

Brian Temu.

Professor Jennifer Esworthy.

DATA 605 Ethical and Legal Issues in Data Science.

29 October 2023.

Ethical Assessment of State Police Strategies in Combating Online Predators

The internet age has created numerous activities that individuals participate in, making the world a village. Such activities may include the online exploitation of minors. Child exploitation is an act of taking advantage of a child for monetary gain. This is subjected to criminal or sexual exploitation such as coercing/blackmailing children for sexual purposes, consuming child sexual abuse materials, engaging a child in sexual acts in chats, grooming by adults, and sharing indecent images of children (“What is online child sexual exploitation?”). In a 2021 national study for young adults aged 18 to 28 years, they were asked about their childhood(<18 years) experiences of “online and technology-facilitated abuse” The results were as follows: “15.6%; image-based sexual abuse, 11.0%; self-produced child sexual abuse images, 7.2%; nonconsensual sexting, 7.2%; online grooming by adults, 5.4%; revenge pornography, 3.1%; sextortion, 3.5%; and online commercial sexual exploitation, 1.7%”(Finkelhor et al.). Technology such as social media has made it easier for predators to target minors and hide behind their screens. There have been strategies that are established to track down these predators such as using fake profiles to look for bad actors, employing ethical hackers to access platforms and websites that predators use, foreign intelligence services to access U.S servers to provide data on online predators without judicial authorization and help from local universities to create artificial intelligence from the data collected. This paper will discuss the ethical issues related to these strategies and use ethical theories to assess them respectively on the continued use of the data collected.

Fake Profiles, This is an act of creating an online account by pretending to be someone else. Using this the authorities can pretend to be minors so as to identify predators on the platform. These platforms can be online games with chats or social media. The creation alone of these accounts isn't illegal but the action done with these accounts might be such as identity theft, harassment, fraud, and exploitation of minors. The creation of fake accounts violates the social media platform rules. A good example is Facebook which states in their community standard that

every individual should only have one account and having multiple accounts goes against it (Trapnell). So this rule also applies to the State Police and they should be accountable for that. Looking at the act it is wrong to pretend to be someone else, falsifying someone's identity may cause a loss of trust in the platform. This can be improved by filling a court and social platform permission for deploying these fake profiles. Using consent images and info when setting up the profile. Most importantly create a set of actions or procedures that will classify a profile as an online predator.

Using relativism it is subjective on whether the data should continue to be used. I would say that data that comes from the use of fake profiles should be used even though it violates the guidelines of some platforms. With ethical egoism it is in our own best self-interest to catch these online predators therefore the data collected from using fake profiles should be used because, at the end of the day, it's to make society safer. Using the great happiness principle in Utilitarianism the actions of using this data from fake profiles is acceptable because reducing the presence of online predators increases the total happiness of this mission of catching them. The first formulation of Kantianism "Act only from moral rules that you can at the same time will to be universal moral laws" doesn't support the use of this data from fake profiles. By accepting this as the universal law it will make people not be themselves and zero trust of profiles on social media.

Ethical Hacking is a process that "involves an authorized attempt to gain unauthorized access to a computer system, application, or data" ("What Is Ethical Hacking and How Does It Work?"). Done by hackers to identify vulnerabilities that can be resolved before exploited by malicious attackers. Ethical hackers have been used to access servers, websites, and online private chat rooms that are engaged in child exploitations to identify these predators. It is unethical to access these platforms without proper approval for this action to be legal and go beyond the defined scope by accessing sensitive data that doesn't have legal approval. This violates users' privacy on these online platforms. It has proven to be effective in catching on predators For instance, "in October, three Californians were collectively sentenced to 60 years in prison for running the so-called Orchid Club, an international service that used the Net to distribute child pornography to its members ("Hacker group battles child porn"). This is an efficient strategy that can be improved by having approval before conducting a hack, remaining

within a defined scope of the search, and respecting and protecting the privacy and sensitive data of other users.

By assessing ethical hacking to be subjective in this case I think it is the proper way of trying to catch these predators and I support it. It isn't against the law and it's done within proper approval and scope. Virtue ethics does not support this strategy and the data collected shouldn't be used, a virtuous person won't access the private chats of an individual without their permission even though they have legal approval from both the government and the platform. Using ethical egoism, the self-interest of state police is to catch these predators meaning if using ethical hackers does the job it's the right strategy to go with. Act Utilitarianism leans on "an action is good if its net effect (overall affected beings) is to produce more happiness than unhappiness"(Quinn). This theory supports this strategy and the use of the data collected from it because the action of using ethical hackers will catch online predators and will try to make online a fast environment. Therefore the overall happiness is high compared to the consequence of the action. Kantianism's second formulation "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) does not support this strategy and the use of the data from it. It's morally wrong to look at private conversations of users on a platform that upholds privacy.

