Richmond Journal of Law & Technology Volume XXV, Issue 4

ALEXA, ARE YOU A FOREIGN AGENT?
CONFRONTING THE RISK OF FOREIGN INTELLIGENCE EXPLOITATION OF PRIVATE HOME NETWORKS, HOME ASSISTANTS, AND CONNECTIVITY IN THE SECURITY CLEARANCE PROCESS

Jonathan Schnader*

Cite as: Jonathan Schnader, *Alexa, Are You a Foreign Agent? Confronting the Risk of Foreign Intelligence Exploration of Private Home Networks, Home Assistants, and Connectivity in the Security Clearance Process*, 25 RICH. J.L. & TECH., no. 4, 2019.

* Jonathan A. Schnader lives in Washington, DC. He earned his bachelor's degree in Psychology and Classical Humanities from Miami University of Ohio. He earned his J.D. *cum laude* from Syracuse University College of Law with a Certificate in National Security and Counterterrorism Law. Following law school, he worked as an Assistant Public Defender in Rochester, NY for five and a half years handling upwards of three-thousand criminal cases. In addition to being licensed to practice law in New York and Washington DC, he became a Certified Anti-Money Laundering Specialist. Jonathan graduated with distinction in 2019 from Georgetown University Law Center, where he completed a Master of Laws in National Security. His academics and current practice focus on national security dimensions of several areas, including cybersecurity; artificial intelligence; blockchain and cryptocurrency; intelligence and counterintelligence; and social media. He currently works as an Attorney Contractor doing cryptocurrency regulatory compliance with a boutique law and strategic consulting firm specializing in cryptocurrency and finTech, Ouroboros, LLP.

I. INTRODUCTION

[1] Virtually all facets of the home can be remotely controlled over the "Internet of Things" ["IoT"]; a Nest brand thermostat controls your furnace and air conditioning, adjusting based on schedules set by the user, or automatically shutting off when you leave the house.[1] Smart light fixtures turn on or off, or dim, in accordance with your wishes.[2] Automatic pet feeders dispense cat food on a schedule or remotely from a smart phone.[3] Wireless security cameras controlled over local network Wi-Fi obviate the need for cumbersome and inconvenient wires.[4] The unifying device—the switchboard, gatekeeper, and operator—is the home assistant.[5]

[1] *See Nest Learning Thermostat*, NEST, https://nest.com/thermostats/nest-learning-thermostat/overview/ [https://perma.cc/3MKQ-LCF9] (describing how the Nest Learning Thermostat automatically adjusts room temperatures according to user preference).

[2] *See* Ry Crist, *Been Sleeping on Smart Lights? Time to Wake Up*, CNET (Jan. 20, 2019, 5:00 AM PST), https://www.cnet.com/news/youre-running-out-of-reasons-not-to-get-smart-lights/ [https://perma.cc/E5XQ-WWUN?type=image] (describing the ease with which users can turn on, off, fade, adjust, or otherwise control smart bulbs).

[3] *See* CI, *10+ iPhone-Compatible Dog Feeders [App Enabled]*, IPHONESS (Mar. 8, 2019), https://www.iphoneness.com/cool-finds/iphone-compatible-dog-feeders-app-enabled/ [https://perma.cc/4BF7-GR67] (listing iPhone app and WiFi controlled dog feeders).

[4] *See* Daniel Wroclawski, *Best Wireless Home Security Cameras of 2019*, CONSUMER REPORTS, https://www.consumerreports.org/wireless-security-cameras/best-wireless-home-security-cameras-of-the-year/ (last updated Jan. 1, 2019) [https://perma.cc/HEH5-NUXG] (listing and describing wireless features of wireless home security cameras).

[5] *See* Jerry Hildenbrand, *What's Home Assistant and Why Should Home Automatic Enthusiasts Consider It?*, ANDROID CENT. (Apr. 12, 2018), https://www.androidcentral.com/whats-home-assistant-and-why-should-home-automation-enthusiasts-consider-it [https://perma.cc/ECC4-6E74] (describing how home assistants function as centralized home automation hubs).

[2] Home assistant devices—like Siri, Canary, and Google[6]—seamlessly weave all parts of a person's life together, allowing for simplified management of those chores at home that can easily overwhelm the working woman or man,[7] but Amazon's Alexa, the artificial intelligence ["AI"] who lives in the device called the "Echo," is the most polished.[8] Link a bank account, your contacts, or streaming music service, and Alexa will manage them for you.[9] Activate Alexa with her special voice command, "Alexa" (you know she heard you because a blue ring of light illuminates almost eagerly when you say her name), followed by a

[6] This paper will use Amazon's Alexa as the example; however, many technology companies have comparable assistants and AI services.

[7] *See What Is Home Automation and How Does it Work?*, SAFEWISE, https://www.safewise.com/home-security-faq/how-does-home-automation-work/ [https://perma.cc/E52B-8EBH] ("Home automation . . . describes homes in which nearly everything — lights, appliances, electrical outlets, heating and cooling systems — are hooked up to a remotely controllable network.").

[8] Amazon's voice recognition technology has a larger database of household voice commands than its competitors. The larger data set allows for better machine learning. *See* Tom Simonite, *Alexa Gives Amazon a Powerful Data Advantage*, MIT TECH. REV. (Jan. 18, 2017), https://www.technologyreview.com/s/603380/alexa-gives-amazon-a-powerful-data-advantage/ [https://perma.cc/RYV7-QZ38] ("The data Amazon is amassing" helps Alexa's machine learning train outside the "standard datasets available for training and testing speech recognition systems" which "don't usually include audio captured in home environments, or using microphone arrays like that the Echo uses to focus on speech from a particular direction.").

[9] *See, e.g.*, *The Ally Skill for Amazon Alexa*, ALLY, https://www.ally.com/bank/online-banking/how-to-bank-with-ally/alexa/ [https://perma.cc/DSG6-56MH] (explaining how customers can link Alexa to their bank accounts to manage their balances); *Add and Edit Your Contacts to the Alexa App*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202136200 [https://perma.cc/E5KK-LZJ7] (provides instructions for how to add personal contacts to Alexa); *Link a Third-Party Music Service to Alexa*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201628770 [https://perma.cc/GE7U-DMDD] (provides instructions for how to link music streaming services to Alexa).

command, and Alexa can undertake quite a laundry list of tasks:[10] "Alexa, purchase a bottle of shampoo on Amazon, and have it shipped to the house"; "Alexa, pay my electric bill"; "Alexa, play a live version of Stairway to Heaven"; "Alexa, turn on the air conditioning"; "Alexa, call grandma." Your wish is Alexa's command. Each one of these commands and corresponding action undertaken by Alexa, is known as a "skill."[11] Alexa can even learn new "skills," which allow vendors and service providers to integrate their products with Amazon and the Echo.[12] Indeed, by 2017, 12,000 products had Alexa "skills" allowing Alexa integration.[13] Amazon introduced the Echo in 2014 solely as a smart speaker, "promising a way to control your music with your voice and little else."[14] What pushes the Echo to the forefront of the "tech arms race" is the accessibility of Echo's code, which is "open" to developers:[15]

> Amazon "made the decision very early on to make it open," says George Yianni, head of technology for Home Systems at Philips Lighting. That openness made it easy for Philips

[10] *See* Recombu, *How to Setup and Use Alexa*, YOUTUBE (Dec. 20, 2018), https://www.youtube.com/watch?v=q3LIghHhoxE [https://perma.cc/F9NQ-JY4M].

[11] *See* Julia Tell, *What are Amazon Alexa Skills?*, GEARBRAIN (Aug. 24, 2017), https://www.gearbrain.com/what-are-amazon-alexa-skills-2471456002.html [https://perma.cc/26XM-MTWA].

[12] *See id.*

[13] *See* Matt Weinberger, *How Amazon's Echo Went from a Smart Speaker to the Center of Your Home*, BUS. INSIDER (May 23, 2017, 6:08 PM), https://www.businessinsider.com/amazon-echo-and-alexa-history-from-speaker-to-smart-home-hub-2017-5 [https://perma.cc/NWM8-X6CB].

[14] *Id.*

[15] *See* Alexa Developers, *Alexa Skill Blueprints – Publish Your Skill to the Alexa Skills Store*, YOUTUBE (Feb. 13, 2019), https://www.youtube.com/watch?time_continue=1&v=UUHggqB5t3s [https://perma.cc/59VG-AL9J].

> to get started integrating Alexa with their Hue smart light bulbs, without needing to totally replace the app and control systems it had already built. That's something the thermostat manufacturer Ecobee agrees with. "The fact that [Alexa is] open to developers ensures that it will continue to gain functionality over time," says Ecobee Stuart Lombard. While Yianni didn't name names, he noted that other platforms were "slower to make them open" – Google and Microsoft only opened up their respective platforms beyond just a select few partners within the last few months.[16]

The ease with which developers can integrate their products into the Amazon ecosystem further enhances the Echo's quality because each device gives Amazon more data-fodder for its machine learning algorithms associated with Alexa—the more data available for the AI, the smarter it gets.[17] So, it gathers that data across all the compatible devices, as well as the commands given by the user, and transmits them to Amazon to feed its AI.[18]

[3] It is not readily apparent from the sleek black cylindrical pillar and blue ring of light, that Alexa is recording your voice and committing those audio clips to its memory banks, all while gathering data about your purchases, commands, among other things. The purpose of Amazon's constant data gathering is to generally improve its products for its customers, and also to allow Alexa to adjust to your needs.[19] The

[16] Weinberger, *supra* note 13.

[17] *See* Ruhi Sarikaya, *The Role of Context in Redefining Human-Computer Interaction*, AMAZON: ALEXA DEVELOPER BLOG (Dec. 12, 2018), https://developer.amazon.com/blogs/alexa/post/3ac41587-f262-4fec-be60-2df2f64b9af9/the-role-of-context-in-redefining-human-computer-interaction [https://perma.cc/YHK4-XUJ3].

[18] *See id.*

"machine learning" element of Alexa makes "her" extraordinarily convenient: she learns your habits, routines, and preferences, reintegrates the data she gathered into her knowledge base, and employs the data to further improve her efficiency, tailored specifically for you.[20]

[4] Amazon claims that Alexa does not record unless it is activated by saying "Alexa."[21] At that point, Alexa "actively" listens—recording the phrases uttered by the user.[22] Skeptics in the tech community claim that Alexa "passively" listens at all times.[23] In other words, she may not record what you say, but she must be listening to "hear" her name called before the user gives her a command, even when she is not "activated."[24]

---

[19] *See id.* Amazon's information-gathering and security practices relate to different and important concerns for national security that are not the subject of this analysis. But "big data" collection and privacy issues are yet another facet of the problem facing the growing incorporation of technology in daily life. *See* Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, BUS. L. TODAY 1, 1 (July 2017), https://www.americanbar.org/content/dam/aba/publications/blt/2017/07/full-issue-201707.pdf [https://perma.cc/B6UL-ZCDA]. Numerous issues arise from data security, information privacy, the antagonism between national security concerns and constitutional rights. *See id.* Those issues therefore require their own separate analyses.

[20] *See* Sarikaya, *supra* note 17.

[21] *See* Sapna Maheshwari, *Hey, Alexa, What Can You Hear? And What Will You Do With It?*, N.Y. TIMES (Mar. 31, 2018), https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html [https://perma.cc/MRX6-43K3].

[22] *See id.*

[23] *See* Geoffrey A. Fowler, *Hey Alexa, Come Clean About How Much You're Really Recording Us*, WASH. POST: THE SWITCH (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/ [https://perma.cc/L84J-9KVU].

[24] *See id.*

[5] While the Echo transmits data to Amazon, it actually stores vast amounts of data and information about its users on its own hard drive.[25] In terms of national security, Alexa's access to users' contacts, bank accounts, daily routines, etc., poses an enormous security risk. The information stored by Alexa is a veritable treasure trove for a foreign government seeking information on a specific person. Foreign agents could extract user data, including voice recordings, and bank account information; manipulate the environment of a target's home; or even surreptitiously record audio or video.[26] Beyond merely gathering information from Alexa, a foreign agent could theoretically act through Alexa, posing as the user, to make purchases, transfer money, open door locks, start cars, or record and transmit video.

[6] For foreign agents to engage in focused surveillance, information theft, or manipulation of regular citizens seems to be a low-risk issue.[27] However, the national security risk posed by Alexa increases dramatically for United States government officials, employees, members of the military or contractors with access to classified national security information, simply because their clearance gives them access to sensitive national security information,[28] which makes them a more likely target than the average American.

---

[25] *See* Yves Smith, *Why You Should Never Buy an Amazon Echo or Even Get Near One*, NAKED CAPITALISM (Nov. 9, 2017), https://www.nakedcapitalism.com/2017/11/why-you-should-never-buy-an-amazon-echo-or-even-get-near-one.html [https://perma.cc/VM6Z-Q64V]. "Data" refers to raw bits of information, facts, or figures that are not necessarily contextualized. "Information," more broadly, refers to how particular data points fit with other pieces of data, thus providing a greater context for the data.

[26] *See id.* Other bad actors like cybercriminals or cyberterrorists may also be able to exploit the vulnerabilities highlighted in this analysis, but they are not the instant focus.

[27] *See* Interview with Retired CIA General Counsel, Central Intelligence Agency, (Name Withheld) (Nov. 19, 2018) [hereinafter "CIA GC Interview"].

