Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 40-48 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

VIRTUAL ASSISTANTS & ARTIFICIAL INTELLIGENCE: TRANSFORMING DIGITAL CENSORSHIP

Yasir Nawaz Shaikh, Cybersecurity, Artificial Intelligence,Organization: PureVPN, Digital Content Producer, Karachi, Pakistan

ABSTRACT

Artificial Intelligence continues to break new barriers each day. Thanks to AI, it is not inconceivable to believe that we may rely even less on actual physical labor than we do now. One such example of virtual assistants such as Alexa, Siri, Google Assistant, Cortana, Bixby, and many more. While currently, they are glorified tools on our smartphones for voice commands, they are quickly being programmed to be the perfect assistant suited for our daily tasks. While that sounds great, it comes with a threat that may not be immediate, but it is only a matter of time until it does; censorship.

This study triangulates the opinion of renowned authors and researchers within the field of Artificial Intelligence to get an idea of what the future holds for censorship online in an era when artificial intelligence-backed assistants are the primary customers toggling through the visible search results, and humans rely on them for their effectiveness and efficiency. The results indicate a need for brands to rethink how they inform their customers, the importance of brand recognition and loyalty in the era ahead and a much better-informed public that does not solely rely on the search results provided to it via these assistants.

KEYWORDS: *Cybersecurity, Artificial Intelligence, Digital Censorship, Virtual Assistants*

Rubrics: Cyber hygiene, cybercrime, information warfare.

Introduction

"AI will overtake humans within the next 100 years. When that happens, we need to make sure the computers have goals aligned with ours" – Stephen Hawking (Matyszczyk, 2015)

Not only did Hawking's prediction come to fruition, but it came a lot sooner than even he may have anticipated. Machines and artificial Intelligence have begun substituting humans in areas that were previously considered impossible (Paulo, 2019). While some might point to the doom and gloom aspect of such wide-scale automation, there is an undeniably enormous amount of potential (Chui, et al., 2016). Nothing will be spared of the effects of Artificial Intelligence becoming more potent, that includes marketers (Talbot, 2019).

Arguably no other facet of modern technology represents AI in its most human-interactive form than virtual assistants. After all, it is an interface designed to "have all the perfections of human interactions and none

of the flaws" (Joshi, 2018). Allowing people to designate mundane tasks, receive timely updates on their billing information, crack a joke or two, and reorganizing the way it interacts based on learning patterns displayed by the users (Jurowiec, 2018).

The rising popularity of voice assistants such as Alexa, Cortana, and Google Assistant has made it easier for users to interact with the Internet (Cheyer et al., 2014). Simultaneously, it has managed to revolutionize the concept of multi-tasking. Forget "just a click away," now whatever you need is a "sentence away" (Guzman, 2019).

However, that has given rise to another question, frequently asked and discussed in both journalistic and academic circles, i.e., what intelligent AI designs mean for online censorship (Black & Fullerton, 2020). Of course, popular culture is filled with anecdotes and references to how an all-knowing AI could become self-aware and proceed to perceive humans as an enemy (Henry, 2020). Nevertheless, in more realistic terms, there is a surprising lack of research about the future iterations of Alexa and Google Assistant means for our access to information.

A more frequently touted scenario is what if humans were to become entirely dependent on these assistants for their daily news. Furthermore, under government regulations, what if these AIs were to omit certain pieces of information (Feldstein, 2019). In a genuinely Orwellian sense, we would not even know what we are not being told since we would not know there is something to miss out on. One might argue that this is an incredible stretch of the imagination, but one must also wonder, "Is it beyond plausible possibility?".

Simultaneously, it is considered inevitable that sooner or later, these virtual assistants will become the prima facto customers online as human activity online becomes increasingly automated (PwC, 2018). Human decisions might be eliminated, or at the very least, severely limited. The information available online will reflect that. We have already begun seeing such technology in its infancy on social media apps like Twitter and Facebook, where each news article is first vetted by bots and then presented to the viewer, with an accompanying fact-check message (Ding, 2018). As mentioned earlier, government regulations in the future could mean that this news vetting process could be taken to the next step. That next step could be draconian, considering the state of modern censorship practiced in modern dictatorships (Mchangama & Fiss, 2019).

Literature Review

Human-Machine Interaction

The prominence that virtual assistants have gained in the past few years falls in line with the guiding principles of AI innovation (Martinez-Lopez & Casillas, 2013). While companies have long foreseen the

looming reality that increased automation will present, there has been ambiguity in maximizing the potential opportunities it will present (Siau & Yang, 2017).

The primary reason for this has been the lack of foresight. That AI is the future has long been an accepted datum within the corporate world. The problem is, how does that future look like? As (Sterne, 2017) states, once technological innovations take a firm grip in terms of societal presence, it can take on a life of their own.

