Academic Paper

Hunter Bishop

Old Dominion University

CPD 494

Professor Akeyla Porcher

April 21, 2023

One problem that we are aiming to address with our innovation is the issue of social media's impact for individuals as well as businesses. Social media has undoubtedly changed the landscape of marketing for companies who are trying to grow their brand or continue to profit off an already established brand. Larger companies will have the ability to engage in more extravagant marketing campaigns that small or medium businesses might not because of the deep pockets the large companies can reach into. Super bowl advertisements, a screen to themselves in Times Square, and more importantly word of mouth are all avenues that are available to large businesses to market their products to the public because of their easy recognizability and, as previously stated, much larger financial reservoir. The number of marketing opportunities for small businesses is significantly lower, however, because they might only have the financial capabilities to get commercials that only air locally and likely have to resort to social media campaigns to get their name out there for others to see. While it can be a great way for businesses to advertise their product and brand, social media also comes with its drawbacks. Larger businesses who might not want to let more competition into their market could decide to try to derail social media campaigns for those smaller businesses trying to enter into the fray. While allowing people to leave constructive criticism for a business in the form of Yelp reviews or Google reviews gives good ideas for improvement and lets other people who are potential customers see what a business might offer, it also leaves room for other companies to take malicious actions to undermine a smaller business who might rely on good reviews and recommendations. Review bombing has become a more popular avenue of slandering rival businesses. Review bombing can be done either by a large coordinated group of people or by one person or organization utilizing bots to leave a multitude of one-star reviews and "avoid"

recommendations which could decrease the potential clientele for a business. Review bombing is commonly done by gamers who want to express their disapproval of what a developer might be doing or the direction they are taking with a game, but it can also be done to businesses just as it happened to Gamer's Nexus, a video game review channel on YouTube. Gamer's Nexus commented on a video that received "the highest immediate influx of downvotes we've ever noticed on one of our videos," which they believe to have been a botnet of accounts made to mass dislike YouTube videos (Moro and Birt, 2022). It is unknown who might have perpetrated the attack on Gamer's Nexus, but it is a prime example of the type of problem we have been looking to solve. The innovation we have proposed is AI monitoring software for social media. We want to design the software to be able to pick up on things like fake reviews or malicious links that might be put in comments on various social media platforms. The main focus so far has been towards businesses, but our product could just as easily be used for individuals and could even be adapted for use by the government. With the AI software, different versions with different filters would be present for users to customize their experience to fit their needs. We would have at least a three-tiered approach which would include an individual package, a small business package, and a package that could be tailored for use by educational institutions. Within each package would also be limited options for customization so that certain filters might be switched on or off. Some of those filters would include making sure a link is legit and is not malicious, ensuring comments are made by actual users of the platform by checking things like account age and comment history, and turning on an option to flag these comments or reviews deemed illegitimate. The likely most logical way of selling this software would be through a subscription basis that could be monthly or yearly. A seven-day trial could also be made available to allow users to try the service out and see if it works the way they would like it to or

if they are willing to go the route of risk acceptance and stay without the service. In any case, customer satisfaction is paramount and we want to create this innovation to help people, primarily focused on small businesses who might struggle to enter into the market.

As I previously mentioned, review bombing is a practice that can cause real harm to small businesses who rely on positive reviews to attract new customers. Local bakeries or floral shops are examples of such businesses who thrive when people rave about them on their own social media account and talk about them with other people. Local businesses also often hold more sentimental value to people who frequent them, which will cause a positive feedback loop of people continuing to prefer these businesses over other brand name corporations. If a larger business were to try to squash their local competition through review bombing, it could cause them to take a hit to their profits and possible lose customers and have to close down. Our AI software would help small businesses like this to protect themselves from things like review bombs, at what we hope to be an affordable price. While we would want the software to be able to flag potentially illegitimate reviews that have been posted by malicious or fake users, we don't want it to simply remove the comments straightaway in case they are a real person who was simply unhappy with the quality of product or service they received at the business they are creating a review of. Reviews from patrons of a business are essential in allowing that business to be introspective and perhaps improve upon the malcontent of their customers to provide a better experience for the whole community going forward (Moro and Birt, 2022). In not outright removing negative comments through the use of our software, it also allows us to indirectly promote self-improvement for these small businesses because, after filtering through potentially illegitimate content and getting to reviews that our AI software has confirmed to be from actual people, the business is able to decide for themselves what they will do with that information. In

the context of growing a business, improving the product or services supplied will undoubtedly serve to bring more customers and allow for more exposure.