[28] *See id.*

[7] Indeed, the security clearance process,[29] as well as the continuous evaluation process,[30] aims to identify and evaluate foreign influences and other national security risks existing at that moment relating to those persons with access to secrets.[31] The information identified in the clearance process, such as connections to foreign governments, ties abroad, and/or exploitable private life problems like gambling, financial, and relationship issues, etc., are major concerns to security clearance evaluators.[32] Why, then, does the government not seriously consider that Alexa is the unwitting foreign agent that can gather such vast amounts of data and information about a person, or even devastate a person's reputation or career through its "skills?" What about Alexa's contribution to a foreign agent finding a person's weaknesses and vulnerabilities, then using that information or the skills to *create* additional weaknesses and vulnerabilities?

[8] The discussion about Alexa is tied closely to private home network security because Alexa connects to devices through a home Wi-Fi network.[33] This analysis uses Alexa as an exemplar of the value of data transmitted through and stored on private home networks to foreign intelligence agents ["FIAs"].

---

[29] *See* LEVERAGING EMERGING TECHNOLOGIES IN THE SECURITY CLEARANCE PROCESS, INTELLIGENCE AND NAT'L SECURITY ALLIANCE 13 (2014), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_LevergingEmergingTech_WP.pdf [https://perma.cc/L6FT-N7JE].

[30] *See id.* at 2.

[31] *See* Interview with Perry Russell-Hunter, Dep't of Defense Office of Hearings and Appeals (Nov. 28, 2018), [hereinafter "Russell-Hunter Interview"].

[32] *See id.*

[33] *See* Kate O'Flaherty, *How To Secure The Amazon Echo*, FORBES (May 25, 2018, 2:26 PM), https://www.forbes.com/sites/kateoflahertyuk/2018/05/25/amazon-alexa-security-how-secure-are-voice-assistants-and-how-can-you-protect-yourself/#177933bc3734 [https://perma.cc/XU7K-G4EV].

[9] The concern for unsecure private networks earned recent media attention because of the home network practices of high-level politicians,[34] demonstrating that private home network security poses a problem for individuals at every level of government. An anemic or weak private home network makes FIAs' access to a person's data and information much simpler,[35] which makes the individual more vulnerable to influence or manipulation.

[10] FIAs can use Alexa to achieve their operational goals, thus affecting United States national security.[36] Those foreign intelligence goals can be ranked from most significant to least significant, as follows:

> 1) the use of Alexa to add chaos or stress in a target person's life, in one of two ways:
>
> a) putting a person in a position of weakness to facilitate recruitment;[37] or

[34] For a discussion on American politicians using home networks for government business, *see Private Email Scandal: Ivanka Trump 'Didn't Know' She Had to Use Secure White House Account*, NEWS CORP. AUSTRALIA NETWORK, (Nov. 20, 2018, 1:20 PM), https://www.news.com.au/finance/economy/world-economy/private-email-scandal-ivanka-trump-didnt-know-she-had-to-use-secure-white-house-account/news-story/dd2128f3d3ab990fdfbee592c67de1bf [https://perma.cc/7TUT-DKHA]; *see also* Z. Byron Wolf, *6 Similarities Between Ivanka Trump and Hillary Clinton's Email Excuses*, CNN POLITICS, (Nov. 20, 2018, 1:26 PM), https://www.cnn.com/2018/11/20/politics/ivanka-trump-hillary-clinton-email-explanations/index.html [https://perma.cc/84EY-FC9Z].

[35] *See* Eric Geier, *5 Ways to Secure Wi-Fi Networks*, NETWORK WORLD, (Sept. 18, 2017, 3:00 PM), https://www.networkworld.com/article/3224539/5-ways-to-secure-wi-fi-networks.html [https://perma.cc/8E36-DPHB].

[36] *See* Andy Greenberg, *A Hacker Turned an Amazon Echo Into a 'Wiretap'*, WIRED, (Aug. 1, 2017, 3:30 PM), https://www.wired.com/story/amazon-echo-wiretap-hack/ [https://perma.cc/CZL4-92AX].

[37] *See* Garrett M. Graff, *China's 5 Steps for Recruiting Spies,* WIRED, (Oct. 31, 2018, 7:00 AM), https://www.wired.com/story/china-spy-recruitment-us/ [https://perma.cc/EGL8-AQBS].

b) threatening to injure, or injuring a person or that person's reputation, in order to influence their role in the bureaucracy or policy-making;[38]

2) the use of data and information collected by Alexa to build a dossier about a person with the aim of recruiting them as a spy or agent through manipulation or relationship building;[39]

3) using Alexa to build a profile about a person with the purpose of finding a weakness, in order to use the person as a "trojan horse" or unwitting servant of a foreign agent.[40]

[11] In order to address how and why the above threats constitute true national security concerns, this discussion will progress in the following manner. First, this paper will address the properties, conveniences, and capabilities of Alexa and the Echo. Secondly, it will discuss ways of attacking the Echo to hijack its capabilities or hack its information. Next, the paper will survey intelligence gathering techniques and strategies. Then, it will review how the adjudicative and investigative components of the security clearance process fail at dealing with Alexa and private home connectivity. Following the review of security clearance adjudication and investigation, the discussion will turn to "Alexa Gone Wrong": how Alexa can be used to achieve the operational goals of a FIA, using known CIA tactics and strategies as a model. Finally, this paper will propose and evaluate several solutions and their limitations, in the framework of security clearance guidelines, for neutralizing the threat of FIAs attempting to use Alexa.

[38] *See id.*

[39] *See* Zachary Cohen, *FBI Documents Detail How the Russians Try to Recruit Spies*, CNN (Jul. 6, 2017, 8:24 AM) https://www.cnn.com/2017/04/15/politics/russia-spy-recruitment-tactics-fbi-carter-page/index.html [https://perma.cc/PT6R-SW4A].

[40] *See id.*

[12] In sum, the national security threat of Alexa must be addressed, specifically for persons with access to sensitive or classified information. This paper proposes three possible solutions: (1) implementing mandatory education for clearance seekers and holders about cybersecurity, focusing on management of IoT devices and home assistants, and how to use "best practices" for managing personal devices and data;[41] (2) requiring a clearance seeker or holder to disable all AI functions on IoT devices in his/her home and certify his/her compliance with that requirement;[42] and (3) adding a "Guideline N" subcategory to the adjudication and investigative processes that addresses private, personal devices and information management practices, which requires disclosure of devices and proposes a mitigation strategy to merge with current background investigation protocols.[43]

[13] While each of the above proposals have limitations, the urgent need for a solution to the threat increases and must be confronted before FIAs begin exploiting the vulnerabilities inherent in Alexa and other home assistants.

II. THE PROPERTIES, CONVENIENCES, AND CAPABILITIES OF ALEXA

What IS *Alexa?*

[14] Alexa is a consumer facing AI created and sold by Amazon.[44] For years, literature has speculated about the philosophical conundrums of AI

[41] *See infra* para. 87..

[42] *See infra* para. 90.

[43] *See infra* para. 94.

[44] *See All Things Alexa*, AMAZON, https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011 [https://perma.cc/2K7L-YB43]; Sean Keach, *What is Alexa? Here's the Ultimate Guide to the Amazon Echo Smart Speakers*, THE SUN

in movies like *Her*, *The Matrix* and *The Terminator*, and books like *Do Androids Dream of Electric Sheep* and *Hyperion*.[45] While the technology surrounding AI on a broad scale continues to evolve, private companies like Amazon make the abilities of AI available to consumers: by and large, AI has provided us with an amazingly beneficial tool that learns algorithms from our digital devices and extracts patterns from data to influence what we buy.[46] Alexa, which refers to the "name" of the AI that lives in the Echo,[47] Amazon's cylindrical black smart speaker, exemplifies the consumer oriented AI.

[15] Notwithstanding the sci-fi novel hype surrounding the evils of AI, the world has embraced AI, inviting programs like Alexa into the home. Over eight million people use Alexa, and the Echo enjoys seventy-three percent market share for smart speakers.[48] Over five million Echo devices are estimated to have been sold since Echo's launch.[49] The Echo was the first mainstream home assistant to be "open," in other words, for its source code to be accessible to developers to encourage integration by products

(Dec. 25, 2018), https://www.thesun.co.uk/tech/5756605/alexa-explained-amazon-echo-smart-speaker/ [https://perma.cc/SAW3-HNWQ].

[45] *See* HER (Annapurna Pictures 2013); THE MATRIX (Warner Bros. Village Roadshow Pictures 1999); THE TERMINATOR (Hemdale Film Corporation & Valhalla Entertainment 1984); PHILIP K. DICK, DO ANDROIDS DREAM OF ELECTRIC SHEEP? (1968); DAN SIMMONS, HYPERION (1989).

[46] *See* Niraj Dawar, *Marketing in the Age of Alexa*, HARV. BUS. REV. (May–June 2018), https://hbr.org/2018/05/marketing-in-the-age-of-alexa [https://perma.cc/W3QS-ZFFL].

[47] *See All Things Alexa*, *supra* note 44; *see also* Kim Wetzel, *What is Alexa, and What Can Amazon's Virtual Assistant Do for You?*, DIGITAL TRENDS (Feb. 16, 2019 7:25 AM PST), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/ [https://perma.cc/K7LH-497B].

[48] *See* Craig Smith, *17 Amazing Amazon Alexa Statistics and Facts*, DMR BUS. STAT., FUN GADGETS, (Jan. 26, 2019), https://expandedramblings.com/index.php/amazon-alexa-statistics/ [https://perma.cc/9U3A-D7VX].

[49] *See* Simonite, *supra* note 8.

and services not officially partnered with Amazon.[50] The user logs into the Alexa application ("app") to activate and link the Echo to "skills" and devices.[51] Once the user logs into the devices or programs with related "skills," the user can, from then on, access those "skills" without specifically logging into those devices or programs.[52]

Alexa's Capabilities

[16] The capabilities of Alexa allow the user to control his/her life through a smartphone, or more importantly, with his/her voice.[53] A person's voice is, in many ways, a unique signature—in terms of communication with the Echo—a person's voice allows the Alexa to identify the user, unlocking access to specific skills or tasks.[54] When Alexa identifies the user, Alexa can use the settings associated with that user that it has learned and specifically tailored to that person's interests.[55]

[50] *See What Is Open Source?*, OPEN SOURCE, https://opensource.com/resources/what-open-source [https://perma.cc/A24U-C2VN].

[51] *See Enable Alexa Skills*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201848700 [https://perma.cc/5THN-6GEZ].

[52] *See Understand Account Linking*, AMAZON DEVELOPER, https://developer.amazon.com/docs/account-linking/understand-account-linking.html [https://perma.cc/D36H-PX7J].

[53] *See* Craig Lloyd, *How to Control Your Amazon Echo from Anywhere Using Your Phone*, HOW-TO GEEK, (Mar. 9, 2019, 11:34 AM), https://www.howtogeek.com/253621/how-to-control-your-amazon-echo-from-anywhere/ [https://perma.cc/N883-TUTN].

[54] Currently, it is unclear if Alexa can distinguish between voices sufficiently enough for the user's voice to be the unique key to using the Echo.

[55] *See* Luu Chang & Kim Wetzel, *Alexa Will Automatically Boot Up Personal App Preferences Based on Your Voice*, DIGITAL TRENDS (May 18, 2018, 12:31 PM PST), https://www.digitaltrends.com/home/amazon-alexa-2/ [https://perma.cc/C9Y7-H7QN].

Indeed, Alexa actually listens, learns about the user's voice, and reintegrates that newly learned data:

> For the software to learn, it must adapt to your style. Alexa is designed to figure out your particular style of speaking. Some people mumble, and others have thick accents. Gradually, Echo's technology takes this into account and gets better at understanding you.[56]

[17] Beyond merely learning the user's voice, Alexa seamlessly connects via Wi-Fi to numerous IoT devices through its various skills, including, *inter alia*: thermostats; video recording systems; landline phones; streaming video services; light switches; cars made by Ford, BMW, and MINI; outlets, doorknobs, and locks; doorbell videos; and GPS wearables.[57] Additionally, Alexa may integrate many services like Google Calendar, music streaming services, and online travel booking sites.[58] Various voice commands allow the user to control the interconnected web of devices or use services.[59] Some notable commands include "Alexa, show my calendar"; "Alexa, show the living room camera"; "Alexa, set a repeating alarm for weekdays at 7 a.m."; "Alexa, call [name]"; "Alexa, add garbage bags to my cart"; "Alexa, lock my back door"; and "Alexa, discover my devices."[60] Indeed, "the list of commands is expanding

[56] Kim Komando, *How to Listen to What Amazon Echo Has Ever Recorded You Saying*, KOMANDO, (May 27, 2018), https://www.komando.com/columns/397201/how-to-listen-to-what-amazon-echo-has-ever-recorded-you-saying [https://perma.cc/QJ23-SD3H].

[57] *See* Samantha Gordon & Daniel Wroclawski, *Everything that Works with Amazon Echo and Alexa*, REVIEWED (June 3, 2018), https://www.reviewed.com/smarthome/features/everything-that-works-with-amazon-echo-alexa [https://perma.cc/2AGY-TMZF].

