Scott Hirabayashi
DATA605

The Ethics of Online Law Enforcement- An Exploration of Preventative Strategies

Introduction

Earlier this year, the National Center for Missing and Endangered Children (NCMEC) reported a 98.66% increase in online enticement reports between January - September 2020 versus the same time period in 2019 (O'Donnell, 2020). Frighteningly, with the disruption of Covid, 2020's accelerated movement towards a stay-at-home model has seen a significant increase in the frequency of such malicious online activity, particularly on social media. Now more than ever, it is incumbent on law enforcement agencies to look for innovative solutions for protecting vulnerable populations.

Case Study: Maryland State Police and New Social Media Strategies

In response, the Maryland State police are exploring several ideas in order to counter exploitation of minors and vulnerable populations. In consideration are four strategies: a) created fake profiles on many popular social media sites to look for bad actors, b) employment of "ethical hackers" to access known social media forums, platforms and websites which have been proven to host inappropriate content and allow for the victimization of individuals, c) requests for foreign intelligence services to access U.S. servers without judicial authorization to provide data in the search of online predators, and d) the hiring of local universities to have its graduate data science students build an artificial intelligence application to further help find online criminals using the data it has collected.

Each strategy comes with impactful considerations on possible usage. This review will critically analyze each strategy in regards to its utilization and potential issues. Following the analysis of each strategy, this paper will ethically analyze each of the strategies through the workable ethical theories of Kantianism, Utilitarianism, Social Contract theory, and Virtue Ethics.

Strategy A: Usage of Fake Social Media Profiles by Law Enforcement

Usage of fake profiles by the general population is common- an analysis by Statistia (2020) revealed that about 11% of social media accounts on facebook were duplicate, and 5% were fake, accounting for millions of profiles. Law enforcement and governmental officials have begun to utilize social media platforms in the interest of information collection against bad actors. Maryland State Police's decision to use fake social media profiles would not be out of line with recent developments in the governmental use of social media. Recently, the Department of Homeland Security moved to begin collecting data in the realms of illegal immigration by way of social media. In a major policy change, the Department of Homeland Security asserted, in uses of Fraud Detection and National Security, "FDNS may use fictitious accounts or identities for social media research when necessary" (Hawkins, 2019).

However, strict limits must be placed on law employment's usage of fake social media. Sometimes lacking a clear directive, law enforcement has used the tool as a form of information collection for those who are not in the process of committing crimes. In the case of activist movements such as Black Lives Matter, the Memphis Police created and collected information through usage of fake social media profiles, an action that arguably broke Memphis law agreements that had been in-place with law enforcement. Claims against these intrusive actions were that previous laws had protected citizens from political surveillance by law enforcement, which fake social media accounts by undercover police largely ignored (Noori Farzan, 2018).

Additionally, such efforts have breached contractual terms of service and raised the attention of social media companies such as Facebook.The platforms themselves explicitly dissuade against the usage of fake social media accounts for such purposes, and have responded by speaking out against future usage of fake social media profiles on its platform by law enforcement (Kirkpatrick, 2018).

Strategy B: Utilization of Ethical Hackers To Protect Against Vulnerabilities

Addressing the second consideration, the Maryland State Police could employ ethical “white-hat” hackers to counter the incursion and dangers presented by malicious “black-hat” bad actors. These ethical hackers could work to identify and protect the vulnerabilities of data and platforms that could lead to online exploitation. And these vulnerabilities are particularly evident for individuals; according to Watkins (2018) “Government actors like the NSA have an established practice of stockpiling vulnerabilities rather than helping vendors remedy them. This approach is highly effective at achieving national security objectives and at committing lucrative cybercrime, but is not effective at protecting individual consumers or companies”.

There is a definite need for knowledgeable actors to search and protect against the vulnerabilities of the individual consumer. In particular, children are easily targeted and exploited by bad actors, and be taken advantage of with use of their collected data. In the case of social media websites, which also contain vulnerabilities to attack, white-hat actors could have a significant impact at protecting against bad actors against data leaks or security flaws.