In a survey done in 2013, it was revealed that 66% of people who use social media cited one of the reasons they will go on social media is to see about different businesses and what others think of them (Jones et al., 2015). In simple terms, two out of every three people will go utilize social media to see if they would like to become a customer of different products or services. This is quite a large audience for businesses and content creators to cater to. With our software, we aim to support these individuals and groups in their efforts to be successful in connecting with others. Social media is mainly used for connection and 88% of holiday shoppers claimed they used social media to connect with different companies when deciding if they are going to purchase their product or not, and 21% of holiday shoppers said that they first consult social media when trying to find out more about a product (Jones et al., 2015). With so many people going onto social media platforms and looking for accurate reviews on a product, it is paramount that the reviews available to them are actually representative of the product and not filled with reviews created by bots, both negative and positive, because customers want to trust that a multitude of negative reviews indicates a poor product and a multitude of positive reviews indicates a good-quality product. In this case, the AI software we create could help businesses make sure there are not an abundance of illegitimate negative reviews, and could also help a customer make an informed purchase by ensuring there are not a multitude of false positive reviews. Another group of people that this will help are content creators who make their living by giving reviews of different products and businesses. As YouTube and Twitch streaming has increasingly become popular over the last two decades, many people have made a career out of getting in on the ground floor of new products that come out or the release of a new video game

or issue of a comic. These content creators could make use of either the individual package or the small business package depending on the scale of their channel or the scope of who might watch their content. This is another reason that offering multiple packages is essential in the successful marketing of our AI software- to allow for each individual or company to subscribe to the package that fits their needs best. Social media is so widely-used in today's society that we want to help everyone to be able to stay safe in cyberspace while being able to make informed decisions. Many scammers will also put malicious links in comments on Instagram and Twitter that might make it through the platform's own content filters, which is why we aim to design our AI to be able to sniff out malicious links and phishing scams so that consumers do not unwittingly infect their own machines with a virus.

Another problem akin to malicious links are phishing campaigns which are quite simple to perform on social media platforms. Phishing usually comes in the form of an email that appears to be legitimate but has been spoofed somehow and is really from an untrusted source and can cause real damage to a user's computer or mobile device and can even compromise passwords used for important accounts. Scammers can masquerade as a content creator who wants to self-promote their profile and post a link to their supposed profile which could actually contain a redirect to a malicious website or install a trojan. With the AI software that we would make, we would include a content filter that would detect an illegitimate link and block users from even seeing it. If the original poster wants to block anyone from providing links in the first place, we could add an option to be able to delete any comments with a link in the text. Phishing scams are one of the most prevalent forms of social engineering. Statistics gathered by Jain and Gupta show that 2015 was the first year in which the number of unique phishing e-mails reported rose above the one million threshold (Jain and Gupta, 2017). One can only assume that the

upward trend in phishing e-mails has continued up through 2023 and it will only continue to be a problem as the world transitions more processes and business to cyberspace. And as more people use social media more often, malicious actors will begin to enact spear phishing campaigns more often, which is a form of phishing that is targeted at a specific demographic. There is something for everyone on social media platforms, and communities that cater to more niche hobbies and interests are at an increased likelihood to fall victim to spear phishing campaigns. With our AI software, individuals who are aware that they might be at a higher risk of being targeted by social engineering could purchase the software through a subscription and cater it to their everyday web surfing. If they wanted to, the community as a group could even put their money together to get a subscription for the small business version and use it to protect whatever websites they may use, whether it is a Facebook group or a full-fledged web domain. In doing so it could help to warn anyone in the community who may have received an e-mail or direct message that contains potentially unsafe material. A good pairing with the AI software would be a sturdy anti-malware software as well, since we do not want our software to delete e-mails it flags, but rather just warn the user so they can decide how to proceed. The anti-malware would be necessary in case users do decide to look at the email. 95% of phishing attacks result in downloaded malware from something within the email, whether it be a link or an image (Bosetta, 2018). The anti-malware software paired with our AI software's individual package would certainly be an adequate duo in protecting a user during their online activities.