[58] *See id.*

[59] *See id.*

[60] *See* Taylor Martin, Tauren Dyson & David Priest, *The Complete List of Alexa Commands So Far*, CNET (Jan. 23, 2019 12:45 PM PST), https://www.cnet.com/how-

rapidly, as is the number of third-party services and devices" supported by Alexa.[61] "Third party" in this context refers to other products and services outside of Amazon that link with Alexa, like Spotify or Capital One.[62] To conveniently use these services, a user's Alexa account and third-party accounts must somehow be connected,[63] as Amazon discusses on its site aimed at third-party skill developers:

> Some skills require the ability to connect the identity of an Alexa end user with a user in another system, such as Twitter, Facebook, Amazon, and many others. For example, suppose you own a web-based service "Car-Fu" that lets users order taxis. It would be very convenient for people to access Car-Fu by voice ("Alexa, ask Car-Fu to order a taxi"). To accomplish that, you'd use a process called account linking, which provides a secure way for Alexa skills to connect with third-party systems requiring authentication… There are many ways you can use account linking to enhance your Alexa skill. For example: you can map this user profile to an existing user in your user database.[64]

---

to/amazon-echo-the-complete-list-of-alexa-commands/ [https://perma.cc/CQ2L-URNG?type=image].

[61] *See id.*

[62] *See* Eric Zeman, *Amazon Alexa Can Now Pay Capital One Bills*, INFORMATIONWEEK (Mar. 11, 2016, 2:06 PM), https://www.informationweek.com/it-life/amazon-alexa-can-now-pay-capital-one-bills/a/d-id/1324660 [https://perma.cc/PDY8-3G9T].

[63] *See generally* Sebastien Stormacq, *Alexa Account Linking: 5 Steps to Seamlessly Link Your Alexa Skill to User Systems that Require Authentication,* AMAZON DEVELOPER (Aug. 3, 2016), https://developer.amazon.com/blogs/post/Tx3CX1ETRZZ2NPC/Alexa-Account-Linking-5-Steps-to-Seamlessly-Link-Your-Alexa-Skill-with-Login-wit [https://perma.cc/W6A8-VHTN] (describing the process of account linking).

[64] *See id.*

[18] Third-party skills requiring a login or some kind of authorization are connected to Alexa through "account linking," which essentially uses code to coordinate login authorizations between products and services.[65] Once the Alexa user logs authorizes and logs into a third-party product or service the first time through its correspondent Alexa skill, the user need not log in manually again, and can make use of the service or product through its Alexa skill.[66] In other words, subsequent to the first use of the skill, the user need not log in again and can activate the skill with his/her voice alone.[67]

[19] Most notably, some skills allow a user to ask Alexa about past credit card transactions, schedule payments including for rent,[68] as well as check his/her balance, pay auto loans, and track his/her spending.[69] According to Capital One bank's terms of service for its Alexa skill:

> The Skill allows you to use your Alexa-enabled device to communicate with Capital One, by voice, regarding your Account(s). Your voice is only used to activate Alexa's

[65] *See Understand Account Linking*, *supra* note 52.

[66] *See* Oyetoke Tobi Emmanuel, *You Can Now Use Any Alexa Skill Without Enabling It*, MEDIUM (Apr. 6, 2017), https://medium.com/@oyetoketoby80/you-can-now-use-any-alexa-skill-without-enabling-it-c29320f152de [https://perma.cc/8273-B5VS].

[67] There are some security features that may be enabled by the user. For instance, a user may disable "purchase by voice," or toggle "voice code," which requires a 4-digit confirmation code before completing purchases. *See Manage Voice Purchasing Settings*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201952610 [https://perma.cc/WXN9-7L9L].

[68] *See Speaking of Alexa As the Personal Billing Assistant*, PYMNTS (Mar. 28, 2018), https://www.pymnts.com/alexa-voice-challenge/2018/amazon-alexa-bill-pay-voice-banking/ [https://perma.cc/V4F2-FGLK].

[69] *See Alexa, Ask Capital One, What's My Balance?*, CAPITAL ONE, https://www.capitalone.com/applications/alexa/ [https://perma.cc/L3E7-X8MQ].

> features and is not used to authenticate the account. To use the Skill, you will have to speak commands and questions aloud to Amazon's Alexa service ("Alexa"), and you will receive responses aloud. Any communication to Capital One via Alexa will be treated by Capital One as a communication authorized by you, and any communication from Capital One via Alexa in response to a request received from your Alexa-enabled device will be treated by Capital One as a communication to you. In other words, you are responsible for all of the interactions with Capital One via the Skill …. Once you set up your Alexa device with the Skill, you are authorizing Capital One to provide information to the device based on the device's security settings. For example, the settings on your device may allow the device to retrieve information about your Account(s) based on only verbal requests from anyone who uses your device, or to save information about your Account(s) for easier access.[70]

Regarding the ability to make payments through Alexa and the Capital One skill, the terms of service state: "By using the Skill on your Alexa-enabled device, you authorize Capital One to initiate payments in amounts up to the greater of your credit limit of your credit card Account or your balance."[71]

[20] The "drop-in" function is a new skill enabled on the version of the Echo with a video camera.[72] It allows the user to approve certain contacts

[70] *Terms & Conditions*, CAPITAL ONE, https://www.capitalone.com/applications/alexa/terms/ [https://perma.cc/RP4Z-ANBE].

[71] *Id.*

[72] *See* Taylor Martin, *How to Use Alexa as an Intercom*, CNET (May 6, 2018, 4:55 PM PDT), https://www.cnet.com/how-to/how-to-use-alexa-drop-in-intercom/ [https://perma.cc/7JMJ-5Y9M?type=image].

who also have Echo devices and to use the Echo as a video intercom.[73] So long as the function is enabled, and a particular contact is approved, that contact may "drop-in," or activate a video connection between his/her Echo and the user's Echo, without actually calling the user or requiring the user to even accept the connection.[74] That contact can simply show-up on the screen of the user's Echo.[75]

How Does Alexa Use Data?

[21] The question of how Alexa gathers, stores, and/or transmits data concerns users and scholars alike.[76] Whether data collected by Alexa should be protected differently than other types of data collected by third parties[77] or to what degree information gathered by Alexa is entitled to Fourth Amendment protections, are serious questions, but are not the subject of this analysis.[78] There is no doubt, however, that Alexa gathers

[73] *See id.*

[74] *See Amazon Echo 'Drop In' Feature Prompts Fears of Easy Eavesdropping*, KPIX (Jan. 5, 2018, 11:31 PM), https://sanfrancisco.cbslocal.com/2018/01/05/amazon-echo-drop-in-feature-prompts-fears-of-easy-eavesdropping/ [https://perma.cc/DY5G-HY22].

[75] *See id.*

[76] *See, e.g.*, Maheshwari, *supra* note 21 (describes how many consumers are becoming increasingly nervous about Alexa's data collecting).

[77] *See, e.g.*, Christopher Burkett, *I Call Alexa to the Stand: The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology*, 20 VAND. J. ENT. & TECH. L. 1181, 1204–06 (2018) (discussing how courts should apply third party doctrine to smart-home technology).

[78] *See* Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924–27, 1937, 1945 (2017). *See generally* Nicole Chavez, *Arkansas Judge Drops Murder Charge in Amazon Echo Case*, CNN (Dec. 2, 2017, 12:52 AM), https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html [https://perma.cc/A9M8-M8DP] (discussing a dismissed murder charge involving evidence that was stored in an Amazon Echo speaker).

substantial data about its user, and transmits much of it to Amazon.[79] How it gathers its data comes mostly from the voice commands:

> Is Amazon Echo always listening? The short answer is yes. Alexa is activated when it detects one of its wake words, which are "Alexa," "Amazon," "Computer," or "Echo." You'll know that the device is ready for a command when the outer ring at the top glows blue. According to Amazon, a fraction of a second of audio before the wake word is stored along with each recording. So if you're having a conversation and say something like, "I love that song! Let's listen to it. Alexa, play the Coldplay song, 'Viva La Vida,' " then Alexa may keep the words "listen to it."[80]

Although Alexa may not record or store everything within its "earshot," it follows logically that in order to "hear" the wake word, Alexa must be listening, perhaps passively. That is, Alexa may not be recording the speech, but she still processes it.[81] Recent reports suggest that, while Alexa may not *record* what people say, Amazon employees are listening nevertheless: "Amazon reportedly employs thousands of full-time workers and contractors in several countries, including the United States, Costa

[79] *See, e.g.*, Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 15, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ [https://perma.cc/VB9G-NNAS] (explaining how Alexa gathers user data).

[80] *See* Komando, *supra* note 56.

[81] *See, e.g.*, Eugene Kim, *Amazon Echo Secretly Recorded a Family's Conversation and Sent It to a Random Person on Their Contact List*, CNBC (May 25, 2018, 7:58 AM), https://www.cnbc.com/2018/05/24/amazon-echo-recorded-conversation-sent-to-random-person-report.html [https://perma.cc/TA98-KYVX] (describing how Alexa records and listens private conversations without being activated).

Rica and Romania, to listen to as many as 1,000 audio clips in shifts that last up to nine hours."[82]

III. METHODS FOR INFILTRATING OR HIJACKING ALEXA AND THE ECHO

[22] This section will address two ways unintended users can access Alexa's stored data or use her capabilities linked to the intended user: "infiltration," that is, accessing the Echo device and its content (akin to "hacking") and "hijacking," fooling Alexa into believing its user is giving it commands. Hacking Alexa offers more information and data (i.e. voice recordings, potential video, account data, etc.), and it may be relatively easy to do.[83] In contrast, despite the ease with which a seasoned hacker could infiltrate a person's home network, hijacking Alexa to use her skills or undertake tasks requires little more than a voice command.[84]

[23] According to former National Security Agency ["NSA"] employee turned consultant, Jacob Williams, digitally infiltrating or hacking Alexa is feasible.[85] However, Williams claims the chances of it happening are

[82] Jordan Valinsky, *Amazon Reportedly Employs Thousands of People to Listen to Your Alexa Conversations*, CNN BUSINESS (Apr. 11, 2019), https://edition.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html [https://perma.cc/7SPM-ZTM8]

[83] *See* Mark Ward, *How Easy Is It to Hack a Home Network?*, BBC (Feb. 25, 2016), https://www.bbc.com/news/technology-35629890 [https://perma.cc/3Y2G-2L4Q].

[84] *See, e.g.*, Craig S. Smith, *Alexa and Siri Can Hear This Hidden Command. You Can't.*, N.Y. TIMES (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html [https://perma.cc/FXL9-95BM]; *see also* Ward, *supra* note 83 (discussing the ease of hacking home networks).

[85] *See* Ail Montag, *Former NSA Privacy Expert: Here's How Likely That it is That Your Amazon Echo Will be Hacked*, CNBC (Sept. 4, 2018, 12:07 PM), https://www.cnbc.com/2018/09/04/ex-nsa-privacy-expert-how-likely-your-amazon-echo-is-to-be-hacked [https://perma.cc/3FRB-XQ8L].

slim simply because the "level of effort to do it is too high in the vast majority of cases" and "[y]our average American just isn't that interesting."[86] But, "they[] make phenomenal listening devices if you can exploit them."[87]

[24] While it may not be a simple task, Chinese hacker-researchers turned an Alexa into a remote listening device: they could "control Amazon Echo for eavesdropping and send the voice data through the network to the attacker."[88] Their serious hardware and software manipulation highlights some potential security risks posed by Alexa's penchant for connectivity:

> They start by taking apart an Echo of their own, removing its flash chip, writing their own firmware to it, and re-soldering the chip back to the Echo's motherboard. That altered Echo will serve as a tool for attacking *other* Echoes: using a series of web vulnerabilities in the Alexa interface on Amazon.com … all since fixed by Amazon – they say that they could link their hacked Echo with a target user's Amazon account […] If they can then get that doctored Echo onto the same Wi-Fi network as a target device, the hackers can take advantage of a software component of Amazon's speakers … that the devices use to communicate with other Echoes in the same network. That [component] contained a vulnerability that the hackers found they could exploit via their hacked Echo to gain full control over the target speaker, including the ability to make the Echo play

[86] *Id.*

[87] Andy Greenberg, *Hackers Found A (Not-So-Easy) Way to Make the Amazon Echo a Spy Bug*, WIRE (Aug. 12, 2018, 3:00 PM), https://www.wired.com/story/hackers-turn-amazon-echo-into-spy-bug/ [https://perma.cc/C3SP-EYMP].

[88] *See id.*

> any sound they chose, or more worryingly, silently record and transmit audio to a faraway spy.[89]

[25] Infiltrating, or "hacking" Alexa remotely, may not always be a simple task, considering the constantly improving digital security patches and updates provided by Amazon.[90] Indeed, Amazon continues to increase the security requirements for developers creating Alexa skills.[91] However, hackers will inevitably continue to adapt to new security measures and engineer means to circumvent them.

[26] To infiltrate Alexa remotely, a FIA would need access to the person's network, and short of physical intrusion or learning the Wi-Fi password, such intrusion may be difficult[92] but not impossible.[93] Mirai botnet, the largest malware-based hijacking of IoT devices in history, would suggest that such intrusion is feasible.[94] If a FIA were to gain access to a person's network, they would have access to numerous devices with information and data, like computers and tablets.[95] Access to a

[89] *Id*. (explaining further that the "requirement that the victim and the attacker be on the same Wi-Fi network represents a serious limitation to the attack").

