In this essay, I will apply Kant's ethical theory to the modern day cybersecurity issue of generative artificial intelligence systems exposing sensitive user data. Large AI platforms like ChatGPT are trained on huge amounts of information and can sometimes reveal the personal, confidential, or even copyrighted data that people never tend to share publicly with others. That makes it a serious problem because some companies using AI systems must balance the innovation and convenience against the privacy and safety of the people. I believe that, referring back to Kant's ethics, some companies using generative AI systems have a duty to protect user privacy and stop sensitive information from being published. I will explain the principles of Kant's ethical theory and explain the ethical problem made by generative AI systems releasing people's personal information.

Kant's ethical theory is a form of focused ethics, meaning its morality is based on their duties and rules rather than consequences. Kant said people should act according to principles that may be applied universally to others. The idea is known as categorical imperative. One description of categorical imperative says that a person should only act according to a rule that they would be ok for everyone to follow. Another important piece of Kant's theory is that people have to always treat humanity as an end in itself and never a means to an end. Or in a simpler way, people should never use people only as tools for money, convenience, or even personal gain. Kant believes that morality came from acting out of respect and duty for rational people. Actions like manipulation, lying, and violating someone's privacy are wrong because they fail to respect the dignity of other people. If a harmful action produces positive outcomes, Kant would say that it's still immoral if it violates a person's rights or treats them as a tool.

One of the new cybersecurity risks created by generative AI systems is the fact that these systems may expose our sensitive information. AI chatbots are trained to use a lot of datasets collected from online sources and digital content. In some situations AI systems have generated outputs containing people's private information, like their house address or even company information. It's plenty of ways it can do it. This would create a major ethical problem because people really do trust AI companies with their information without fully knowing how their information is stored or processed. This problem becomes more acknowledged when companies only prioritize AI development over just using strong privacy protections. An example I have for that is an AI company may still deploy systems despite knowing there's a risk of exposing these people's data. The company may try to justify their decision by arguing that their technology benefits millions of people, and increases profits. Even though that may all sound nice, people whose information gets exposed may suffer from identity theft, financial harm, or even damage to their professional reputations.

Kant's theory shows a clear way to solve this problem. Kant said companies developing generative AI systems have a duty to respect others as rational individuals rather than treating them as a way of making profit. If a company knowingly allows an AI system to expose information, they'll fail to respect the autonomy and dignity of people. A reason companies do this is because they are trying to achieve financial success, or mark dominance. Looking at it from Kant's perspective, the ethical responsibility of AI companies is not simply to maximize profit or efficiency. Their primary goal is to respect others and protect their rights. This would

mean that companies must use strong safeguards dealing with sensitive data, and avoid releasing systems that they are well aware of that they know may compromise people's privacy.

I feel like companies should have implemented stronger cyber protections and testing procedures to avoid the likelihood of data being revealed by these AI systems. If these developers found that the system could copy private information, they should have delayed the deployment until this problem was fixed. Companies should limit the amount of information being collected in the first place. Collecting irrelevant data increases the risk of exposure and misused information. Kant ethics says organizations have a requirement to minimize risks that could harm others. AI developers should design systems that protect privacy by default instead of grabbing so much data at once.

In conclusion, the ethical challenge created by generative AI systems exposing sensitive data can be resolved by using Kant's ethical theory. Using Kant's ethics, companies have a duty to respect others as ends in themselves rather than treating them as a tool for profit or technology advancements. Allowing AI systems to expose people's private information violates this duty Kant is talking about, because it disregards the person's autonomy and privacy. Kant's categorical imperative also showed that in a world in which companies freely risk exposing people's data would take away people's trust within them. For these reasons companies should prioritize strong privacy protections, informed consent, and do more responsible deployment practices. Kant's ethical theory provides a convincing framework for resolving this cybersecurity problem.