Although we are trying to create something new with our artificial intelligence software, we know that we would not be the first ones to do something along the lines of using AI for protection in cyberspace. Many social media platforms already use some form of artificial intelligence for their content filters to decide what messages to block by default. Twitter, one of

the most used social media platforms, utilizes machine learning to analyze text in tweets to decide what is spam and what is not spam and it has been shown to be quite effective, being able to detect around 70% of spam accounts and messages (Santos et al., 2014). Knowing that Twitter's content filter is quite effective and that it uses a form of artificial intelligence successfully, we would be able to use that knowledge to potentially build upon when we are creating our own artificial intelligence software that could be used to perform similar functions on a wider range of websites and applications. One drawback to this, however, is that when using the content filter function of our own AI mixed with the machine learning content filter from Twitter or other social media sites, we might find that there is still a cap in effectiveness of the filters or even that they cause further issues with being able to see tweets or posts that should not be filtered out but are. This would be something we would have to consider when we design our product and also something we might put into the SLA so that consumers are aware of the possible problems that could be encountered. I have put a focus on individuals using Twitter here, but small businesses also make use of Twitter, being such a popular social media platform. We would want to make sure that our artificial intelligence does not cause problems in being able to reach their customers or garner more exposure for themselves, while still trying to increase security from phishing scams and other social engineering tactics. As mentioned by Santos et al., spam is not only bothersome but also a potential security risk which continues to cost businesses billions of dollars collectively (Santos et al., 2014). Small businesses can be financially ruined by even just one unfortunate incident, so purchasing software that will help to increase security and perhaps cover up where employees might slip up and fall for a phishing scam would be a valuable asset in financial security. And as we work on our own product, we might continue to improve upon the machine learning that Twitter uses for its spam filter and eventually attract

more attention to the issue as a whole. Doing so would allow more people to become aware of the issue and likely draw more brilliant minds to the cause to help make cyberspace more secure; although we want to help with our innovation, the overall goal of any cybersecurity professional, and any morally concerned entrepreneur, is increasing safety for the public and facilitating the advancement of society.

While this product is designed for use at an individual or small business level on a subscription basis, we hope to be able to design the software so that it is elastic and can be adapted for more large-scale use. One of the largest scales our software is a government level agency making use of the product. As stated, while the main focus will not be large scale businesses or the government, we do not want to close off avenues of growth for ourselves. The ultimate goal is for this software to be used to help people and facilitate making cyberspace more secure, so if being able to adapt our product for government use is a way to do that, then we would certainly want that ability. The problem with making our technology available to the state is that we aren't always sure what they might use it for. Additionally, it is likely that the government already makes use of similar tools for monitoring social media and may have no need for our artificial intelligence in the first place. The National Security Agency is even able to gain access to personal data held by companies based in the United States, so monitoring up front might be redundant when the agencies can just go to the communications companies that store the data themselves (Brown, 2014). If the opportunity were to arise for us to adapt our software for government or law enforcement use, one thing we could adapt is the artificial intelligence's ability to decide what comments and posts are made by legitimate users. In the same way it is able to tell apart real from fake, we could input certain phrases or keywords that the AI would send alerts for such as threats people decide to post on social media. This would