[90] *See, e.g.*, *Alexa Device Software Updates*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602210 [https://perma.cc/HGT8-SZUU].

[91] *See, e.g.*, *Security Best Practices*, AMAZON, https://developer.amazon.com/docs/alexa-voice-service/security-best-practices.html [https://perma.cc/MJZ3-EJHZ] (presenting a technical discussion on security requirements for third party developers).

[92] *See* CIA GC Interview, *supra* note 27.

[93] *See generally* Lily Hay Newman, *The Botnet That Broke the Internet Isn't Going Away*, WIRED (Dec. 9, 2016, 7:00 AM), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/ [https://perma.cc/9HHV-Y3NR] (discussing ways for consumers to protect themselves from intrusion and security breaches).

[94] *See id*.

[95] *See* CIA GC Interview, *supra* note 27.

computer has the potential to give FIAs access to a person's private data, like social security numbers, bank accounts, etc., because of programs like Quicken or Turbo Tax.[96] However, anti-virus software specifically installed on the computer by the user could alert that person to an intrusion into their computer,[97] whereas with Alexa, the user must simply trust that Amazon's security measures are sufficient to repel digital infiltration attempts. So, a cunning FIA might steer away from a computer, and instead focus on Alexa, since she provides a centralized hub, that, if accessed, would have a "treasure trove" of information about a person.[98] Infiltration of Alexa thus represents the maximum benefit to FIAs who exploit a person's home network.

Hijacking Alexa to Act

[27] Doubtless, the threat of hacking Alexa poses a concern. However, a seemingly more obvious and insidious method for misusing Alexa arises from its dependence on the user's voice to receive commands. Fooling Alexa into believing that its main users are speaking enables Alexa to undertake action using her various skills on behalf of those same main users. Consequently, Alexa's most attractive feature, its ability to take voice commands, quickly and easily becomes its most glaring security vulnerability.

[28] Scientists utilized complex tools to trick Apple's AI voice command controls in manner that could be done to Alexa.[99] The

[96] *See id*.

[97] *See* Cynthia Harvey, *Types of Malware and How to Defend Against Them*, ESECURITY PLANET (Apr. 4, 2017), https://www.esecurityplanet.com/malware/malware-types.html [https://perma.cc/3U8E-L45L].

[98] *See generally* Greenberg, *supra* note 87 (explaining how attackers may access Echo devices through Wi-Fi networks and Amazon's security fixes and procedures).

[99] *See* James Vincent, *Inaudible Ultrasound Commands Can Be Used to Secretly Control Siri, Alexa, and Google Now*, THE VERGE (Sep. 7, 2017, 6:30 AM),

"DolphinAttack,"[100] a creative method demonstrated by Chinese researchers, employed sound, inaudible to the human ear, to trick home assistants into thinking a person had activated it with his/her voice and subsequently carried out commands:

> In this work, we design a completely inaudible attack, DolphinAttack… By injecting a sequence of inaudible voice commands, we show a few proof-of-concept attacks, which include activating Siri to initiate a FaceTime call on iPhone, activating Google Now to switch the phone to airplane mode, and even manipulating the navigation system in an Audi automobile.[101]

[29] Similarly, researchers at University of California, Berkeley were able to use a mathematically calculated distortion of sound waves to take an audio clip of a person saying "it was the best of times, it was the worst of times," and turn it into the same person saying "it is a truth universally acknowledged that a single…"[102] The Berkeley researchers claimed that "we are able to turn any audio waveform into any target transcription with one-hundred percent success by only addition a slight distortion…[w]e

https://www.theverge.com/2017/9/7/16265906/ultrasound-hack-siri-alexa-google [https://perma.cc/KRE6-92C6].

[100] *See id*.

[101] Guoming Zhang et al., *DolphinAtack: Inaudible Voice Commands*, ACM CONFERENCE ON COMPUTER COMMUNICATIONS SECURITY (Aug. 31, 2017), https://arxiv.org/abs/1708.09537 [https://perma.cc/E7QX-T4WF]. *See also* Karissa Bell, *Researchers Just Proved Why It's So Scary that Digital Assistants are Always Listening,* MASHABLE (May 10, 2018), https://mashable.com/2018/05/10/hidden-commands-digital-assistants-dolphin-attack/#qnq6LWjtaaqg [https://perma.cc/B5JS-AJZ9].

[102] Nicholas Carlini & David Wagner, *Audio Adversarial Examples: Targeted Attacks on Speech to Text*, U.C. Berkeley 1, 1 (2017), https://nicholas.carlini.com/papers/2018_dls_audioadvex.pdf [https://perma.cc/SZP2-YWCH].

can cause audio to transcribe up to fifty characters per second… cause music to transcribe as arbitrary speech, and hide speech from being transcribed."[103] It follows that these scientists created a system for mimicking a person's voice using virtually any audio clip of comparable length.[104] As applied to Alexa, and assuming they have an audio sample, it is likely that scientists can generate audio clips that mimic a user's voice to access Alexa through voice commands.

[30] Alexa now includes the capability to recognize multiple voices in the household, allowing a user's voice to access separate accounts.[105] Regardless of the number of voices Alexa recognizes, other people besides the account-holding user can issue voice commands to Alexa, and she will carry out the commands.[106] Alexa has not achieved the level of sophistication for user's voice to function as a key, denying access for instance to voices not linked specifically to the account.[107]

[31] The vulnerabilities of voice activated devices like Alexa should not be underestimated. There is no need to hack Alexa if a person can instead fool it into hearing the user's voice. Engineering complex audio attacks

[103] *Id*. at 6.

[104] *See id*. at 1.

[105] *See* Emily Price, *How to Set Up Multiple Voice Profiles on Your Amazon Echo*, LIFEHACKER (Oct. 14, 2017, 3:54 PM), https://lifehacker.com/how-to-set-up-multiple-voice-profiles-on-your-amazon-ec-1819474600 [https://perma.cc/8HSD-PPZD]. *See also Using Household Profiles on Alexa Devices*, AMAZON, https://www.amazon.com/gp/help/customer/display.html/ref=as_at?linkCode=w61&imprToken=uwKhbGNCVLlKxbWwDgrdEg&slotNum=0&ascsubtag=b9da921d4818b168be2159be79cf006fee589866&nodeId=201628040&tag=lifehackeramzn-20 [https://perma.cc/4TCE-BCSQ].

[106] *See About Alexa Voice Profiles,* AMAZON, https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=202199440 [https://perma.cc/TGW4-4MDU].

[107] *See id*.

seems practically difficult, but the reality is much simpler. Assuming the user neglected to toggle enhanced security features like a 4-digit confirmation code for his/her purchases, a similar voice to the user's may be able to cause Alexa to act on that user's behalf.

IV. INTELLIGENCE OPERATIONS: STRATEGIES, TACTICS, AND TECHNIQUES

[32] In order to better understand why Alexa presents an attractive entry point into a person's life from an intelligence operations perspective, this paper will discuss numerous publicly known strategies and tactics employed by the CIA. Two assumptions underlie this section of the analysis. First, if CIA uses a technique, a foreign intelligence service might employ a similar or comparable technique. Second, a person with security clearance has access to sensitive information sought by FIAs, so a clearance seeker likely would not be a target until he/she completes his/her security clearance process.[108] The toolkit for intelligence services is broad, but this analysis will discuss three general categories of operations: recruitment, targeted bureaucratic disruption, and unwitting Trojan horses.[109]

[108] Later, this analysis discusses how the security clearance process can evaluate clearance seekers' home network security and Alexa vulnerabilities, and assumes that it is easier for the government to catch and address potential vulnerabilities before a person earns a security clearance rather than after they earn it. Only when a person has clearance would they, from a practical standpoint, have access to classified information and thus become a target for FIAs.

[109] *See generally* Katherine Herbig, *The Expanding Spectrum of Espionage by Americans, 1947 – 2015*, DEPARTMENT OF DEFENSE (Aug. 2017), http://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-17-10_The_Expanding_Spectrum_of_Espionage_by_Americans_1947_2015.pdf?ver=2018-02-14-073446-943 [https://perma.cc/KP52-XR5R] (providing a comprehensive study on Americans who committed espionage and their motivations for doing so).

General Recruitment Methods Used by Intelligence Services

[33] Many methods of gathering intelligence exist, but recruitment of agents is the quintessential human intelligence ["HumInt"] tool for intelligence services.[110] To successfully conduct recruitment, intelligence services use a three-step process: select, recruit, and manage the relationship.[111] The "selection" process, also known as "spotting," requires the recruiter to have the ability to "spot" or "identif[y]… individuals [who] have the placement and access to provide desired information and well as beginning the process of determining their motivations, vulnerabilities, and suitability."[112] In other words, the selection process requires spotting a target with access to information, exploitable vulnerabilities, and is worth the time and effort to recruit.[113]

[34] Once intelligence agents spot a target, they begin "developing a relationship with the individual to further… explore whether they will be responsive to tasking for intelligence information."[114] Some of the most

[110] *See* Interview with retired Clandestine Service Officer, Central Intelligence Agency (Name Withheld) (Nov. 20, 2018) [hereinafter "CIA Op. Interview"]; CIA GC Interview, *supra* note 27.

[111] *See* Randy Burkett, *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*, STUDIES IN INTELLIGENCE, Mar. 2013, at 7, 8–9.

[112] *Id*. at 13.

[113] *See* CIA GC Interview, *supra* note 27; CIA Op. Interview, *supra* note 110. Finding a suitable target with access and vulnerabilities can be difficult, however, social media platforms like LinkedIn often describe a person's job title or department, providing hints about a person's clearance level. Recently, massive data breaches – like the hack of Equifax for example – exposed the credit history and private data of millions of Americans. For an example of monetary vulnerability, *see also* Catalin Cimpanu, *US Government Releases Post-Mortem Report on Equifax Hack*, ZERO DAY NET (Sept. 7, 2018, 11:17 AM), https://www.zdnet.com/article/us-government-releases-post-mortem-report-on-equifax-hack/ [https://perma.cc/5RLW-NH96] (discussing the Equifax hack).

[114] CIA GC Interview, *supra* note 27.

common exploitable weaknesses and vulnerabilities are money, ideology, coercion (blackmail), and ego.[115]

[35] The target must be worth the effort, so naturally, the intelligence officer must make an assessment, balancing the usefulness, actionability, volume, or frequency of the information sought against the effort or time it would take to recruit.[116] Only if the value of information surpasses the amount of effort or time to recruit will an intelligence agent proceed with recruitment.[117] In other words, they must "put quality first."[118]

[36] To successfully recruit an asset, the intelligence agent must build a profile of a target, evaluate and/or create a weakness or vulnerability, and finally exploit that vulnerability to encourage recruitment.[119] Historically, building a profile involved surveillance, learning a person's habits, motivations, likes and dislikes.[120] Ultimately the intelligence agent's goal is a "serendipitous" meeting with the target in a location that is neutral to the target.[121]

---

[115] *See* Burkett, *supra* note 111, at 12–13.

[116] *See* CIA GC Interview, *supra* note 27. Sources could be anyone ranging from janitors to secretaries, to professionals.

[117] *See id*.

[118] Burkett, *supra* note 111, at 9.

[119] *See id*.

[120] *See id*. at 13.

[121] *See* CIA Op. Interview, *supra* note 110. However, building a profile today presents several novel problems: younger people who grew up with social media and universal connectivity live online, and it thus can be difficult to lure or cajole a person into a social situation where an intelligence agent stages a "chance" meeting. *Id*. Social media offers data and information about a potential target, sometimes publicly accessible, but often it is devoid of much needed context for painting a full picture of a person with nuance and subtlety. *Id*. Thus, social media cannot be relied upon indubitably for intelligence purposes. Vast amounts of raw data without background or context about a target makes

[37] The background information gathered about the target helps shape the relationship between the intelligence agent and that target,[122] beginning with rapport-building:

> The larger lesson is to find ways to connect with potential agents – similarities in background (the case officer and agent are both sons/daughters, husbands/wives, parents, have similar personality traits), shared interests (sports/hobbies), and general out-look (interested in world affairs, background, life-style). Flattery is highly recommended for virtually everyone enjoys being praised and future meetings will come more easily… A case officer creates an ever-deeper relationship through the process – from becoming an "associate" then a "friend" in the assessment phases and then moving to the role of "sounding board" and "confidant" as development moves to recruitment. A case officer's goal should be to have a prospective agent come to believe, hopefully with good reason, that the case officer is one of the few people, perhaps the ONLY person, who truly understands him (emphasis in original).[123]

identifying valuable snippets of information difficult because it is unclear what data is relevant to the goal. *Id*. The task of determining relevance of data or information is much like trying to find a needle, that looks like hay, in a haystack. One of the most significant challenges for the intelligence community, especially when working in foreign territory, is the difficulty generating a false identity. *Id*. With social media, online databases, etc., faking an identity is difficult: the problem used to be getting through the foreign country's customs, but now the problem is getting a ticket with the false identity at Dulles. *Id.* Additionally, foreign intelligence outfits know the identity of each of the people who boards (particularly in that foreign country's territory), and can follow them to their destination and wherever they may go. *Id*. It makes sense that an operation (like hacking) that can be orchestrated remotely could minimize the risk of detection.

[122] *See id*.

[123] *Id*.