In other words, brands might have specific strategic objectives and tactics for virtual assistants in mind today based on how they exist today. Those strategies and tactics may become obsolete within a few years, depending on the direction virtual assistants take (Hoc, et al., 2013). These strategies and tactics might very well take on a more aggressive look once government agencies adopt them.

There is a flip side to the ease of inducing increased AI presence in our lives. Through various legislation, governments can create a back-channel in all these virtual assistants. There have been modern instances of mass-scale surveillance. Virtual assistants would make censorship far easier since there will be an active actor within our households that could be used. Such an act's legality would be debated, but one cannot remain optimistic if past examples are to go by.

Censorship in the Digital Age

New leaps in technology always promise a more effortless flow of information. The advent of the Internet meant that information could be communicated far easier and more accurately than ever. Subsequently, emails, multimedia options, and lastly, social media meant that information travels almost instantaneously. However, just because technology promises something does not always translate into practice. Governments, mainly, repressive ones have always held a penchant for stifling any such easy flow of information (Tenczer, et al., 2016).

They will undoubtedly welcome any tool that aids their efforts in restricting information they might be dangerous. These governments might welcome such developments since dissenters have begun evolving their methods (Shiwen & Mai, 2019). Unlike the past, where silencing journalists and provocateurs meant effective control of information, the digital age has transformed anyone with a smartphone into a conduit for information (Nadaf, 2020).

In such a scenario, a virtual assistant could be weaponized against the proliferation of such information deemed dangerous. We have seen how tech giants like Facebook and Google have had to bow down to demands by repressive governments worldwide (Coskuntuncel, 2018). Such past precedence begs the

question of how Orwellian virtual assistants in every house might be. In an age where virtual assistants are the primary source of information, if the assistants could be programmed to restrict their users' access to specific content, they might not even realize that they are being denied information (Qiang, 2019). 2+2 would become 5 since the user would not know how addition works. Hence, they would be unable to raise objections to the results being shown to them.

VPNs in the Age of Alexa

Virtual Private Networks (VPN) have been an essential asset available to dissenters by far when it comes to circumventing the restrictions imposed on them by repressive governments. (Peterescu & Krishen, 2020). Journalists, whistleblowers, and activists have relied on the tool to help them retain access to the Internet even when widespread restrictions have been imposed in their countries (Ververis, et al., 2019).

VPNs have retained their popularity since they are easy to set up and inexpensive. The paid ones provide better features and a far more secure sense of anonymity online, but the free services are good enough to unblock blocked content (Lilkov, 2020). However, that entire paradigm is likely to go a complete upheaval in the age of virtual assistants like Alexa (Perry & Roda, 2017). For instance, VPNs are already criminalized in several countries. However, no mechanism allows governments to restrict users from downloading the service (Khan, et al., 2018). Several VPNs usually set up mirror sites that allow users to easily download the service from within those countries even if the original website is banned (Hobbs & Roberts, 2018).

Enter the virtual assistant. Since the virtual assistants are the primary customer, governments could program them to ensure that users could not download the service via their internet connections (Wang, et al., 2020). Moreover, even if somehow users could install VPNs, these virtual assistants could alert the government agencies that such an app was detected on the user's device (Black & Fullerton, 2020). This might all be conjecture and speculation at this point, but since this study follows a secondary research model, past research indicates that governments have employed agents within populations to spy on their citizens' activities. There is no reason to believe that given the capability, governments would not, or at least would not attempt to carry out such protocols (Kaylee, 2020).

Research Question

How will VPNs adapt to the age of virtual assistants and ensure seamless accessibility to users in the most vulnerable countries?

Despite their obvious uses, will virtual assistants become government surveillance tools inside every house they are in?

Methodology

Since this study aims to study the potential effects of what the progress in virtual assistants and AI means for digital censorship, the primary source of data to be studied will be secondary. This means that this project will build on the work already done by researchers and past studies.

Initially, a thorough analysis of the secondary data available will be conducted. This would include a more exhaustive and extensive study of the literature that already exists on topics that lie on the fringes of the problems that this study hopes to address. The study of peer-reviewed literature will enable us to understand the academic discourse on the subject (Callaham, et al., 2002).

Since virtual assistants are a relatively new concept, it is necessary to understand the psychological motivations behind how government agencies could use them to censor information online.

In the end, data collected from up to 5-10 studies will be used to support arguments for what lies ahead in terms of censorship (Strauss, 1987). Since the purpose of this study is to triangulate the relationship between the rise in AI, its censorship potential in the hands of governments, and how VPNs will evolve in the light of those, the studies will be varied to cover all three subjects adequately (Maxwell, 2008).