allow law enforcement to take preemptive action and be out in front of any possible criminal activity. Mateescu et al. find that law enforcement agencies utilize social media platforms for a variety of reasons from surveillance over individuals or groups they suspect are likely to be involved with a crime to using social media account details and posts to gather evidence on someone for a trial, given that the posts are public and the account has not been set to private (Mateescu et al., 2015). With the artificial intelligence software we intend to develop, police departments and other law enforcement agencies could be even more effective in trying to stamp out crime before it happens. With a subscription plan, the cost of the software license would be affordable for the department to use and it would allow them to unsubscribe at any point if they feel that the software is no longer necessary. We could additionally develop a private cloud for the department to use so that they are able to store the data without having to worry about local storage, and it will allow for easier backups to our own system so they are able to continue their investigation in case the software fails locally. This would serve to make entire communities safer if our product is successful in reducing crime. Indirectly, this would serve our original idea of catering to small businesses and individuals, because small businesses tend to fare worse in the wake of criminal activity whether that is a cyber-attack, which can cause complete financial ruin, or a physical crime like a break-in, which can sometimes be a hefty financial burden in repair costs and lost revenues due to time shut down for repairs. As crime decreases, it will allow for these small businesses to experience more prosperity and, as studies show, economic growth breeds more economic growth and will allow small businesses to better protect themselves from criminal activity (Islam, 2014). So, if by adapting our software for use by law enforcement we are able to reduce crime in communities, it will make cyberspace and the real world safer for individuals and small businesses.

In determining whether or not our innovation is effective, we will likely have to take a look at multiple different sources of information. One of the most effective ways of determining how our product works is, coincidentally, something that our software aims to protect- customer reviews. When we gain a new subscriber, be it an individual or a business, we would send a survey along with the software license for them to do before they begin using it. After a certain period of time, perhaps a month or a quarter, we would have an automated email set up to send with a post-survey that the individual or the users affiliated with the business using our product would fill out with the same questions as the pre-survey so we could compare the difference on our end. Some questions we could ask would be about confidence in ability to recognize fraudulent messages from real ones, the frequency of spam getting through email or social media content filters, and quality of interactions on social media platforms. We could see how our software is helping our subscribers, or also how we might not be helping enough or in certain ways. A way of determining product success specifically for new businesses would be to measure the number of flags that our software has sent regarding social media communications with the small business, and look at how many of those flags the users at the business marked as true and how many were marked as false positives. We would use that ratio and aim to get to a false positive ratio that is superior to other products on the market, because that will make our artificial intelligence more attractive to potential customers when they compare it with other companies. Additionally, we could ask if willing businesses who use our product and are satisfied with its performance would make a social media post or a shoutout on their website mentioning our product so that we could gain more exposure and broaden our own client base. Overall, most of our measures of initial success will be qualitative rather than quantitative because of our focus on customer satisfaction and increased security.

One connection that our product has to a class I have taken outside my major of cybersecurity is my Philosophy 355E class. In this class, I was required to study the perspectives of multiple different philosophers, both modern and not-so-modern, and take on one of their viewpoints to argue for or against different issues. One of the essays I had to write was about corporate social responsibility, which Investopedia defines as "a self-regulating business model that helps a company be socially accountable to itself, its stakeholders, and the public" (Fernando, 2022). Our artificial intelligence software ties into this quite well because it would be a tool that businesses can use to be more socially responsible. With the filtering components we would have available through the AI, it allows the businesses who subscribe and use our product to make sure their social media is filtered from illegitimate content and that they are able to put forth a quality website or a quality social media profile that others can trust is authentic. Corporate social responsibility means that businesses are taking on the role of a custodian of accountability and ensuring authenticity as well as cybersecurity on their end is a quintessential way of not only securing their own business but also attracting more customers and gaining a good reputation. In regards to one problem we are attempting to fight against, which is the struggle small businesses might encounter when trying to break into the market, I took a class called STEM 251G which was about computer information literacy. Information literacy and being technologically savvy are two skills that are valuable for small businesses to utilize. While our software might not teach information literacy directly, it can aid in helping users learn what kind of things to be wary about and will teach telltale signs in determining if information can be trusted and if online profiles are authentic and able to be trusted. When users make use of our content filter option, they would be able to see what kind of information or text pattern gets flagged and, even if some turn out to be false positives, they can be used as examples to go by in