Along that vein, when a relationship that appears innocent to the target, develops between the intelligence agent and the target, the intelligence agent begins to exploit the weaknesses.[124] For instance, if a target has financial problems, the intelligence agent can suggest that if the person ever needed financial help, the agent, posing as the target's friend, knows a way to ameliorate the financial strain, thus baiting the target to ask for help.[125]

[38] Another example might be a target with serious health issues. An intelligence agent might use that knowledge to suggest that they have a contact with medical expertise that can access specialty medicine.[126] To gain more leverage, the intelligence agent might discover a way to disrupt the target's medicine supply, creating a deeper weakness, greatly pressuring the target to come to the intelligence agent for aid.[127]

[39] An intelligence agent can also create additional weaknesses by strategically introducing a variable of apparent chaos, maybe starting with an inconvenient or minor interruption to the target's life but potentially rising to the level of wreaking havoc in that target's life.[128] The FIA could cause additional stress or obligations, predicting what the target's weaknesses will be subsequent to the event and then capitalizing on those vulnerabilities.[129] For example, an intelligence agent could cause a car crash with a target or target's family member, causing the target great stress, clouding the target's judgment. All the while, the intelligence agent

[124] *See id*.

[125] *See id*.

[126] *See* CIA Op. Interview, *supra* note 110.

[127] *See id*.

[128] *See id*.

[129] *See id*.

knows the target will be absent from work, tired, or need support, and the intelligence agent will be able to fortuitously offer help when the target needs it, creating leverage over the target.

[40] These tactics and techniques require quality background information and context.[130] An unclear or incomplete profile about a target could undermine the mission goal to "[g]et full information about a potential agent before approaching him e.g. interests, weaknesses, character, religion, politics, nationality,"[131] or mislead the intelligence agent about the target's value.[132] Thus, intelligence agents put a premium on the quality of information gathered about a target, and the ability to obtain such quality information is essential.

Targeted Bureaucratic Disruption

[41] Targeted bureaucratic disruption[133] refers to an intelligence operation in which strategic release or plant of information about a target person, whether true or false, discomposes an institutional, political, governmental or other bureaucracy, with the goal of causing turmoil, chaos, or disunion, for a national security purpose.[134] A real and extreme example of targeted bureaucratic disruption would be the international

[130] *See id*.

[131] Burkett, *supra* note 111, at 9.

[132] See DEP'T OF ARMY, FIELD MANUAL 2-22.3, HUMAN INTELLIGENCE COLLECTOR OPERATIONS 1-7 (Sept. 2006).

[133] This is a form of "doxing." *See e.g.*, Joey Blanch & Wesley Hsu, *An Introduction to Violent Crime on the Internet*, 64 CYBER MISBEHAVIOR 2, 5 (2016).

[134] *See Psychological Operations*, U.S. ARMY, https://www.goarmy.com/careers-and-jobs/special-operations/psyop.html [https://perma.cc/D4Q5-8JBZ] (defining psychological operations, or PSYOPs).

crisis that occurred when FIAs hacked a news outlet in Qatar, and planted a "fake news" story:

> [T]he hacker entered the news agency's system and uploaded a news story filled with fabricated quotes attributed to Qatar's emir… The story cited [the emir] purportedly criticizing Trump and praising Iran – the US's main strategic rival in the region... [and] speaking warmly of Hamas… The fake news story went live on the website at about 12:13am, and had soon become the most popular in the website's history.[135]

Indeed, in the age of social media, even fake stories gain traction and go "viral," reaching millions of people in a short time.[136] If an embarrassing or sensitive video leaked on social media, it could irreparably damage the reputation of a person, cause him/her to be fired, or even have criminal charges brought against him/her.[137] Likewise, threatening to expose negative or damaging information about a person on social media to gain

[135] Peter Salisbury, *The Fake-News Hack that Nearly Started a War this Summer Was Designed for One Man: Donald Trump*, QUARTZ (Oct. 20, 2017), https://qz.com/1107023/the-inside-story-of-the-hack-that-nearly-started-another-middle-east-war/ [https://perma.cc/NG6U-3T5F].

[136] *See* Maria Temming, *How Twitter Bots Get People to Spread Fake News*, SCIENCE NEWS (Nov. 20, 2018, 11:00 AM), https://www.sciencenews.org/article/twitter-bots-fake-news-2016-election [https://perma.cc/7MCY-AVUR].

[137] *See* CIA Op. Interview, *supra* note 110. *See also* Meredith McGraw & Emily Shapiro, *Franken is 'Ashamed' of Tweeden Photo, Says She Didn't Have Any Ability to Consent*, ABC NEWS (Nov. 26, 2017, 4:30 PM), https://abcnews.go.com/Politics/sen-franken-embarassed-groping-claims-rebuild-trust/story?id=51394106&utm_source=AWIN&utm_medium=Affiliate&awc=10844_1543018774_d3014d0ece4b831c753fdad9ca8cacca&catalogId=10051&offerId=53204D&source=IONEMAIL&sourceId=x [https://perma.cc/X5YP-3DJA]. Notably, this story differs from targeted bureaucratic disruption because it was the victim who released the photographs, and she did not intend to release the photos for a disruptive national security purpose, but rather to expose the Senator's misconduct.

leverage over him/her for recruitment is an effective tool for FIAs, even if that negative information is fabricated.[138]

[42] A new technological development called "deep fakes" is essentially an audio or visual lie: fake videos or audio clips that look and sound real but are in actuality false or partially false.[139] Often deep fakes contain enough truth to make them difficult to disprove or even identify.[140] "[Deep-fake technology] leverages machine-learning algorithms to insert faces and voices into video and audio recordings of actual people and enables the creation of realistic impersonations out of digital whole-cloth."[141] Such convincing and realistic false footage could be a means to blackmail or extort a person:

> Deep-fake videos could depict a person destroying property in a drunken rage. They could show people stealing from a store; yelling vile, racist epithets; using drugs; or any manner of antisocial or even embarrassing behavior like sounding incoherent. Depending on the circumstances, timing, and circulation of the fake, the effects could be devastating. It could mean the loss of romantic opportunity,

[138] *See* Nico Hines, *Cambridge Analytica Offered to Blackmail Politicians with Prostitutes*, THE DAILY BEAST (Mar. 19, 2018, 3:18 PM), https://www.thedailybeast.com/ex-trump-consultant-and-cambridge-analytica-ceo-alexander-nix-offered-to-blackmail-politicians-with-prostitutes [https://perma.cc/PP7K-HE2P].

[139] *See* Margaret Rouse, *Deep Fake*, WHATIS.COM (June 2018), https://whatis.techtarget.com/definition/deepfake [https://perma.cc/W6QF-J5AA].

[140] *See* Oscar Schwartz, *You Thought Fake News Was Bad? Deep Fakes are Where the Truth Goes to Die*, THE GUARDIAN (Nov. 12, 2018, 5:00 AM), https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth [https://perma.cc/YX92-ST9H].

[141] Robert Chesney & Danielle K. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALI. L. REV. 4, 19 (forthcoming 2019).

> the support of friends, the denial of a promotion, the cancellation of a business opportunity, and beyond.[142]

The release (or threat of release) of "deep fakes" onto a social media platform, whether audio or video, seems like a rapid and efficacious way of ruining a target's reputation or undermining his/her fitness to work. Any attempt by the target to control the damage would be slow-going compared to how quickly the deep fake disrupted his/her life.[143] So, even the threat to release a deep fake could be used to pressure a person into recruitment, because the effects of instant social media infamy carry extreme consequences for a person's life—both in the private sphere and career domain.[144]

Unwitting Trojan Horses

[43] Intelligence agents can also use unwitting targets to undertake objectives on behalf of those agents.[145] For instance, an intelligence agent could drop a gadget into a target's purse, unbeknownst to her. When she goes to work at a secure government building, she does not know that the gadget transmits location data or signal data back to the intelligence agent. Such a technique provides an advantage to the intelligence agent because he/she need not necessarily meet or communicate with the target, but the

[142] *Id*. at 18.

[143] *See id*. at 19. *See also* John Villasenor, *Artificial Intelligence, Deepfakes, and the Uncertain Future of Truth*, BROOKINGS: TECHTANK (Feb. 14, 2019), https://www.brookings.edu/blog/techtank/2019/02/14/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/ [https://perma.cc/W7PW-U84C].

[144] *See* Chesney & Citron, *supra* note 141, at 18.

[145] *See* Jeffery R. Jones & Ryan Averbeck, *The 3 Types of Insider Threat*, CSO (May 12, 2011, 8:00 AM), https://www.csoonline.com/article/2128501/the-3-types-of-insider-threat.html [https://perma.cc/Q7DQ-5ASS].

target achieves the objective, nevertheless.[146] The drawback to this technique is the lack of control over the operation and the limitations of what a target will actually do.[147] Since the target is acting on behalf of the intelligence agent unwittingly, the target likely has not aligned with the intelligence agent's mission (nor does he/she know the mission),[148] and consequently, orchestrating particular or complex tasks may be difficult. For instance, it seems unlikely that an unwitting Trojan horse of an FIA, who believes him or herself to be a patriot, will insert an unknown thumb drive planted in his/her wallet into a government computer, contrary to her information security training.

[44] The intelligence agent's toolbox is deep, and many techniques and strategies exist for conducting intelligence operations.[149] While some have limitations or drawbacks, they all tend to require gathering information about a target to obtain a complete picture.[150] As will be argued Alexa is the simplest way for an intelligence agent to obtain a full picture about a person, surveil, or even manipulate them.[151]

[146] *See id*.

[147] *Cf. id*. (discussing how the unwitting insider is manipulated into performing a task, the consequences of which they are unaware).

[148] *See id*.

[149] *See generally* Burkett, *supra* note 111 (discussing techniques and strategies that intelligence agents use to recruit and control assets).

[150] *See generally id.*

[151] *See infra* Part VI.

V. THE SECURITY CLEARANCE ADJUDICATION AND INVESTIGATIVE PROCESSES

[45] The reason this analysis focuses on security clearance holders is that, as previously discussed, intelligence agents make sure to spot potential targets because the targets have access to desirable or valuable sensitive information.[152] Clearance holders are potential targets of FIAs because, by virtue of their security clearance, they are deemed by the United States government to be suitable for access to secrets.[153]

[46] The major issue however, is that the current guidelines and adjudicative and investigative processes do not account for, or even expressly consider, the national security threats posed by Alexa or weak private home networks. Public social media posts are examined by investigators, and thus factor into the clearance adjudicative process,[154] but IoT devices, specifically Alexa, do not.[155] The security clearance guidelines exemplify the government's concerns about a person's access to classified information; the guidelines identify those specific traits about people the government believes pose the most significant threats to classified information security.[156] Beyond exemplifying the government's concerns, the gatekeeping function of the clearance process cannot be

[152] *See supra* para 6.

[153] *See All About Security Clearances*, U.S. DEP'T OF STATE, https://www.state.gov/m/ds/clearances/c10978.htm [https://perma.cc/ZB2C-2DPQ].

[154] *See* PEREGRINE RUSSELL-HUNTER, PANEL IV – REVIEWING CURRENT CONTROVERSIES SURROUNDING SECURITY CLEARANCES (Am. Bar Assoc. 28th Rev. of the Field of Nat'l Sec. L. Conf.) (Nov. 1–2, 2018), https://www.c-span.org/video/?453934-3/security-law-conference-security-clearances [https://perma.cc/7CR2-BRZE] [hereinafter "Russell-Hunter Panel"].

[155] *See* CIA GC Interview, *supra* note 27; CIA Op. Interview, *supra* note 110.

[156] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SECURITY EXECUTIVE AGENT DIRECTIVE 4 app. A, at 5-24 (2017) [hereinafter "SEAD 4"].

understated. There is a reason why people with access to secrets require vetting before they actually gain that access.[157] The vetting process paints a picture of suitability (or unsuitability) and highlight national security weaknesses in the candidate.[158] Private home devices like Alexa do not rank high on the government's list of objects that undermine suitability to access classified information.[159] It is possible that the government does understand the risks posed by government employee private home connectivity, but does not know how to actually address the problem.

[47] The government encountered a similar issue in the late 1990's when the NSA implemented an all-out employee ban of "furbies," the cute, alien creature-like toys that purportedly learned from, and responded to their owners, for fear that the toys had recording devices in them.[160] "Because of its ability to repeat what it hears, [NSA] officials were worried that people would take [furbies] home and they'd [sic] start talking" about classified information.[161] One article sardonically stated that "anyone at the NSA coming across a Furby, or a crack team of Furbies infiltrating the building has been asked to contact their Staff Security Office for guidance,"[162] but clearly the author did not understand, from the NSA's perspective, how real the security risk was. NSA maintains a ban on recording devices in its facilities,[163] and if a Furby

[157] *See* CIA GC Interview, *supra* note 27; CIA Op. Interview, *supra* note 110.

[158] *See* 32 C.F.R. § 147.2 (2018).

[159] *See id*.

[160] *See* Lauren Davis, *The NSA Once Banned Furbies as a Threat to National Security*, GIZMODO: IO9 (Feb. 20, 2014 11:40 AM), https://io9.gizmodo.com/the-nsa-once-banned-furbies-as-a-threat-to-national-sec-1526908210 [https://perma.cc/4FU9-A9K9].