One caveat lies in the uncertain delineation between white-hat and black-hat hackers. Notable U.K. hacker Marcus Hutchins faced serious criminal charges in his alleged creation of the Kronos malware, despite years-later working as a white-hat hacker to play a major role in the prevention of the devastating WannaCry virus (Wiedeman, 2018). A bad-actor-turned-good, Hutchins highlights the difficulty in determining how to judge the actions of hackers, as well as considerations for employing such hackers. In such cases, it is very difficult to understand and ascertain motivations and intentions of the actor, making it difficult to fully trust them, and create incentives for their help.

Strategy C: Foreign Intelligence Access and Data Sharing

Bad actors who engage in online exploitation are not confined to local or regional borders. Predators of vulnerable populations can remain anonymous and global, making them increasingly difficult to find and prosecute, and there is great need for recognition of bad actors outside our borders. Were Maryland to take up such actions, they may be improved in certain areas. For Maryland State Police’s usage and allowance of foreign intelligence to access US databases for criminal information and data, this strategy should be seen as a collective agreement across countries. In effect, a two-way street between law enforcement agencies across the world. Eoyang et. al (2018) state the importance of international cooperation, "Effective engagement with other countries on cyber threats requires a coordinated international effort as we make catching cybercriminals a top priority for the United States."

Eoyang et. al (2018) state three primary strategies in terms of international cooperation. First, an "Ambassador-level armchair quarterback", where diplomacy on shared data led by a national governmental body that could provide guidance and supersede the Maryland law enforcement body. Second, "Stronger Tools in the Diplomacy Arsenal", which addresses Maryland's stated hope for data sharing with other international entities and law enforcement bodies that currently struggle with issues of red tape. Thankfully, the creation of policies to improve international cooperation has already begun, such as with the CLOUD act, which allows direct access of countries to access company data, as well as raising standards for civil rights. The third consideration by Eoyang et. al state is, "Better International Capacity for Enforcement", which requests expansion, funding, and the creation and clarification of international data laws, a particular need at present time.

Maryland's choice of data sharing without requirement of judicial approval, for foreign intelligence could be understood as a cooperation between parties, a sharing of data in order to track data about online predators. With cooperation through treaties and allowances, it might forgo traditional issues encountered through judicial branches, treaties, and the slower speed of bureaucracy in order to expedite the protections against online exploitation.

Strategy D: The Creation of AI Applications to Algorithmically Prevent Crime

The last strategy consideration that the Maryland State Police have is the employment and usage of an AI-powered application created by an outside entity to additionally identify crime. Of the aforementioned strategies: A and B, data could be taken and utilized from each source or agreement in order to build an application by private or public entities to further assist in fighting online predation of children or the vulnerable. An AI application built with an algorithm, might detect those who were flagged as at higher likelihood of committing crimes.

While it could have very positive utility in preventing cases of future online exploitation, it assumes that the data is sound and the algorithms come with no bias. However, the reality is that many algorithms are plagued with issues of bias. Issues have surrounded the usage of facial recognition technologies, which have issues with pattern detection of certain races and genders (Singer, 2019). Moreover, Silva and Kenney (2018) found that bias persists in many stages of algorithmic law enforcement. Strikingly, they write "The studies of algorithmic decision making in activity such as criminal sentencing, deciding probation, and even deciding whom the police should stop have repeatedly shown that it leads to biased outcomes". Essentially, at every step of the process of algorithmic creation, there was a threat of bias.

Of specific danger for this project, a project limited in data sources, are issues regarding predictive policing strategies that lead to feedback loops. As Silva and Kenney (2018) describe, "Similarly, for things like predictive policing, when police officers go into a neighborhood to find crime, they find crime. This raises the crime rate of the community, leading to the dispatch of more police, who make arrests, initiating a self-reinforcing feedback loop" (p. 25). In these cases, law enforcement might be directed to communities where some online exploitation is present, overly emphasize and target a specific community, yet miss on warning signs from those outside of the community. Thus, particular attention must be placed on using a variety of data sources and strategies to prevent bias, or creating cycles of bias, in the case of algorithmic applications for fighting crime.