the future when they might be looking at information that our software has not evaluated or maybe that they are seeing in real life. A third class that I have taken that our product relates to is Criminology 215. Criminology 215 is an introductory level criminology class that focuses on the motivations for crime and the risk factors for victims as well. In creating an artificial intelligence that will be capable of mitigating risks for individuals and businesses alike, these are two of the things that would be significant to look into. Of the two, risk factors for victimization are the more pressing issues, since we are not always sure what kind of malicious actors we would be trying to combat. But if we can help mitigate the risk and lower the surface area for attack, then that will go a long way in making our innovation successful. We could include precautions against more common types of attackers, namely opportunistic attackers who tend to seek out vulnerable websites or servers to launch their attacks against. And Criminology 215 would be an especially pertinent resource of knowledge if we were to seriously consider developing our artificial intelligence to have the capabilities that law enforcement would find necessary. I learned from Criminology 215 that oftentimes, criminals are not particularly adept at hiding their tracks and will leave some trace of how and why they might have perpetrated their crime. By looking at these "how's" and why's", we might be able to change our software accordingly depending on an organization's needs, location, target demographic, and budget among many other factors. IDS 300W is also a class that is relevant to our innovation. IDS 300W is an interdisciplinary research class which taught me how to take information and ideas from multiple different, sometimes unrelated, fields of study and organize them into a coherent argument. With our artificial intelligence software, we would be bridging the gap between cybersecurity, computer science, and business as well as potentially criminology/law and

marketing. In doing this, we have had to connect our ideas in a coherent manner and ensure that our work will make sense to readers and viewers from different academic backgrounds.

Turning our idea for this artificial intelligence into a reality is easier said than done. As somebody with a few years of background in computer programming and coding, machine learning and artificial intelligence is still well out of my area of expertise and even comfort. But this comes with a silver lining: although finding and hiring a team of people to work on an artificial intelligence project can be quite costly, nobody is really starting from scratch. In today's world of technological excellence, "Square One" continues to advance forward in the process. Software developers no longer have to create artificial intelligences from the ground up, but rather they have at their disposal a wide range of examples from which to learn and open-source materials to pull from. But nonetheless, creating a complex AI software takes a team of highly skilled developers to pull off, so that is one thing that will be paramount to the success of this project. Another thing that goes hand-in-hand with the previous point is money. We will need financial backing from investors who have faith that this project would be worth their money and trust that it will be successful. We would have to come up with some convincing pitches to these investors and show them that this is different than other similar products on the market and that we have the potential to go above and beyond what is already out there to attract customers. Additionally, we would want to talk to people and businesses who we believe might be interested in the software we are making to try to get some potential clients onboard with our idea from the get-go. We would also want to poll businesses and anyone who might use this artificial intelligence to see what kind of capabilities they would desire it to have. Doing so would allow us to continue to narrow down how we want the software to be developed so that we are likely to get sales to start off. Since we are focusing on small businesses and individuals,

we would want to make sure our software is affordable for that demographic; we would need to come up with a subscription plan, likely with multiple packages to choose from as I had suggested previously, that will be fairly priced but also enough so that we are able to make profit but also to show our investors and the public that we are confident in our product and its potential. In creating any sort of software to be released for sale, we would need to patent it. While there are similar machine learning programs or artificial intelligence software out there, each one has uniquities put in by the developers to make them stand apart from their competitors. We would have to do something similar and make sure we are coming up with a fresh spin on artificial intelligence that has not been exactly done before so that we can be granted a patent. Along with legal documents, subscriber-based software need to have a service-level agreement, or SLA, to outline the proper use and handling of the software by the user and provide contact information in case of any problems or questions that might come up. And finally we would need to create an effective advertising campaign along with a brand and logo so that we are able to gain memorable exposure through social media, word of mouth, and an eye-catching website. This would probably require us to have someone dedicated to running a social media account and/or website for the brand we choose to represent our product. All of these things – investors, interested buyers, a talented development team, proper legal documentation, advertising, etc. – would need to come together to make our innovation a reality. Creating something new as an entrepreneur is more than just the creation process, but it is also the process of marketing our product, ourselves, and our brand so that we do not just get a few sales and then fall away because we don't have an effective marketing system. Another key component that will be necessary for success is the right attitude. It is highly unlikely that our product would succeed on take one. It will probably take multiple tries over an extended period of time to work out bugs

from the program, find an adequate number of investors, find enough potential customers to get us off the ground and more. But failure is a part of learning how to grow and how to do things better the next time around.