[161] *World: Americas Furby Toy or Furby Spy?*, BBC NEWS (Jan. 13, 1999, 10:12 AM), http://news.bbc.co.uk/2/hi/americas/254094.stm [https://perma.cc/P9E6-HGE5].

[162] *Id*.

[163] *See id*.

were a recording device, it could have posed a security risk for classified national security information. NSA's knee-jerk reaction to the Furby demonstrates the difficulty for some agencies balancing classified information security against their employees' private home lives.

[48] The following discussion will address the security clearance process, as well as its benefits and shortcomings, and then show the way Alexa poses a specific and novel danger to national security.

Legal Authority for the Issuance of Security Clearances

[49] In order for a person to have access to classified information, he/she must obtain a security clearance, the process for obtaining such clearance being described in various Executive Orders ["E.O.'s"].[164] That process, known as adjudicative process, is the process by which a candidate for security clearance is evaluated for suitability based on existing facts and circumstances at the time of his/her application.[165] Adjudication is grounded upon a regulatory scheme with mandatory factors to consider when evaluating a candidate,[166] applied to the information collected by security clearance investigators.[167] Ultimately, the adjudicators rely upon the information gathered by investigators to make their recommendations.[168]

[164] *See, e.g.*, Exec. Order No. 10,450, 3 C.F.R. 72 (1953); Exec. Order No. 12,968, 3 C.F.R. 391 (1995); Exec. Order No. 13,467, 3 C.F.R. 196 (2008); Exec. Order 13,549, 3 C.F.R. 234 (2010).

[165] *See* 32 C.F.R. § 147.2 (2018).

[166] *See, e.g.*, *Intelligence Community Directive*, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented information and Other Controlled Access Program Information (Effective Oct. 1, 2008); *see* SEAD 4, *supra* note 156. The intelligence community uses similar guidelines, but they have minor substantive differences.

[167] *See All About Security Clearances*, U.S. DEP'T STATE, https://www.state.gov/m/ds/clearances/c10978.htm [https://perma.cc/2MAT-WQ7Y].

The Security Clearance Adjudicative Process

[50] The main goal of the security clearance process is to determine a person's suitability for access to classified information "through the evaluation of all information bearing on an individual's loyalty and allegiance to the United States."[169] Said differently, the clearance adjudication process is designed to evaluate traits and vulnerabilities that exist at the time the person applies for the clearance.[170]

[51] A person who applies for a security clearance must fill out the seemingly exhaustive "Standard Form 86," [SF-86] which requires the applicant to divulge and report a large volume of information about himself/herself.[171] The information sought by the SF-86 parallels the information required under the guidelines and is used to evaluate the clearance seeker under each guideline,[172] as well as by investigators, who collect more information based on the contents of the SF-86.[173]

[52] "National security eligibility determinations take into account a person's stability, trustworthiness, reliability, discretion, character,

[168] *See generally* 32 C.F.R. § 147 (2011) (providing adjudicative guidelines for determining eligibility for access to classified information); 5 C.F.R. § 731, 732, 736 (2012) (stating how personnel investigations work).

[169] SEAD 4, *supra* note 156, § E(4).

[170] *See* William Henderson, *Security Clearance: The Whole Person Concept*, CLEARANCE JOBS (Dec. 27, 2010) https://news.clearancejobs.com/2010/12/27/security-clearance-the-whole-person-concept/ [https://perma.cc/3HH6-QQ3Y].

[171] *See Questionnaire for National Security Positions, Standard Form 86,* U.S. OFF. PERSONNEL MGMT., https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf [https://perma.cc/7HHW-24AD].

[172] *See* SEAD 4, *supra* note 156, § D(2)(c); *see also infra* p. 20.

[173] *See All About Security Clearances*, *supra*, note 167.

honesty, and judgment."[174] There are thirteen guidelines ["SEAD Guidelines"] intended to evaluate the dimensions of a person that bear upon potential national security vulnerabilities:

> Guideline A: Allegiance to the United States
> Guideline B: Foreign Influence
> Guideline C: Foreign Preference
> Guideline D: Sexual Behavior
> Guideline E: Personal Conduct
> Guideline F: Financial Considerations
> Guideline G: Alcohol Consumption
> Guideline H: Drug Involvement and Substance Misuse
> Guideline I: Psychological Conditions
> Guideline J: Criminal Conduct
> Guideline K: Handling Protected Information
> Guideline L: Outside Activities
> Guideline M: Use of Information Technology.[175]

[53] Guideline B addresses "[f]oreign contacts and interests, including, but not limited to, business, financial and property interests, [because they] are a national security concern if they result in divided allegiance."[176] Moreover, "conditions that could raise a security concern and may be disqualifying include… shared living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion… [and] indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or

[174] SEAD 4, *supra* note 156, Appendix A §1(b).

[175] *See id.* at § D(2)(c).

[176] *Id.* at § 6.

coercion…"[177] These two provisions underscore some of the national security concerns that inform the adjudicative process.

[54] Guideline M addresses "use of information technology," specifically a person's "[f]ailure to comply with rules, procedures guidelines, or regulations pertaining to information technology systems… includ[ing] any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information."[178] This guideline fails, however, to address private use of technology and generally deals with unauthorized use of computer systems and networks on a narrow basis.[179] Nowhere in the directives, regulations, or procedures is there any kind of determination as to the risk inherent in or arising from a person's private devices.

[55] Guideline E addresses "personal conduct" and includes behavior characterized as "questionable judgment."[180] For instance, a person who peruses pornography on a government computer while at work may not be misusing systems under Guideline M, as discussed previously[181](unless they stored pornography on a government server), but that person's conduct would likely be considered bad judgment under Guideline E and considered accordingly by evaluators.[182]

[177] *Id.* at § 7(e), (h).

[178] *Id.* at § 39.

[179] *See* SEAD 4, *supra* note 156, § 40.

[180] *See id.* at § 15.

[181] *See id.* at § 39–40.

[182] *See* Russell-Hunter Interview, *supra* note 31.

Investigative Process

[56] The adjudicative process relies heavily on the efforts of background investigators who gather information used to ultimately adjudicate clearance seekers.[183] The National Background Investigations Bureau ["NBIB"] at OPM conducts most of the background investigations associated with the security clearance process, which includes "simple record checks, suitability and credentialing investigations, and more labor-intensive national security investigations."[184] In order to manage the security clearance backlog, "NBIB has improved fieldwork logistics by centralizing and prioritizing cases; increasing efficiencies of Enhanced Subject Interviews and reporting; and using more efficient methodologies by leveraging the power of technology to collect information."[185] The newly "increased digitization and automation of data, records, and information," NBIB predicts, will "facilitate[] faster case closings and adjudications."[186]

[57] NBIB also helps in the "continuous evaluation" process. Recently, they launched "programs to continuously evaluate personnel with security clearances to determine whether these individuals continue to meet the requirements for eligibility."[187] In other words, security clearance holders are subject to ongoing investigations periodically to verify their suitability.[188]

---

[183] *See Hearing on Security Clearance Reform Before the Select Comm. on Intelligence,* 1 (2018) (statement of Charles Phalen Jr., Director, National Background Investigations Bureau).

[184] *Id.* at 2.

[185] *Id.* at 3.

[186] *Id.*

[187] *Id.* at 4.

[188] *See Hearing on Security Clearance Reform*, *supra* note 183, at 4.

Gaps in the Security Clearance Regulations

[58] The current regulations and guidelines governing the issuance of security clearances, as well as the investigations that supply information to the process, fail almost entirely to address a person's private personal network connectivity. The SF-86 requires no information about a person's laptop, cellphone, Wi-Fi, social media accounts, or IoT devices linked in the home.[189] While the guidelines address information systems in Guideline M,[190] that guideline is designed to address a person's past misuse of networks in government or employment situations.[191] It neglects, however, to address a person's personal connectivity or network habits. Consequently, the adjudicators cannot gain a meaningful understanding of how a candidate uses IoT devices and whether that candidate's use is healthy or acceptable in terms of risk of foreign influence.[192]

[59] The stated purpose of Guidelines B and C is to minimize and know the extent of a person's foreign contacts.[193] Those guidelines even require information with regard to future risk of manipulation by foreign influences.[194] Many national security experts understand the need to modernize the clearance process: at least one expert in the field notes that background investigations evolve and that adjudicators should, at the very least, review a person's public social media posts.[195]

[189] *See Questionnaire for National Security Positions*, *supra* note 171.

[190] *See* SEAD 4, *supra* note 156, at Guideline M.

[191] *See id.*

[192] *See id.*

[193] *See id*. at Guidelines B & C.

[194] *See id*.

[195] *See* Russell-Hunter Panel, *supra* note 155.

Goals for Adapting the Security Clearance Process in a Highly Connected World

[60] Of chief importance is the need to adapt the process for more modern times while not over regulating clearance holders.[196] The process must strike a balance between a person's privacy and national security.[197] Historically, background investigations for security clearances included an investigator going to the candidate's neighborhood, knocking on doors, gathering background about the person,[198] yet today, "the internet is the neighborhood."[199] The new neighborhood requires a canvas of a different sort,[200] which explains the exploration of candidate's public social media.

[61] A major concern for policy makers in the security clearance space is navigating between the "Scylla and Charybdis" of valid threats to protect secrets and the imposition of onerous regulations on security clearance seekers and holders in their personal lives.[201] Regulating connectivity discourages the tech-savvy talent pool from applying to the government.[202] That a highly connected candidate would give up his/her

[196] *See id.*; *see also* Russell-Hunter Interview, *supra* note 183.

[197] *See* Russell-Hunter Panel, *supra* note 154.

[198] *See id*.

[199] *Id.*

[200] *See id.*

[201] *See* Russell-Hunter Interview, *supra* note 31 (Mr. Russell-Hunter likened the struggle to balance the government's national security interest against an employee's private life interests as navigating between the mythical beasts Scylla and Charybdis, two mythical monsters from the *Odyssey* who lived at the mouth of a strait. Scylla perched on the cliffside, while Charybdis lived in the water across the strait, inhaling water and causing a whirlpool. Any ships desiring to enter the strait would have to sail past the monstrous duo, and either risk being eaten by Scylla or destroyed by Charybdis' whirlpool).

[202] *See id.*

home devices to work for the government is dubious,[203] and so, the government must find a middle ground. It must not over-regulate a person's private home devices, but must account for the devices' vulnerabilities.[204] The tone of the article about the NSA ban on Furbies represents and demonstrates, in a way, the incredulity of society about the potential national security threats everyday devices pose.[205] Is it actually worth it to regulate stuffed animals that can mimic 100 English words if they can be used as crude recording devices? The NSA's vigilance with Furbies may have been extreme,[206] but ironically, the overreaction to an apparently minor threat in that situation contrasts significantly to the lax approach of security clearance adjudicators and investigators to evidently higher threat, intelligent devices like Alexa.[207] While the comparison between Furbies in NSA offices and Alexa in the homes of security clearance seekers and holders is not exact, it highlights, at this moment, the government's acceptance of technology's universality, or at least the government's delay in addressing the concerns of that universality.[208]

[62] Nevertheless, despite the stated need to adapt to the quickly changing technological landscape, the government has stalled in

[203] *See id.*

[204] *See id.*

[205] *See generally* Davis, *supra* note 160 (discussing how the National Security Agency's intelligence on Furbies in 1990 was "a bit off").

[206] *Cf. Talking Toy or Spy*, CBS NEWS (Jan. 13, 1999), https://www.cbsnews.com/news/talking-toy-of-spy/ [https://perma.cc/U35E-7CYQ] (expressing a concern that Furbies could record and act as personal audio equipment, which the owner of Furby refutes is a possibility).

[207] *See* Matt Toomey, *IoT Device Security Is Being Seriously Neglected*, ABERDEEN, (Feb. 5, 2018) https://www.aberdeen.com/techpro-essentials/iot-device-security-seriously-neglected/ [https://perma.cc/MEC6-QKKA].

[208] *See id.*

addressing these issues,[209] and not because the problem is invisible.[210] Policy makers are aware of the inherent lack of security in IoT devices[211] and how the Furby was banned,[212] yet they have made no attempt to protect against Alexa acting as a conduit for FIAs.[213] Nor have they tackled other issues arising from weak home network security, evidenced by the lack of regulations or directives confronting the problem.[214]

[63] Before discussing proposals to bolster and reinforce the security clearance process to account for the growing threat of IoT devices, specifically Alexa, this article will turn to hypothetical examples of FIAs manipulating clearance holders using Alexa.

VI. ALEXA GONE WRONG: USING ALEXA TO ACHIEVE FOREIGN INTELLIGENCE GOALS

[64] Once created through the audio or video obtained through Alexa, deep fake audio or video could be used as blackmail material, held ransom until a person pays money or completes a task for the blackmailer. Similarly, evidence of private or embarrassing sexual behavior, drug or alcohol abuse, or domestic violence, could be broadcast over social

[209] *See id.*

[210] *See id.*

[211] *See id.*

[212] *See Talking Toy or Spy*, *supra* note 206.

[213] *See generally* Toomey, *supra* note 207 (stating that security has been seriously neglected and that no laws have been passed that do regulate IoTs).

