Ethical Issues: Discussion Posts

# Find a Fellow Student Online

**What did you find out about a fellow student online? Were there any associated ethical issues?**

I don’t know the other students since I am taking this course online, so I decided to see what I could find out about my husband. He has a very common first and last name and his information was made more difficult to find by the fact that there are some (unrelated) famous people with his name. I began by typing his name and the city we live in. It actually brought up his LinkedIn fairly quickly, which might be because we are connected on that platform. Nevertheless, there was nothing concerning there other than a profile photo that’s a bit too old.

After further digging, I was able to find our home address and saw websites that would allow you to pay for more contact information. I didn’t pay for the deeper look, but I was able to see that, while some of the information posted was incorrect, a lot of it was correct. It is concerning to me that you can find someone’s address so quickly. It also included names of people close to him including his parents, sister, and myself. These people are much more likely to be findable and have more information on him available to the public due to less common names, smaller cities, and more activity on social media. While my husband is not particularly active on social media, it is easy to find more on him than what he himself puts out there because of those who know him that are active.

Overall, there were not overt ethical issues on his part. The things he has put out there are strictly professional. However, I have seen ethical issues in the connection of people on the internet and quick access to information they may not want out there for the public. It seems very easy to stalk someone with this information because you now know where they live and work and can even pay to get their phone number, which would likely provide access to even more information. After taking the cybersecurity course, it seems that targeting a specific person would be pretty easy, which is concerning to say the least.

# Analyze a Case Study

**Choose a case study from the ones provided with the ACM Code of Professional Ethics, at** [**https://www.acm.org/code-of-ethics/case-studies**](https://www.acm.org/code-of-ethics/case-studies)**.   Write and post (on the discussion board) an essay of 500-800 words that:**

* **Briefly analyzes this case from the perspectives of each of the ethical frameworks we have studied: Kantianism/Deontology; Virtue Ethics; Utilitarianism.   For each, do you feel that framework suggests whether the situation is ethical or not?  Or do you feel it does not lead to a conclusive determination?   Whichever you feel (ethical / inconclusive / not-ethical) please state briefly what you feel that framework leads to that conclusion.**
* **From what you have seen so far, which ethical frameworks appeal to you most, and least, and why?**

*Case Study: Automated Active Response Weaponry*

*Q Industries is an international defense contractor that specializes in autonomous vehicles. Q’s early work focused on passive systems, such as bomb-defusing robots and crowd-monitoring drones. As an early pioneer in this area, Q established itself as a vendor of choice for both military and law enforcement applications. Q’s products have been deployed in a variety of settings, including conflict zones and non-violent protests.*

*In recent years, Q has suffered a number of losses, as protestors and other individuals have physically attacked the vehicles with rocks, guns, and other weapons. To reduce this problem, Q has begun to experiment with automated active responses. Q’s first approach was to employ facial recognition algorithms to record those present and to detect individuals who may pose a threat. This approach was shortly followed by automated non-lethal responses, such as tear gas, pepper spray, or acoustic weapons, to incapacitate threatening individuals.*

*Q has recently been approached—in secret meetings—by multiple governments to expand this response to include lethal responses of varying scales. These capabilities range from targeted shooting of known individuals to releasing small-scale explosives. When Q leadership agreed to pursue these capabilities, several of Q’s original engineers resigned in protest. Some of these engineers had previously expressed concern that the non-lethal responses had inadequate protections against tampering, such as replacing tear gas with a lethal poison. Knowing that these individuals were planning to speak out publicly, Q sued them for violating the terms of their confidentiality employment agreement.*

Deontology relies on universal moral laws that are based on reason, making duty and intent of the utmost importance. Furthermore, all humans are inherently equal and should be treated as an end, not the means to an end. Essentially, deontology can be summed up with the “golden rule.” In this case study, Q Industries would undeniably be condemned by Kant and his followers. For one, Kantian ethics reject killing people and would certainly look down upon using violent methods of changing human behavior. Second, Q’s lawsuit against the employees that planned to speak out publicly inherently places the needs of the company, a non-human entity, over those of the humans, which are being supported by the former employees.

While deontology is fairly cut and dry in this case, it does not actually address the widespread concerns over facial recognition. Privacy is not clearly defined as a universal moral law or not because different people and different cultures prioritize it (or not) to different extents. As a result, Kantianism cannot make judgements on the technology itself, only on the resultant actions taken from the data it gathers.

Virtue theory is provides less obvious answers to the ethics of the scenario. While virtue theory places the most importance on having virtuous qualities rather than useful results or following some set of rules, it doesn’t account for changes in what is considered virtuous overtime. If you think justice or even revenge are more virtuous than mercy, then perhaps Q’s technology would not be considered unethical from this perspective. On the other hand, the drones are attacking people who have not actually done anything, at least not yet. If the injustice has not taken place yet, is it possible to deal out justice? My intuition tells me that virtue theory, like deontology, would end up condemning Q’s technology. However, it is not as short a debate.

Privacy is not typically thought of as a virtue, so again, we find ourselves judging the ethics of the case study through a lens that does not address one of cybersecurity’s biggest concerns. Part of the reason that the last two ethics theories are not as useful in a scenario such as this, is that they were created in a pre-modern era when virtues were only discussed as something humans could hold. There was little to no room for non-human entities to have virtues. Indeed, even cities in ancient Greece, where virtue ethics was born, were called by the name of the people as if the city and the people were the same entity, inseparable.

Utilitarianism was founded with more kinds of entities in mind than just humans. Keeping an eye on the greater good over individualism, it emphasizes the importance of the end over the means. With this view in mind, Q’s drones would not be considered unethical due to the result of keeping more people safe by eliminating threats before they occur. Any action that would threaten the greater good, in this instance public safety, including the public discussion of such technologies by former employees would be considered unethical.