Ethical Look: Kantianism and Utilitarianism

Kantianism runs on two categorical principles: first to “act only from moral rules that you can at the same time will to be universal moral laws”. Second, to “act so that you always treat both yourself and other people as ends in themselves, and never only as a means to an end” (Quinn, 2017, pp. 68-69). Do each of these strategies follow these values? For the first imperative, each strategy would struggle to be generalizable, as each has significant downsides under certain circumstances, as previously mentioned. For example, it would be difficult, under Kantian ethics, to assert that to prevent exploitation, law enforcement should be able to make any social media profile at any time, in order to chase after a suspect. However, of greater note is in the second categorical imperative, where each strategy encounters a greater problem- the imperative that people may not be used as a means to an end. For strategy A, it would be difficult for law enforcement to create fake accounts for information gathering that did not unwittingly involve other people.

Strategy B’s Ethical hackers could be unwittingly endangering or revealing the data of vulnerable persons, and we would be placing great trust in the hands of actors who may or may not be acting in our best interests. Strategy C’s exposure of data to foreign intelligence would need to ensure that only the data of suspects were targeted in data sharing, yet it seems very likely that data sharing would include innocent actors as well, unintentionally using innocents as a means. Finally, any algorithm, as employed in strategy D, that looks for patterns of data present in bad actors would require the usage and data of good actors as well, thus using them as a means to an end as well; moreover, the data taken from strategies A and B, if unethical, would make the usage of the algorithm they are based on unethical as well.

In contrast, utilitarianism is consequentialist- is there a net utility that we can obtain from utilization of each of these strategies? Specifically, utilitarianism focuses on utility “the tendency of an object to produce happiness or prevent unhappiness for an individual or community” (Quinn, 2017, p. 72). The primary question then, is whether the utility of each strategy could be seen to outweigh the downside. For strategy A, fake social media profiles are already in use by government officials and police departments in countering crime. So long as it did not additionally infringe or endanger lives, it could be seen as ethical from a utilitarianism perspective, so long as it can prove it is somewhat effective in stopping child exploitation and crime.

For white-hat hacker employment, it is additionally difficult to ascertain whether or not they could play a beneficial role; if most of the hackers were suspected to act in the best interest of law enforcement officials, it could be net-beneficial in protecting the data and information of the vulnerable populations. With regards to the sharing of foreign intelligence, Eoyang et. al (2018) state their belief in the great benefits that law enforcement might have with cooperation, thus, specific sharing of data that could lead to criminal prosecution of bad actors would have positive utility. Finally, an algorithmic program, if the data collected were valid and unbiased, and if the program were to be successful at identifying bad actors, could have net positive utility, though they would depend on not encountering any issues with strategies A and B.

Ethical Look: Social Contract Theory and Virtue Ethics

The social contract theory focuses on the importance of a contract, an agreement between parties. In this case there are multiple competing contracts- first, the rights of the individual, and next, of the rights of the companies and law enforcement. In terms of the government, primarily in the 4th amendment of the United States Constitution, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". In the case of fake social media profiles, as previously mentioned, there were issues raised as to how data collected on political parties was breaching previous rights. Moreover, there is a contractual agreement with social media companies that is additionally not being withheld; thus, fake social media profiles would be unethical. In the use of ethical hackers, law enforcement's employment of them would similarly break the expected contract between citizen and law enforcement: we trust the police to protect us from vulnerabilities. White hat hackers are looking and attempting to break into supposed vulnerabilities in systems, which would breach contracts of privacy, security, and personal protection.

In terms of foreign intelligence data sharing, this could be seen as an overreach of power on the 4th amendment. It is one thing to collect data from within a country, but another thing altogether to have it shared- our social contract is with our government, not with foreign governments outside of the United States. We should not be expected to be held accountable for laws of other countries if we have not broken laws outside of the country, thus the sharing of data and information on actors within the United States to countries outside of it should be considered to break the social contract. Finally, in terms of algorithmic creation of- if the data collection from fake media profiles, information sharing, and white hat hackers was unethical, any use of this data within an algorithm would make the utilization of an AI program unethical as well.