[214] *See generally Selected Reports*, U.S. DEP'T DEF., https://www.dhra.mil/PERSEREC/Selected-Reports/#TR18-16 [https://perma.cc/JFR6-9ZT5] (providing a catalogue of declassified analyses released by Defense Human Resources Activity and the Defense Personnel Security Research Center ["PERSEREC"]).

media—or at least the threat of broadcast could result in a great deal of leverage over a person.

[65] In terms of control, Alexa has the ability to link bank accounts, cars, door locks, and security video.[215] With access to a person's Alexa, a hacker FIA could jump from a hacked Alexa into a person's Alexa connected car, infiltrate the car's systems, and threaten to cause serious injury or death to a person or his/her family by shutting down the engine or hijacking the steering.[216] Alternatively, FIAs could plant suspicious bank transactions, car trips, or other data by jumping from an infiltrated Alexa into other linked services or devices, thus creating a trail of false evidence to "frame" the Alexa user.

[66] To illuminate the national security threat posed by Alexa, this article uses hypothetical worst-case scenario examples of Alexa being used by FIAs as a tool against people with access. More specifically, the hypotheticals focus on security clearances holders and demonstrate how these threats might materialize for three security clearance holders with different jobs.

Scenario 1: Young Employee "J" of Department of Homeland Security

[67] The young employee of Department of Homeland Security ["DHS"] called "J" lives alone and has worked for DHS in Washington, D.C. for five years. J's SF-86 and other information leaked onto the internet after the OPM hack.

---

[215] *See* John Matarese, *How Safe are Amazon Echo and Google Home?*, NEWS 5 CLEVELAND (May 23, 2018, 3:15 PM), https://www.news5cleveland.com/money/consumer/dont-waste-your-money/how-safe-are-amazon-echo-and-google-home- [https://perma.cc/36H3-4EWV].

[216] *See* JC Reindl, *Car Hacking Remains a Very Real Threat as Autos Become Even More Loaded with Tech*, USA TODAY (Jan. 14, 2018, 5:50 PM), https://www.usatoday.com/story/money/2018/01/14/car-hacking-remains-very-real-threat-autos-become-ever-more-loaded-tech/1032951001/ [https://perma.cc/4XKL-9E6M].

[68] FIAs use algorithmic analytics to identify potential targets by cross referencing DHS employee names with the database of information leaked in the Equifax hack. The FIAs' goal was to identify a person with financial instability who worked for DHS. FIAs identified J as vulnerable, because of his declining credit score and high level of debt. FIAs then parse J's social media posts, particularly Facebook and Instagram, but are unable to build a full picture of J's life because J keeps social media information relatively private. However, FIAs do find several of J's close friends because he follows them, intermittently comments on their Instagram pages, and has numerous mutual friends with them.

[69] FIAs, without much effort, conduct a phishing attack of J's personal email, disguising malware in an email from J's friend. J mistakenly clicks on the email and does not notice the subtle phishing scam. Once J clicks the link in the email from J's smartphone, connected to J's home Wi-Fi network, FIAs gain access to his network and find that J has an Amazon Echo with a built-in camera that is linked to numerous other devices in J's house. Since they have remote access to J's network, FIAs slowly, but surely, bypass the built-in security of the Alexa and gain access. The FIAs then download all of J's Amazon purchase history, contacts, bank account information, calendars, and a record of two years of voice commands made by J to Alexa. With the information gathered from Alexa, the FIAs build a comprehensive dossier and profile on J, focusing on the following facts:

- J calls his mother in Arizona every few days and speaks to her for approximately 30 mins each time (from Alexa contacts and calls);
- J has serious student debt, a car loan, a mortgage, and a private loan (from J's Capital One account linked to Alexa);
- J made frequent purchases at a pharmacy for between $500-$600 in Arizona for several hundred dollars, several times a month (through the NowRX Alexa skill);
- J asked Alexa what the most effective treatment for level II heart disease was (through PharmD Alexa skill);

- J flies from Washington, D.C. to Arizona approximately every two months (through Kayak.com Alexa skill);
- J's Echo connects via "drop in" function several times per week to J's mother's Echo;
- J works at the Nebraska Ave NW office of DHS (through the Alexa TrackR skill);
- J takes approximately thirty-five minutes to bike to work through Rock Creek Park (through the Garmin Alexa skill);
- J works late, and does not arrive home until approximately 7:30 or 8 p.m. (through the Nest thermostat Alexa skill);
- J walks to a coffee shop from his home on either Saturday or Sunday and spends an hour at the coffee shop (Alexa TrackR skill);
- J walks to a local pub on Sunday afternoons (Alexa TrackR skill);
- J purchases Arizona Cardinals football gear periodically in the fall and early winter (Amazon purchase history on Alexa);
- J purchases science fiction books that are forwarded to his Kindle e-reader and has a subscription to *The Atlantic* (Amazon purchase history on Alexa);
- J's Echo is in J's bedroom, and J keeps all valuables in the top right dresser drawer, including credit cards, etc. (Echo's video camera function);
- J's four-camera security camera system covers his front and back doors (outside), foyer, and back door (inside) (Alexa's Nest camera skill).

[70] From the profile, FIAs determine that J's mother is extremely sick with class II heart failure, and that J is supporting her, going so far as to take out a private loan to mollify the healthcare costs. J works hard but has crippling debt, and the cost of J's mother's drugs and travel to see her takes a toll on J.

[71] With the profile, the FIAs design a plan to "serendipitously" run into J at the coffee shop, meet J, build a relationship based on mutual

interests (e.g. science fiction, the Cardinals), become friends, and hint that they have contacts in the healthcare industry. Once rapport and trust are built, the FIAs will plan an "event" to strain J's finances even further. FIAs count on J feeling pressure to deal with the situation quickly, so the FIAs would attempt to bait J into asking for help with money or medical treatment. While J may have other options, the FIAs would manipulate J into turning to them.

[72] The event, they determine, will be a mugging, where they will steal J's wallet and credit cards during J's commute home through Rock Creek Park, in a specific location along that route with little traffic and few pedestrians or bystanders. The FIAs' objective is to force J to cancel his credit cards immediately before his mother's prescription autopay enables, delaying her access to medicine, and requiring him to reauthorize the new credit cards to pay for the prescriptions. J also will have to report the mugging to the DHS security officer, causing extreme stress for J, making J vulnerable to recruitment.

Scenario 2: Political Appointee of Executive Branch Agency "H"

[73] H, a clearance holder, was appointed as head of a federal executive branch agency. H has a substantial media presence and testifies publicly before Congress occasionally. FIAs target H originally for H's access, but also because H is an outspoken critic of the FIAs' government and an ally to the President. The foreign intelligence operational goal of targeting H is to assuage the current administration's harsh policies against FIAs' government.

[74] FIAs compile H's speeches and testimony and build a "deep fake" speech bank, mimicking H's speech patterns and voice, using the voluminous audio they gathered. With the speech bank, FIAs can mimic phrases of moderate complexity. FIAs decide to "frame" H for money-laundering.

[75] After studying H's general travel schedule (for speeches, talks, etc.), FIAs determine that H and H's spouse will be gone from their home

in Washington, D.C. for two days. Prior to H's departure, FIAs take thirty-five thousand dollars-worth of operational funds and deposit the funds into a bank account in Gibraltar.

[76] While H is away from his home, FIAs case H's home and see that H has an Echo in the kitchen, approximately twenty-five feet from a ground level window. With a hyper-directional speaker that focuses sound onto a specific place, from outside of the house, FIAs use H's synthesized voice to say "Alexa, activate the Capital One skill," thus enabling that Alexa skill. After approximately one minute, the FIAs use H's synthesized voice to say "Alexa, link my checking account with the following account," and they give Alexa the details of the FIA Gibraltar account. Alexa confirms that the accounts are linked. Immediately, the FIAs initiate a transfer of the thirty-five thousand dollars from the Gibraltar account into H's personal account.

[77] When H returns home, the FIAs, posing as local students, email H and arrange to meet over coffee to discuss academic paper ideas for policy issues related to H's agency. Upon meeting in a public place, the FIAs explain to H that they transferred thirty-five thousand dollars to his personal account from an offshore account and that they are ready to spread the story on social media in a social media feedback loop. The story would not only tarnish H's reputation and undermine his political image but also subject him to criminal charges. All that the FIAs ask is that H softens his policies toward the FIAs' government and stop speaking out against them.

Scenario 3: Support Staff Federal Employee "M" with Security Clearance

[78] Federal employee "M" enters data for the Governmental Accountability Office ["GAO"]. M obtained a security clearance several years ago. FIAs targeted GAO employees specifically because the FIAs

planned to mount a two-part "AirHopper" attack,[217] which facilitates transmission of data from an "air-gapped"[218] computer without actually physically accessing the computer. The FIAs had already infected GAO computer systems with a dormant "AirHopper" emitter malware ["AirHopper emitter"], which could transmit small amounts of data using radio frequencies emitted from a monitor connected to the infected computer, between one and seven meters away.[219] For the second part of the attack, FIAs needed to place a AirHopper receiver malware ["AirHopper receiver"] infected device within seven meters of an AirHopper emitter, that way the emitting computer could send data to the receiving device without physically interfering with the computer. Thus, FIAs are seeking a GAO employee to who worked in proximity to the AirHopper emitter infected computers to bring a device with an AirHopper receiver into the GAO.

[79] FIAs identify M as an employee of the GAO from the leaked database from the OPM hack. Based on her job description, FIAs extrapolate that M has access to classified information, or at the very least, information about sexual harassment complaints, corruption investigations, and waste allegations against numerous public officials, all of which is highly valuable to the FIAs. Thus, ex-filtrating that information from GAO computers became highest operational priority. To hack the GAO to obtain that information, they would need keystroke logs of network passwords and individual logins, information sufficiently small to transmit via AirHopper. Based on the value of the information, FIAs

[217] *See generally* Mordechai Guri et al., *AirHopper: Bridging the Air-Gap Between Isolated Networks and Mobile Phones Using Radio Frequencies*, DEP'T INFO. SYS. ENGINEERING, BEN-GURION U. (Nov. 2, 2014), https://arxiv.org/abs/1411.0237 [https://perma.cc/3YCL-NDBE] (providing a background on AirHopper technology).

[218] *See id.* ("Air-gap" refers to self-contained networks or computers not connected to the general internet, as a way to prevent internet-based hacks against a system).

[219] *See id.*

plan to investigate M further to see if M has exploitable vulnerabilities that might predispose her to recruitment.

[80] FIAs determine that M's home network may be susceptible to attack,[220] so they penetrate M's network, and access M's data on Alexa. The FIAs reprogrammed M's Alexa to surreptitiously listen and record continuously.[221] The FIAs then listen to M in M's home, gathering data about M's habits, and they determined M might be difficult to recruit from a HumInt standpoint. The FIAs took note of M complaining about M's mobile phone. At that point, FIAs decide M would work as an unwitting Trojan horse.

[81] To bait M further into purchasing a phone as a part of their plan, FIAs deliver a "promotion" to M's home, giving M a fifteen-percent discount on a new Samsung phone if M made the purchase through Amazon.

[82] Eventually, M says to Alexa: "Alexa, buy me a new Samsung phone, and have it shipped to the house in two days," a command Alexa confirms. With the knowledge that the phone would arrive at the house in two days, the FIAs purchase an identical phone and install the AirHopper receiver in it. The FIAs then repackage the phone, package it into an Amazon Prime box, print an identical FedEx label, and wait for the phone to be delivered. Once the delivery driver leaves the package on M's front doormat, FIA's replace the newly purchased phone with the AirHopper receiver-fitted phone. The AirHopper receiver would allow M's new

[220] *Cf.* Steve Bell, *How Hackers Access Your Computer*, BULLGUARD BLOG (Apr. 27, 2015), https://www.bullguard.com/blog/2015/04/how-hackers-access-your-computer [https://perma.cc/6MWX-E7MV] (demonstrating that many computer hacks are based on sweeping probes; therefore, every computer may be a target).

[221] *See* Kevin Murnane, *Amazon's Alexa Hacked to Surreptitiously Record Everything It Hears*, FORBES (Apr. 25, 2018, 09:00 AM), https://www.forbes.com/sites/kevinmurnane/2018/04/25/amazons-alexa-hacked-to-surreptitiously-record-everything-it-hears/#73e8bea34fe2 [https://perma.cc/L2RF-7JQN].

phone to log keystrokes and passwords, sent from air-gapped, secure computer systems nearby, already infected with the AirHopper emitter.[222]

[83] M unwraps the phone, syncs it on the home network, and takes it to work at the GAO, past security. M thus unwittingly carries the phone with the AirHopper receiver to M's desk. The AirHopper receiver-fitted phone syphoned small amounts of information, like network passwords, M's login credentials, *inter alia* from inside the GAO. Once M returns home and the new phone connected to M's home network, FIAs ex-filtrate the password and security data from M's phone.

VII. PROPOSALS FOR CONFRONTING THE NATIONAL SECURITY THREAT POSED BY ALEXA

[84] The FIA's threat of misapplication of Alexa to hurt United States national security interests is real. The above hypotheticals illustrate only a few of the ways Alexa poses a danger to security clearance holders.[223]

[85] While policy makers acknowledge the effect that technology's evolution is having on national security, they seem to disregard a major issue: people with access to classified and sensitive information are connected to the internet in their personal lives.[224] Even assuming *arguendo* that government systems are fortified or impenetrable, the millions of employees with clearances have phones, wearables, and Amazon Echoes with glaring cyber-vulnerabilities. Because of the vast amount of information those devices contain about their users and the relatively low level of digital security, user's information is left exposed

[222] *See* Guri et al., *supra* note 217, at 3.