Nature of Research

The nature of this research will be in interpretivist terms. Such an approach would allow the researcher to integrate the contrasting nature of the data gathered via different past studies and cases studied.

Findings

Since this paper follows a secondary form of research in an area that is still in its relative infancy, the ideas discussed continually undergo changes. However, all the resources used in this study illustrate a standard agreement on the one fundamental assertion; the relationship between humans and the Internet will change. This will undoubtedly be further exacerbated by the consistent improvement in how Artificial Intelligence, specifically virtual assistants, understand the Internet.

Aggravated Control:

It seems as if the writing is on the wall in terms of virtual assistants becoming increasingly popular. Like with invention in the internet age, virtual assistants will change the entire way humans interact. For instance, Stuard Russell and Peter Norvig state in Artificial Intelligence: A Modern Approach that these virtual assistants' sheer capabilities mean that humans will be unlikely to refuse to let them take over. If a human were to look over the Internet for a particular brand of shoes available at the lowest price, a virtual assistant could easily outperform and out search any human in a significantly less amount of time. Through the virtue

of pattern studies and previous search patterns, there may even come a time when these virtual assistants could easily predict exactly which criteria to use when searching for specific products.

Need To Reinvent

This is where ethical dilemmas truly start emerging. Alec Ross argues in his The Industries Of The Future that the very idea of privacy will come under attack in the age of virtual assistants. The book carefully investigates how, despite the ease of use they offer, it comes with several trade-offs. Moreover, we still do not know how severe or impactful these trade-offs can be in the long-run. For instance, in a future where virtual assistants are essentially the primary customers (Considering they are the ones that make the actual searches on Google through voice commands), it is the virtual assistant looking at the SERPs. At this point, the full potential of AI will come into place as these virtual assistants can easily comb through websites that use SEO black hat techniques to climb up the search results without offering the best product in return. If this is how it plays out, this essentially means two things. One, digital marketers will need to rethink their approach towards building their brand entirely. The current modus operandi of offering a value proposition often elicit an emotional response from the user. This will be absent entirely when it comes to AI-powered virtual assistants doing those searches for us.

Similarly, it gives most government agencies an unprecedented opportunity to control the way their citizens behave online. There is little or no government regulation directly dealing with these virtual assistants, but that is likely to change in the future. If, at any point, these were to be programmed to comply with government regulations, they could easily be used to filter out and censor search results a government does not want visible to its citizens. Furthermore, if humans are not the ones looking at the SERPs, they may not even know the results are being censored in the first place. Regarding VPNs, if a government were to ban VPNs, the virtual assistants would omit any relevant SERPs to them completely. A more infant form of similar censorship is already a staple of the Great Firewall of China, where most VPN providers are not allowed to operate and are entirely opaque to a significant part of the population. AI-powered censorship could multiply that manifolds.

Discussion

This paper deals with two essential questions: VPNs' future in an artificial intelligence-reliant world and whether it is headed towards obscurity in front of government regulation. Most of the current literature suggests that it is likely that governments are trying to pressurize VPNs to operate, with a catch, sharing complete activity logs. Complete bans have been enforced in the past, and they do remain in effect in several countries around the world. However, that does nothing to discourage users eager to use a VPN from simply

choosing the next available VPN service. By giving this small leeway, governments may end up gaining the amount of informational control since all VPNs will be required to provide logs. Considering how the general populace remains mostly unaware of how much data is being collected about them, it is not far-fetched to imagine them signing up for these services without reading the fine print.

This brings us back to the initial question; is that the future of VPNs? Government-mandated, in other words, government oversight. It does not have to be that way, but that would depend on more than one factor. Current research, as well as market incentive, lacks substantial study of such a scenario. However, the onus will fall on the developing end of these VPN providers to address these concerns. It would have to start with how they would deal with voice commands and voice searches in particular regions. Governments cannot control how a private business operates, but it can affect those options' visibility to potential customers. Since the projections indicate that most online searches will shift to voice searches, it will not be the humans making the best decision for themselves. Humans will probably not even be exposed to the SERPs. Hence, it would be worthwhile for VPN providers to start planning how to target and maximize their visibility to users through these voice assistants. More importantly, how they would evade restrictions by governments on these SERPs.