The problem with this perspective, other than the potential for killing or harming innocent people, is that it weighs short term benefits more than the costs. For instance, it only stops the potential for an individual or a small group of people to do something violent. It does not address the reasons for the protests in the first place, nor does it consider the possibility of more protests and increased violence in reaction to the harm done in the initial protest.

This case study is better addressed by the social contract theory, which balances the rights of individuals with the security and benefits that governments can provide. In the United States, our constitution acts as a social contract which can be ammended and change over time. If the people agree that security is more important than privacy or an individual’s life, then Q’s actions would be considered ethical. If Q Industries was an American company today, it would be considered unethical in that it punishes people who have not yet committed a crime, robbing of both the chance to not commit a crime and due process if they do.

While Kantianism appeals to me on a human level, it breaks down at larger scales. Therefore, social contract theory can be helpful in translating Kantian ideals into wider society and non-human actions.

# Recommender Systems

**Select one ethical framework (your choice) and write on the discussion board whether you think this framework supports or does not support the use of recommender systems to feed you more YouTube content (songs) and with that, more advertisements.   If you prefer to comment on the case where recommender systems suggest political content as discussed by Tufecki, rather than on musical content that is fine too.**

Through deontology, we can conclude that the using recommender systems to feed you more songs and thus more advertisements is not ethical. This is because the recommender system is using the human viewer as a means to an end. In other words, the goal is advertising, not enriching the users’ lives with more music or useful videos. This remains true for increasingly extremist political content recommendations as the well-being of the individual is literally being sacrificed for the goal of increasing profits.

# The Right to Be Forgotten

**Comment on the following in the discussion board:**

* **Do you feel there should be a Right to be Forgotten in your current nation of residence?**
* **Do you think this policy should be universal, or vary in different countries / regions?**
* **What is the basis for your opinion?  (Ethical framework we’ve studied, or something else)**

I think there should be a right to be forgotten in the United States. The basis of my opinion for this is deontology. Through this ethical lens, humans are all equal and we should essentially treat each other how we ourselves would like to be treated. In this sense, most people would not like the mistakes or simply embarassments of their youth to be made known until the end of time. Furthermore, information about past states of your affairs (financial, personal, or otherwise) is not necessarily relevant to current matters but could result in discrimination. In conclusion, unless the safety of the public is a concern, the right to be forgotten has deontological standing.

# Report #1

**Write a report of 500-800 words that includes:**

* **The reference information for the article (title, author, where and when published, link if online)**
* **A summary of the content of the article**
* **The issue(s) in data ethics that this article is relevant to**
* **Your assessment of whether the issues discussed in the article are being handled and resolved properly, and what additional steps you feel should be considered.  Please refer to at least one ethical framework in making this assessment**

McCue, TJ. (2019). “Alexa Is Listening All the Time: Here’s How to Stop It.” *Forbes*. <https://www.forbes.com/sites/tjmccue/2019/04/19/alexa-is-listening-all-the-time-heres-how-to-stop-it/>.

McCue expertly navigates readers through the settings of the Alexa app on how to turn off sharing your Echo data with Amazon. He even adds some cues for users that have Google Home and Apple HomePod. McCue recognizes that completely unplugging is difficult in the modern age, especially with cellular devices in all our pockets. However, he recommends another DIY hack for stopping Alexa and other listening devices from hearing and recording any given conversation in your home. This hack is essentially building a white noise machine that can only be turned off with a spoken command. Otherwise, it is supposed to block other devices from capturing human language in a distinguishable way. McCue also notes that there are starting to be some white noise devices of this kind on the market as well. Considering that this piece was written in 2019, there are likely many now.

Finally, it is necessary to note that the entire basis of needing instructions like these was the news that Amazon was paying thousands of workers across the globe to listen to recordings from Echo Dots. The purported reason for this was to have humans identify human language, transcribe it, and feed it back into the system so that Alexa could learn to identify speech better and improve its usability. Of course, this practice can also raise serious concerns.

The main ethical concern of the article was the capture and use of conversations that were not meant for Alexa’s use. However, I would also like to add another ethical concern, which is the capture, use, and (most importantly) lack of deletion of user data. Using data that you have not been given express permission to use, and similarly capturing personal data that your device was not supposed to capture, is a violation of privacy. At least in the United States, we highly value personal privacy. This is even written into our bill of rights in several places, including the first and fourth amendments protecting rights to assembly and against unwarranted searches. No matter the ethical framework, whether that be deontology, social contract theory, or virtue ethics, this invasion of privacy, or even the potential for it, would be considered unethical. Even utilitarianism could view it as unethical when considering there are other ways of training Alexa’s speech capabilities.

Because the article is about six years old, I was curious whether these issues had been addressed by the company. I have an Echo Dot in my own home, a graduation present from my mother-in-law, that we use mainly for keeping our grocery list. The settings and app navigation have changed significantly since the article was written so I had to do a bit of searching on my own. Through this investigation I found two things: (1) Amazon has still kept the default data sharing setting on, and (2) I could view everything Alexa had captured about my husband and I since we first took it out of the box and plugged it in.

This was disappointing because, not only had the company continued to take advantage of those of us who hastily added devices to our homes without taking the time to think about the security and privacy risks, it also was making us more vulnerable to privacy concerns by storing unnecessary data for extended periods of time. This was easily remedied by changing the data settings to not store any information it grabbed and deleting the history it already stored. However, it is still a problem that the default is to capture and keep everything, especially because it is completely unnecessary for both the user and the company providing the service.