[223] *See supra* Part VII.

[224] *See* Michael Kan, *Potential Apple Watch Snooping: A Not-So-Paranoid Cyberespionage Risk*, PC WORLD (Oct. 10, 2016), https://www.pcworld.com/article/3129459/potential-apple-watch-snooping-a-not-so-paranoid-cyberespionage-risk.html [https://perma.cc/8Y53-B2R4].

and ripe to be plucked.[225] For a person with access to sensitive information, that exposure is a serious vulnerability that FIAs are trained to exploit. Clearance holders with Alexa at home make it easy for FIAs to collect information about them, leaving them exposed.

[86] The security clearance adjudicative and investigative processes, as the gatekeeping functions for access to classified information,[226] seem to be the ideal frameworks to incorporate measures designed to protect against home network vulnerabilities, exemplified in this discussion by Alexa. The following proposals function as guideposts for protecting against the national security vulnerabilities inherent in IoT devices, private home networks, and Alexa. Notably, none of the proposals require an outright ban on Echoes or IoT devices. Rather, the proposals seek to illustrate how the government can navigate between the "Scylla and Charybdis" of over-and-under regulation and find a reasonable middle ground that achieves protection of security clearance holders without onerous terms.

Proposal I) Mandatory education for clearance seekers and holders about cybersecurity, with a focus on management of IoT devices and home assistants, and how to use "best practices" for managing personal devices and data.

[87] The importance of education and training, especially for technological issues which are rapidly evolving, cannot be understated. The federal government already requires yearly cybersecurity training,[227] but an additional segment in such a training focusing exclusively on private home network security, and/or the security vulnerabilities of IoT devices and home assistants would provide a cheap way of bolstering

[225] *See id.*

[226] *See* U.S. DEP'T STATE, ALL ABOUT SECURITY CLEARANCES, https://www.state.gov/m/ds/clearances/c10978.htm [https://perma.cc/5KYB-MQAV].

[227] *See* 5 C.F.R § 930.301 (2019).

network security in the private lives of security clearance seekers and holders. This proposal would require the clearance seeker to undergo the education before actually earning the clearance, and it would require the clearance holder to undergo the training as a part of the continuous evaluation process.

[88] The downside to this proposal is that federal government employees already undergo comprehensive cybersecurity training annually.[228] Some federal employees find the cybersecurity training to be a nuisance and a waste of time,[229] and additional material might overwhelm employees in a way the renders the presentation of the private home network security issues ineffective. Additionally, the government collects no information as a part of this proposal, and thus has no way to measure or check whether those receiving the education actually implemented safeguards accordingly.

Proposal II) Disable artificial intelligence features on all home IoT devices.

[89] Somewhat analogous to the NSA's Furby ban in the late 1990's, this proposal would require that a security clearance candidate disable the AI functions on any IoT devices in the home. The goal is not to ban IoT devices, but rather to limit the degree to which the digital tentacles of an AI (i.e. Alexa) reach into a person's life. Alexa would become nothing more than a smart speaker.

[90] This simple yet broad proposal would require a candidate, before completing the security clearance process, certify or attest that they disabled the AI functions on all IoT devices in the home, specifically the

[228] *But see id.*

[229] *See* Matt Miller, *Cybersecurity Training: A Guide to Making It Stick*, IT FREEDOM BLOG (Oct. 21, 2016), https://blog.itfreedom.com/blog/cyber-security-training-guide-making-stick [https://perma.cc/6D9U-YGN7].

AI functions of home assistants.[230] Clearance holders would complete and submit the certification as a part of the continuous evaluation process.

[91] This proposal deals with the national security risk of AI based devices in one sweeping decree. It requires few resources and could be easily implemented and would only minimally affect the security clearance process. Also, it does not deprive people of any devices, only those features that are most risky.

[92] However, this approach lacks finesse and fails to address the root of the problem. It fails to account for the core reasons why a person's AI devices might be national security risk: poor home network security, weak passwords, etc. The proposal's prohibitions are over-inclusive, over regulating facets of a person's private home life unnecessarily and probably upsets the balance between government interest in security and an employee's (as well as the employee's co-habitant's) private interests at home. Implementation of this proposal would likely cause extreme disenchantment with the government for those clearance holders with Alexa-enabled devices and make it difficult for the government to recruit technologically-savvy people in the future because of the proposal's imposition into people's home lives.

Proposal III) Adding a fourteenth subcategory in the SEAD guidelines to address private, personal devices and information management practices, follow up investigations, and temporary suspension of clearance process for mitigation.

[93] The SEAD guidelines outline thirteen categories of criteria to determine suitability for access to sensitive information protected by security clearance.[231] The clearance adjudicative process requires that a

[230] Whether or not the disabling of AIs should extend to smart phones is a question that would need to be addressed if this rather extreme proposal were implemented.

[231] *See* SEAD 4, *supra* note 156, at 6.

clearance seeker reveal private information, sometimes intimate information about drugs, alcohol, friendships, sexual behavior, and other areas.[232] But, the SEAD guidelines neglect to address private home network security. The failure to ask about such an important facet of a clearance seeker's personal life seems like a serious oversight, or at least a reflection of the government's slow response to national security issues arising from private home connectivity. The government should attempt to gain a better understanding of potential security risks borne from a person's weak private network security. Notably, this proposal could be implemented for security clearance candidates and for clearance holders undergoing continuous evaluation.

[94] This paper proposes a "Guideline N" addressing "private home network security and device management." The purpose of the guideline is to evaluate the strengths, weaknesses, risks, and vulnerabilities of a person's home security and IoT networks, and to measure those vulnerabilities in a standardized way.

[95] The guideline would require a clearance seeker to list the following:

i. all IoT devices, home assistants, routers, computers, and mobile phones;

ii. the number of letters and numbers, symbols, and total characters of the password for each device (not actually divulging the password), note how many of the devices have the same password, and how often the person changes the password;

The answers to sections (i) and (ii), would be standardized in a way to comply with NBIB's new digitized and automated system[233] to allow for

[232] *See id.*

[233] *See* Statement of Charles Phalen, Jr., *supra* note 183, at 3.

more efficient recommendations for adjudicators. The "preliminary scores" given would be coded so that a higher score means a higher national security risk due to poor network security. In (ii) above, the question would be framed in such a way that it did not reveal too many details about the password. For instance, the question might be "if your password is 1-5 characters long, enter a 3; if it is 5-10 characters, enter a 2; if it is 10-15, enter a 1," etc. That coding would give investigators sufficient information to judge the strength of a password without actually getting specific details about the password.

[96] The preliminary scores would help guide the investigators with their collection of information about a particular candidate. The scores would correspond with three tiers of national security risk: low, medium, and high-risk. A low-tier score, indicating "adequate" private home network security, would not require additional investigative action.

[97] The medium-tier score, indicating "sub-optimal" private home network security, would require a telephone interview with the candidate, in which the investigator would learn specifics about the person's private home security habits, as well as how often they use their home assistants, why they use them, what "skills" the home assistants have, whether they have video capabilities, and so on. From the information gathered, the investigator would decide if the case could be treated as a low-tier score case, not requiring further action, or a high tier score case, moving to a high tier score case protocol.

[98] The high tier score case, indicating "high risk" private home network security, would require a field visit to the candidate's home by the investigator. The investigator would not only interview the candidate about the network practices, but also inspect the various IoT devices and home assistants. With the information gathered during the field visit, the investigators would then make a decision: first, recommend that the candidate be denied security clearance due to high-risk home network security, or alternatively recommend that the clearance process be "suspended" for thirty days for the candidate to engage in private home network security mitigation.

[99] If a candidate's clearance process was suspended, they would be given an additional form, a private home network security mitigation form ["mitigation form"] requiring them to improve their home network security practice. The mitigation form would require the candidate certify compliance on a "yes or no" basis, in accordance with specific parameters: change passwords install anti-malware software, clear data on various devices, and/or limit some device capabilities. If the candidate completes the form and submits it within the allotted time, the investigator reviews the form and either recommends that the suspension be lifted, and they be treated as a low tier score candidate, or that the candidate be denied a security clearance. For clearance holders undergoing continuous evaluation, rather than a "suspension," the holder would have thirty days to satisfy the criteria on the mitigation form and submit it to the continuous evaluation investigators.

[100] A primary benefit of this proposal is that it requires only a few questions be added to the SF-86. Also, the involvement of investigators corresponds with the new NBIB digitization and automation of security clearance investigations,[234] aimed at high investigative efficiency. Candidates are only intensely screened for private home network security risks if they are deemed to be a high risk. Lastly, and most importantly, the proposal's modifications to the existing system require, in the most vulnerable candidates, action on the government's part to evaluate the risk. This proposal, like a net, will catch only the large risks, letting low risk candidates pass through without additional action. Also, the proposal does not limit what a person may or may not possess in his/her private life. Therefore, the proposal achieves a balance between the government's national security interests and the private interests of its employees.

[101] The proposed solution does have limitations. First, writing information about passwords on an SF-86 may itself be a security risk, especially considering the recent OPM hack in which almost all SF-86s

[234] *See id*.

were leaked.[235] Any information about a password could aid a hacker or FIA crack that password, assuming they gain access to a person's SF-86.

[102] Moreover, it does not account for spouses' or roommates' private home network security practices. The candidate's co-habitants have the capability of becoming private home network weak points, creating additional network security risks. A solution might be for the preliminary score to reflect the risk added by co-habitants or those with frequent access to the network, and for the investigator to talk with those co-habitants in a middle tier or high tier score scenario.

[103] The proposal suggests an unusual mechanism in the security clearance process that veers from the typical clearance process' course: the mitigation suspension period. Historically, the clearance process determines weaknesses and vulnerabilities at the time it is conducted.[236] Besides submitting to a polygraph, submitting forms, or submitting to interviews, granting or denying a clearance is not based on any action on the part of the candidate.[237] This proposal adds an atypical procedural hurdle, which puts the onus onto the candidate, in some circumstances, to mitigate his/her poor home network security practices. While this characteristic may be viewed as a limitation, it is also a strength: with the onus on the candidate to mitigate, the government need not spend more money, while receiving assurance from the candidate that he/she improved his/her private home network security.

[235] *See* Ellen Nakashima, *Hacks of OPM Database Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.f0842aea1508 [https://perma.cc/B9V3-EV7J].

[236] *See supra* Part V.

[237] *See supra* Part V.

VIII. CONCLUSION

[104] The security clearance process, although not by any means perfect, takes a measured and careful approach to evaluating clearance seekers for vulnerabilities and weaknesses. It can be easy to forget that people with security clearances have lives outside of the SCIF, and the clearance process does, in many ways, try to balance the government interests in national security and protection of classified information with a clearance seeker's home life privacy interests.

[105] Enter Alexa: extraordinarily convenient, "she" manages many facets of a person's home life, and, if a person gives her the ability, she will carry the keys to the car, the bank vault, and, quite literally, the door to the house. This article detailed how Alexa can inadvertently give those keys to FIAs, with those FIAs putting forth little effort. As a result, the government faces an extraordinary task: how can it protect classified information and guard national security interests now that millions of people, including clearance seekers and holders, have Alexa in their homes?

[106] Amazon and other companies that sell home assistants must do their part to improve the security of devices like the Echo, because IoT devices lack built-in security measures. Hopefully, Congress will see fit to enact legislation mandating some degree of built-in cybersecurity on home devices to prevent infiltration by hackers and FIAs. The government's cybersecurity capabilities are extensive, yet companies like Amazon are best positioned to improve the security of the devices they sell and are best positioned to assure the security of individual devices for individual users.

[107] However, the government cannot wait until companies like Amazon devote serious resources to security of their devices or wait for Congress to enact broad legislation. FIAs and criminals continue to advance and evolve their technological means, just as the cybersecurity technology improves. Therefore, it is incumbent upon the government to take action to achieve its national security goals.

[108] The three above proposals, in terms of the security clearance process, vary in terms of balancing national security goals and individual private interests. The first two proposals fail to achieve the balance, under-regulating or over-regulating the clearance seeker or holder. The third proposal seeks to strike the right balance, navigating between "Scylla and Charybdis." It neither overhauls the current system, nor imposes heavy budgetary burdens. It may not be perfect, but it would achieve a high degree of risk management for vulnerabilities in clearance seekers. Fortuitously, the investigative process based on recent developments in the investigative process by NBIB, the government could implement the Proposal III system not only for clearance seekers, but also for clearance holders undergoing the continuing evaluation process, with only small adjustments.

[109] Certainly, the government must manage, to some degree, the threat of FIA influence on individuals with access. The goal of the security clearance process is to evaluate suitability of a particular person for access to classified information, by analyzing the person's potential vulnerabilities to foreign influence. To grow and evolve with the national security threats to individuals, the government must adapt to and address the connectivity of people generally, and it must rise to combat the exploitation of that human interconnectivity by foreign influences. Alexa may be AI, but she is not yet intelligent enough to prevent FIAs from taking advantage of her. The government must decisively step in and manage the vulnerabilities of its employees arising from private home connectivity and implement measures to encourage responsible use of Alexa at home, so she does not get recruited by foreign agents.