Foreign intelligence refers to "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" ("50 USC 3003: Definitions"). Some examples of intelligence agencies are the Central Intelligence Agency(CIA), Foreign Intelligence Service(SVR RF), Secret Intelligence Service known as MI6 and the Defence Intelligence Organisation. It is wise to solve international online crimes with assistance from foreign intelligence agencies with consent from the government. It is morally wrong and illegal to access United States Servers without judicial authorization. This action violates the privacy of the users and the sharing of sensitive information that may not be needed in the investigations. Sharing foreign information has proven to catch online predators. In 2012 an international operation was able to identify fifty-five individuals using social networking groups that exchanged child pornography and six individuals identified were living in the United States this information was forwarded to twenty countries where the targets are living ("International operation targets online predators using social networking sites"). This enabled them to catch the predator by intelligence services working

internationally together. This strategy can be improved by the state police asking for legal authorization from the government to access the servers, presenting the scope of the search and how the data will be used. With this set of rules, I think the strategy will help in combating online predators globally.

Applying subjective relativism using foreign intelligence to access United States servers without judicial authorization is morally wrong and illegal. The State police should not use this strategy and the data collected from it. Cultural relativism points out the same, that it is illegal in the United States what the State Police did. The first formulation of Kantianism “Act only from moral rules that you can at the same time will to be universal moral laws”(Quinn) doesn't support this strategy. This strategy will violate the data privacy of all users online if their data can be accessed in that way. Using Virtues Ethics state police strategy is wrong and a virtuous person wouldn't act in that way. Because they have broken the law and affected the privacy of other users. Therefore this data should not be used in any means. Act utilitarianism supports the State Police strategies because the total happiness of saving children online from predators is what at least everyone wants even though it means violating the privacy of those predators. Rule Utilitarianism says differently about this strategy and doesn't support it. As a universal law corporations or businesses won't be able to protect users' data violation from foreign intelligence therefore the continuation of the data collected should stop.

The strategy of hiring graduate students from a local university in order to create an artificial intelligence application has some ethical issues. First, the state police are exposing sensitive data that contain personal data of individuals to students who may have no clearance to view in the first place. Second, exposing such data may lead to data leakage and cause people to take action on their own. At this point that data has leaked and it is publicly available that may alert the online predators and make them cover up their tracks and make the whole operation fail. Also, graduate students aren't professional on this matter so they can create a biased system or poorly constructed system that may deceive prediction of online activities. The strategy can be improved first by assigning a professional lead who will oversee the project. Second, select outstanding graduate students who will be working on the project with security clearance. And third, creating a secure data pipeline that can be accessed by special programs and laptops that are monitored 24/7. This will try or eliminate the ethical issues just discussed above.

Assessing the local university strategy using Act Utilitarianism there is no harm created in making this system, only the possible risk that exposing such kind of data may lead to data breach. But the overall total happiness is to catch the online predators and this is the main focus that Act Utilitarianism supports this strategy. Being subjective to the matter I think the state police should take precautions on exposing this kind of data to students because it may lead to data breaches. So I don't support this strategy at all because students are not professionals in such fields. In Kantianism's second formulation students are used as a means to an end of catching these online predators. This formulation does not support this strategy because students are used as the means to catch these online predators. Rule Utilitarianism doesn't support this strategy because if this is a universal practice it may have the potential to expose online predators during investigations due to breaches and cause chaos. Ethical Egoism is focused on the self interest and the main interest of the state police is to catch the online predator. So if using local university graduate students' artificial intelligence applications proven to be effective thus the way to go.

In conclusion, The State Police Strategies are on the right path but all of them need some improvements. If the discussed improvements are adhered to it will be the first step to combat online predators in an ethical way. Also due to the increase of minors using the internet and social media in general, these platforms should also be accountable. Just as creating tools that guardians can use to monitor their online activities. Also creating a kid's version of applications that will be monitored by the company for any suspicious activities like how YouTube made YouTube kids. More and more platforms are created it has become hard to track down everything. But cooperating together with both Internet platforms and the State Police is the right main step in combating online predators.

Works Cited

Quinn, Micheal J. *Ethics for the Information Age*. 7th ed., Pearson, 2017.

“50 USC 3003: Definitions.” *U.S. Code*,

[www.uscode.house.gov/view.xhtml?req=\(title:50%20section:3003%20edition:prelim\)](http://www.uscode.house.gov/view.xhtml?req=(title:50%20section:3003%20edition:prelim)).

Accessed 19 October 2023.

Finkelhor, David. “Prevalence of Online Sexual Offenses Against Children in the US.” *NCBI*, 14

October 2022, www.ncbi.nlm.nih.gov/pmc/articles/PMC9568794/. Accessed 6 October

2023.

“Hacker group battles child porn.” *CNET*, 2 February 1998,

www.cnet.com/tech/services-and-software/hacker-group-battles-child-porn/. Accessed 16

October 2023.

“International operation targets online predators using social networking sites.” *ICE*, 10 February 2023,

www.ice.gov/news/releases/international-operation-targets-online-predators-using-social-networking-sites. Accessed 19 October 2023.

Trapnell, Laura. “Fake social media accounts | Are they illegal? | Paris Smith Solicitors.” *Paris Smith LLP*, 10 December 2021,

www.parissmith.co.uk/blog/fake-social-media-accounts-legal-and-ethical-issues/.

Accessed 6 October 2023.

“What Is Ethical Hacking and How Does It Work?” *Synopsys*,

www.synopsys.com/glossary/what-is-ethical-hacking.html. Accessed 16 October 2023.

“What is online child sexual exploitation?” *ACCCE*,

www.accce.gov.au/help-and-support/what-is-online-child-exploitation. Accessed 5

October 2023.