The major thing I learned from this project was that entrepreneurship is probably not for me. I understand how the process of entrepreneurship can be enticing for many people, but I would rather be a part of something instead of leading the charge. I want to be able to fly under the radar and work behind the scenes and feel accomplishment from afar and not in the limelight. Piggybacking off of that, I learned a little bit more about myself going into my career. At the moment, management doesn't sound like my forte, and that is not a bad thing because it has shown me a possible area of improvement for me. I know I am still young and my opinions and perspectives will undoubtedly change throughout the course of my life, so one day I may want to be a supervisor of some kind. But in doing this project, I think I would rather be a cog in the machine and not the conductor. Another lesson that I did not learn for the first time in this project process but rather that has been reinforced is that success and failure are not black and white. Success is not always good and failure is not always bad. Someone might be successful financial but corrupt morally, so can their success really be called a good thing? Similarly, failure might yield negative results in the short run, but if I am able to learn from the mistakes I made and figure out how to do something better, then failure was just another stepping stone towards success. If I were to have done something differently along the way, I would probably have been more meticulous with my work. I take medications for both ADD and anxiety, but some days they are not as effective as others. I need to realize when I am having good days where my symptoms are less severe and take advantage of that time where my mind is most clear and most

active so I can do my best work. I just need to continue learning about myself and remembering to control the things I can control, and control my reactions to the things I cannot control.

References

Bossetta, M. (2018). THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY. *Journal of International Affairs*, *71*(1.5), 97–106. https://www.jstor.org/stable/26508123?seq=7

Brown, I. (2014). Social Media Surveillance. *The International Encyclopedia of Digital Communication and Society*, 1–7. https://doi.org/10.1002/9781118767771.wbiedcs122

Fernando, J. (2022, May 27). *Corporate Social Responsibility (CSR)*. Investopedia. https://www.investopedia.com/terms/c/corp-social-responsibility.asp

Islam, A. (2014). Economic growth and crime against small and medium sized enterprises in developing economies. *Small Business Economics*, *43*(3), 677–695. https://doi.org/10.1007/s11187-014-9548-6

Jain, A., & Gupta, B. B. (2017, January 10). *Phishing Detection: Analysis of Visual Similarity Based Approaches*. Hindawi; Hindawi. https://www.hindawi.com/journals/scn/2017/5421046/

Jones, N., Borgman, R., & Ulusoy, E. (2015, November 16). *Impact of social media on small businesses*. Emerald Insight; Journal of Small Business and Enterprise Department. https://www.emerald.com/insight/content/doi/10.1108/JSBED-09-2013-0133/full/html?journalCode=jsbed

Mateescu, A., Brunton, D., Rosenblat, A., Patton, D., Gold, Z., & Boyd, D. (2015). *Social Media Surveillance and Law Enforcement*. https://datasociety.net/wp-content/uploads/2015/10/Social_Media_Surveillance_and_Law_Enforcement.pdf

Moro, C., & Birt, J. (2022, August 17). *Review bombing is a dirty practice, but research shows games do benefit from online feedback*. The Conversation.

https://theconversation.com/review-bombing-is-a-dirty-practice-but-research-shows-games-do-benefit-from-online-feedback-188641

Santos, I., Igor Miñambres-Marcos, Laorden, C., Patxi Galán-García, Aitor Santamaría-Ibirika, & Pablo García Bringas. (2014). Twitter Content-Based Spam Filtering. *Springer EBooks*, 449–458. https://doi.org/10.1007/978-3-319-01854-6_46