To Catch a Pedo: What It Takes

DATA 605: Ethical and Legal Issues in Data Science

Stephanie Zhang

Minors are the most vulnerable target of predators, online and otherwise. Personally, I believe in the pursuit of justice, that in and of itself justifies the means. In other words, according to relativism as it pertains to me, there need not be an ethical compromise because this is inherently ethical. Every technique used to catch criminals, much less pedophiles, is simply what they deserve.

The purpose of this paper is to discuss in sequential order, the four topics of fake profiles, ethical hackers, foreign intelligence, and university backed AI programs used by the State police to catch online predators. Specifically, in each scenario I will examine possible ethical issues, applicable ethical theories, and recommendations for improvement.

Additionally, the ethical theories applied in each scenario are relativism and utilitarianism. I believe these are the most relevant theories because they are straightforward and universally applicable. Relativism relates to the individual’s judgement, and utilitarianism relates to the consequences for society.

If we used Kantianism, I could just say all the topics are unethical, no questions asked. Virtue ethics focuses primarily on character and does not have much to add to the dialogue in terms of policy advice.

On the topic of fake profiles, this is one technique the State police has implemented since the rise of social media. With the rise of social media, exploitation of minors through the internet has skyrocketed. This is the tragic reality of the modern world.

Ethical issues related to this strategy include the legal ethical rules “prohibiting misconduct and deception” (SMI, 2020). These usually apply to lawyers; but they could also apply to the police in this scenario. The issue lies in the intent of the police, which is to deceive. In accessing the ethical viability of the continued use of the data gathered using fake profiles, I say it is completely ethical and should continue to be used.

Although the intent of the Police is to deceive, it is for the purpose of reeling in and catching predators. With relativism, it is up to the individual to determine if using fake profiles for the purpose of catching predators is ethical or not. I say deceiving a predator to take him off the streets not only makes the streets safer, it is a necessary justice.

In terms of utilitarianism, it is also ethical because according to Dan, a detective sergeant for the Metropolitan police, “Take an abused child and look at the long-term cost to health, education, the justice system and lost work opportunities for the rest of their lives, in economic terms, this work makes complete sense.” (Tickle, 2012).

Thus, the ends justify the means. Luring predators using fake profiles is justified because this is what is needed to take them down and allow the internet to have one less predator. Regarding my recommendations for any ethical safeguards or improvements, I do not have any because I believe this is completely ethical.

Furthermore, on the topic of ethical hackers, these are commonly referred to as white hats. As opposed to black hats, who are cyber criminals, white hats hack for the sake of good. Again, the theme of intent comes into play here. Both are doing the exact same thing, only one commits crimes while the other neutralizes them.

Their ethical issues are also of a legal nature, “The legal risks of ethical hacking include lawsuits due to disclosure of personal or confidential information. Such disclosure can lead to a legal battle involving the organization and the ethical hacker.” (Johansen, 2017).

Using the ethical theory of relativism, I believe it is ethical due to the intent. There are risks that come with hacking, however if the hacker remains very careful in their information handling, then the possibility of leakage would be very slight. Using utilitarianism, the risk of leakage is a cost that hackers and the police must bear, and it is worth it because gaining access to social media websites, platforms, and forums will allow the police to catch a significant amount of predators.

I would recommend that the police hire the most experienced and skillful white hats that their budget allows, because cyber criminals are getting more sophisticated by the day. Thus, the police need people who can keep up.

Another strategy the police have implemented is asking foreign intelligence services to access U.S. servers without judicial authorization to provide data in the search of online predators. An ethical issue is the question of access by foreign governments to U.S.-located data (Wiegmann, 2017). There are many rules and regulations in place that make it a hard process for foreign countries to access U.S. owned data, for the purpose of protecting U.S. interests and security.

This has caused more harm than good, “frustrated investigations and risked thwarting the pursuit of justice.” (Wiegmann, 2017). Using relativism, I believe that to combat crime internationally and domestically, the U.S. needs to be open to giving away their data. Foreign governments should naturally reciprocate, thus creating synergy.

Crime is universal, and just because it is happening in a foreign country, does not make it any less of our concern. International co-operation is critical in fighting crime and making the world that little bit safer. With utilitarianism, again there would a global benefit to international co-operation.

I would recommend that the U.S. needs to implement a legislative solution to solve this problem of international data deadlock. Law enforcement regardless of nationality need to be able to “obtain digital evidence without undue delay. Waiting months for evidence critical to solving fast-moving investigations – such as terrorism, computer intrusion, and child sexual exploitation cases, just to name a few – is dangerous and harmful to the safety and security of Americans.” (Wiegmann, 2017).

Lastly, the police have also hired 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. AI has a lot of ethical issues, and to summarize, “AI presents three major areas of ethical concern for society: privacy and surveillance, bias and discrimination, and perhaps the deepest, most difficult philosophical question of the era, the role of human judgment.” (Pazzanese, 2020).

With relativism, I think that the numerous benefits of AI, such as increasing efficiency, ease of handling large data sets, and capability to predict models by far outweighs the risks. In fact, the risks already exist entirely on their own.

In business and the workplace, “rife with human decision-making, have always been riddled with all sorts of biases that prevent people from making deals or landing contracts and jobs.” (Pazzanese, 2020). Therefore, discrimination is already prevalent in regular decision making. At least with AI, these biases can be skewed towards objectivity rather than human subjectivity.

With utilitarianism, the benefits of AI far outweigh the potential risks. At this point the rise of AI cannot be stopped. It is moving at a breakneck pace, due to the modern world’s increasing reliance on big data and advancing technologies. Therefore, the value to society is too great for the risks to even compete with.

To improve AI algorithms is to make them more objective. To do this, it needs to be trained using more data. Thus, I recommend advocating against the ethical stigma attached to AI. From a utilitarian perspective, the sharing and usage of data should be actively embraced by society.

In conclusion, we identified ethical issues pertaining to the four topics of fake profiles, white hats, foreign intelligence sharing, and AI algorithms. Then, we examined these issues using the ethical theories of relativism and utilitarianism and made the appropriate suggestions.

Critics can argue that the police are doing bad things. Maybe they are, but they need to because they cannot allow the alternative. Perhaps this is the price they must pay. The sacrifices they must make. The risks they must take. The burdens they must carry to prevent disaster.

References

SMI, (2020). *Lawyers Using Fake Profiles Will Find Themselves in Real Trouble*, SMI Aware, Retrieved from <https://smiaware.com/blog/lawyers-using-fake-profiles-will-find-themselves-in-real-trouble/>

Tickle, Louise, (2012). *How police investigators are catching paedophiles online*, Guardian News & Media Limited, Retrieved from <https://www.theguardian.com/social-care-network/2012/aug/22/police-investigators-catching-paedophiles-online>

Wiegmann, Brad (2017), *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights,* Homeland Security Digital Library, Retrieved from <https://www.hsdl.org/?view&did=807294>

Pazzanese, Christina*,* (2020)*. Great promise but potential for peril: Ethical concerns mount as AI takes bigger decision-making role in more industries*, The Harvard Gazette, Retrieved from <https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/>

Johansen, Rowena, (2017). *Ethical Hacking Code of Ethics: Security, Risk & Issues*, Panmore Institute, Retrieved from <http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues>