Assistant*, Forbes [online] https://www.forbes.com/sites/ryanwhitwam/2017/04/12/burger-king-created-a-commercial-that-hijacks-your-google-assistant/#45a006921d7b (accessed 5 May 2017).

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T. and Xu, W. (2017) *DolphinAttack: Inaudible Voice Commands*, arXiv preprint arXiv:1708.09537 [online] https://endchan.xyz/.media/50cf379143925a3926298f881d3c19ab-applicationpdf.pdf (accessed 11 October 2017).

Notes

1 The Amazon Echo was not the only smart device involved in the *Arkansas vs. Bates* case. The police also found that Bates had installed a smart water meter in his home. Suspecting that Bates used extra water to clean blood off his hot tub and patio, the police checked the water metre. Records showed that 140 gallons of water were used between 1:00am and 3:00am on the night of the murder (Pogue, 2017).