Virtue ethics values the importance of one's virtues- either moral or intellectual virtues (Quinn, 2017, pp. 88-89). In the case of the use of fake social media profiles, the Maryland State Police would be employing a form of deception to gain information. Truth is a common virtue in many societies; thus, ethically, it is wrong to deceive- the strategy is unethical. Similarly, the employment of ethical hackers, who search and attempt to exploit and test vulnerabilities in order to ultimately protect the populace, could be seen as unethical because we are employing those who may be acting to stop others.

Sharing information with foreign governments, at face value, it would not appear to be unethical. International communication and cooperation towards a common goal includes virtues of friendship and goodwill, as a collaborative and shared effort towards assisting fellow governments in their own battles against online exploitation. However, it also breaks faith with the American citizen, as there is an expectation that data would not be shared without prior knowledge or, at least, judicial approval. Thus, it may be seen as unethical if citizens were not expecting it. Lastly, the use of AI applications to algorithmically prevent crime could also be considered ethical at face value, though only if the data was fully bias-free, which, at present appears to be an impossibility. If rolled out as only a working (and improving) algorithm, virtue ethics suggests that it would be unethical because it does not treat people fairly, breaking virtues of fairness and equal treatment.

Conclusion

Maryland State Police’s exploration of ideas to counter online exploitation appear to be done in good faith, but each encounters ethical issues under the different ethical theories. In the hopes to curb the spread of online exploitation of children, each proposed strategy comes with inherent risks and a challenge to the current understanding of an ethical ‘right’ for policing and protection.

It should be incumbent on law enforcement and government officials to provide and detail specifics on exactly how, and in what way these strategies might be used, so that the public can gain a greater understanding of whether or not to support them. Ultimately, the issues presented in this paper may hopefully shed some insight into focus and improvement areas for the future.

Works Cited

Agan, A. Y. (2011). Sex offender registries: Fear without function? *The Journal of Law and Economics*, *54*(1), 207–239. https://doi.org/10.1086/658483

Eoyang, M., Peters, A., Mehta, I., & Gaskew, B. (2018). *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*. Third Way; JSTOR. https://doi.org/10.2307/resrep20153

Hawkins, D. (2019). *Privacy Impact Assessment Update for the Fraud Detection and National Security Directorate*. U.S. Citizenship and Immigration Services. https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-013-01-fdns-july2019_0.pdf

Infographic: 16% of all facebook accounts are fake or duplicates. (n.d.). Statista Infographics. Retrieved October 24, 2020, from https://www.statista.com/chart/20685/duplicate-and-false-facebook-accounts/

Kirkpatrick, A. (2018, September 24). *Facebook letter to memphis police department on fake accounts*. https://www.eff.org/document/facebook-letter-memphis-police-department-fake-accounts

Mateescu, A., Brunton, D., Rosenblat, A., Patton, D., Gold, Z., & Boyd, Danah. (2015). Social Media Surveillance and Law Enforcement. *Data & Civil Rights: A New Era of Policing & Justice*, 11.

Noori Farzan, A. (2018, August 23). *Memphis police used fake Facebook account to monitor Black Lives Matter, trial reveals*. Washington Post. https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/

O'Donnell, B. (2020). *Covid-19 and missing & exploited children*. National Center for Missing & Exploited Children (NCMEC). https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children

Quinn, M. J. (2017). *Ethics for the information age* (7th edition). Pearson.

Silva, S., & Kenney, M. (2018). Algorithms, platforms, and ethnic bias: An integrative essay. *Phylon (1960-)*, *55*(1 & 2), 9–37. JSTOR.

Singer, N. (2019, January 24). Amazon is pushing facial technology that a study says could be biased(Published 2019). *The New York Times*. https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

Watkins, J. (2018). No Good Deed Goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and "White Hat" Hackers. *MINN. J.L. SCI. & TECH.* , *19*(535 (2018)). https://scholarship.law.umn.edu/mjlst/vol19/iss2/7

Wiedeman, R. (2018, March 6). *Does a hacker hero always have to have a past?* Intelligencer. https://nymag.com/intelligencer/2018/03/marcus-hutchins-hacker.html