REFERENCES

1. Akgun, Ali Ekber, Ipek Kocoglu, and Salih Imamoglu. 2013. "An emerging consumer experience: Emotional branding." Procedia-Social and Behavioral Sciences 99: 503-508.
2. Ana, Canhoto Isabel, and Yuvraj Padmanabhan. 2015. "We (don't) know how you feel'– a comparative study of automated vs. manual analysis of social media conversations." Journal of Marketing Management 31 (9-10): 1141-1157.
3. Anand, Priya. 2018. The Reality Behind Voice Shopping Hype. Accessed October 11, 2019. https://www.theinformation.com/articles/the-reality-behind-voice-shopping-hype.
4. Barrett, Lisa Feldman, Ralph Adolphs, Stacy Marsella, Aleix Martinez, and Seth Pollak. 2019. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements." Psychological Science in the Public Interest 20 (1): 1-68.
5. Basch, Charles. 1987. "Focus group interview: An underutilized research technique for improving theory and practice in health education." Health education quarterly 14 (4): 411-448.
6. Bazeley, Patricia, and Kristi Jackson. 2013. Qualitative data analysis with NVivo. Sage Publications Limited.
7. Biernacki, Patrick, and Dan Waldorf. 1981. "Snowball sampling: Problems and techniques of chain referral sampling." Sociological methods & research 141-163.
8. Biernacki, Patrick, and Dan Waldorf. 1981. "Snowball sampling: Problems and techniques of chain referral sampling." Sociological methods & research 10 (2): 141-163.

9. Black, Joanna, and Cody Fullerton. 2020. "Digital Deceit: Fake News, Artificial Intelligence, and Censorship in Educational Research." Open Journal of Social Sciences 8 (07): 71.
10. Black, Joanna, and Cody Fullerton. 2020. "Digital Deceit: Fake News, Artificial Intelligence, and Censorship in Educational Research." Open Journal of Social Sciences 8 (7): 71.
11. Bolls, Paul, and Darrel Muehling. 2007. "The effects of dual-task processing on consumers' responses to high-and low-imagery radio advertisements." Journal of Advertising 4 (36): 35-47.
12. Bonnington, Christina. 2018. What It Would Mean for Amazon to Bring Ads to Alexa. Accessed October 19, 2019. https://slate.com/technology/2018/01/amazon-echo-getting-ads-as-company-finds-promotional-partners-for-alexa.html.
13. Brooke, Sophia. 2019. Why AI for Logo Detection Is the Next Marketing Must-Have. Accessed September 22, 2019. https://blog.markgrowth.com/why-ai-for-logo-detection-is-the-next-marketing-must-have-e57a195a730a.
14. Brooks, Joanna, Serena McCluskey, Emma Turley, and Nigel King. 2015. "The utility of template analysis in qualitative psychology research." Qualitative Research in Psychology 2 (12): 202-222.
15. Buckley, Ralf. 2016. "Aww: The emotion of perceiving cuteness." Frontiers in psychology 7 (1740).
16. Calisir, Fethi, and Demet Karaali. 2008. "The impacts of banner location, banner content and navigation style on banner recognition." Computers in Human Behaviour 2 (24): 535-543.
17. Callaham, Michael, Robert L Wears, and Ellen Weber. 2002. "Journal prestige, publication bias, and other characteristics associated with citation of published studies in peer-reviewed journals." Jama 287 (21): 2847-2850.
18. Carrier, Mark, Nancy Cheever, Larry Rosen, Benitez Sandra, and Jennifer Chang. 2009. "Multitasking across generations: Multitasking choices and difficulty ratings in three generations of Americans." Computers in Human Behavior 2 (25): 483-489.
19. Chang, Yuhmiin, and Esther Thorson. 2004. "Television and web advertising synergies." Journal of Advertising 2 (33): 75-84.
20. Chowdhury, Rafi, Adam Finn, and Douglas Olsen. 2007. "Investigating the simultaneous presentation of advertising and television programming." Journal of Advertising 3 (36): 85-96.
21. Chui, Michael, James Manyika, and Mehdi Miremadi. 2016. Where machines could replace humans—and where they can't (yet). Accessed October 13, 2019. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet.
22. Clabiorne, Alejandro, Chris Stephenson, Craig Atkinson, Karine Courtemanche, Klint Finley, Malcolm Devoy, and Mark Holden. 2015. Sentience: The coming ai revolution and the implications for marketing.

23. Clark, Emily. 2019. Alexa, Are You Listening? How People Use Voice Assistants. Accessed October 26, 2019. https://clutch.co/app-developers/resources/alexa-listening-how-people-use-voice-assistants.
24. Coskuntuncel, Aras. 2018. "Privatization of governance, delegated censorship, and hegemony in the digital era: The case of Turkey." Journalism Studies 19 (5): 690-708.
25. Cüneyt, DIrican. 2015. "The impacts of robotics, artificial intelligence on business and economics." Procedia-Social and Behavioral Sciences 195: 564-573.
26. David, Stewart, and Prem Shamdasani. 2014. Focus groups: Theory and practice. Sage Publications.