Eventually, the law will catch up in every region. Every country has different policies and different viewpoints on Generative AI. Let's begin with data privacy concerns. So, when working with a service like ChatGPT, there's a couple of concerns here with regards to data. There are two forms of data. Your company's data, which may include intellectual property, and your user's data, which may contain sensitive user information. Back in March 2023, ChatGPT had a breach, and this expose user information, and their chat histories. And there's a couple implications here that has to be considered. Let's start with the chat histories. If you're working on a project for your company and you're feeding your company's data or intellectual property into a service like ChatGPT and there's a breach. What are the implications of that breach, if it is your company's data that was exposed? And this kind of exposure is happening with large companies too. So, one of the issues at hand is, when dealing with your company's proprietary IP, there may be needed additional security checks. Going back to one of my original statements that some of this is just common sense, but sometimes we do not think about these issues until they're put in front of us. So, what are the measures we can do to protect our data?

First, before using a service, read their privacy statement, find out what they do with the data and how long they store the data. Revisiting your privacy policy allows you to compare your privacy policy with the potential service you may be using to make sure they are in alignment. It also allows for an opportunity to update your privacy policy in the face of rapidly technological changes that are occurring in the world today, such as Generative AI. Third, and I mentioned this a little earlier, implement additional security checks to make sure you are protecting your data.

Lastly, when dealing with user data, you should anonymize that data, especially before feeding it into a third-party service. This allows your data to be worry free about the implications of the security breach. Now let's talk about Generative AI bias. The Diffusion Bias Explorer uses Generative AI image technologies such as stable diffusion to see if there are any biases. The way this explorer works is that I will choose an adjective and a profession. And through those two choices, those two prompts, it will generate a series of images. Now on the page, it does state you do not have to use an adjective, but from personal experience, sometimes when an adjective is not given, the explorer will not generate any images. To start this process, I'm going to choose confident Doctor and it takes a couple seconds for the images to generate. Now that this is done, I will scroll through the images. Do you see any potential bias in these images?

Further the demonstration on the right side, I will choose confident nurse and after a couple seconds the images have generated. And I will scroll through the nurses and there appears to be a bias here. They may be asking what is the bias, a gender bias? There are no female doctors and there are no male nurses. So, the reason why this can happen is that Generative AI can inherit biases through its training data. And this will perpetuate certain stereotypes as witness through this Diffusion Explorer, all male doctors, all female nurses. So, how do we combat bias? Well, here are three suggestions actively working to mitigate during training. And this could be a few things. One approach is to expand the number of datasets that you are training with to reduce potential biases. Another approach could be to remove potential biases from your data, but that could also skew your data and create a new bias. Second, you should test your datasets to see if there are any existing biases.

Doing so will give you a better understanding of what could be potentially wrong with your data. Lastly, be transparent when bias exists and take that into account when referencing your data. If a bias exists and you cannot remove the bias from your data, because it will either create new biases or create inaccuracies when working with your data. If you're aware of them, you can at least plan for them and maybe work around them. And now let's end the video with a conversation about IP and copyright on the screen. I have a program that will generate images based on a prompt, and I'm going to type in a prompt for a iconic movie character. I'm going to speed up the process because it takes about two minutes for this to complete. Now that this is completed, the image is on the screen and you may not recognize this character. That's fine if you haven't seen the movies. It's totally understandable. But the implication here is twofold.

The first implication, which should be obvious, is I can't use this material on a website or to create content with, because it is copyrighted material. I would be violating somebody else's IP. Having a conversation about it is one thing, like in this matter. But if I were to make a movie or a series of images and state that this is my copyrighted material that I would be selling as a product, that would lead to a lot of legal issues. Second, in order to create this image, there had to be some training data involved, and that training data involved copyrighted material. This is an accurate image. So, there's an implication there that we might not be aware of when working with Generative AI tools, such as this one. And now, for another example, how about an eagle soaring through the sky? And once again, I'll speed up the Generative AI process. And on the screen, I have two eagles soaring through the sky. Let's say, I want to treat this as copyrightable material.

Well, in the United States legally I can't. The courts have repeatedly supported the position of the US Copyright office that works created with Generative AI are not subject to copyright protections. Why did state images? This applies to all generative AI content. The US Trademark and Patent office will not apply patents or trademarks to works created through Generative AI. And every region has its own set of laws to protect IP and copyright. One of the issues in this time period is that usually, the governments are slower to respond, than the technology. As technology evolves, I believe law will eventually catch up and evolve with the technology. So, what are some concerns or potential questions you may have when using Generative AI? Does the Generative AI tool sources of data violate another company's IP copyright? And this is the sort of question that needs to be asked to protect you or your company from a potential legal battle.

I think about this through a programming perspective. And one of the main concerns is when you use a tool like GitHub Copilot that does help you program. Are we using copyrighted code to create a product? And that leads to the next concern. Is your IP being used for others? If you're providing data to these Generative AI tools, is that being used to further train the model. And in return, you're leaking your IP or copyrighted information to others. In the beginning of the video, I did mention the ChatGPT lead. These sort of situations could put your IP at risk. Lastly, because things will change, what is the current state of IP copyright protections? This will evolve over time, and I can guarantee you that within a year or two of making this video, the landscape has changed. The laws will change as governments react. So, there's a lot of considerations to take into account when working with these Generative AI tools, and I will leave it at that. Thanks for watching at Cloud Academy.

Let's now then have a look at some of the ethical concerns around the use of [AI](https://platform.qa.com/course/module-0-what-is-machine-learning/introduction-to-ai/). So the first issue here is one of mistakes and safety. And here is the principle. If the history of data that the machine has seen looks like, or is very, very, very, very similar to the data it is seeing when it solves the problem, then you're okay. If it doesn't, then you are seriously not okay. You are possibly deeply unsafe. So that's one. Ethical concern number two, so the origin let's say and quality of the historical data, which is sometimes called the training data, the data the machine is fed when it is specializing the algorithms it will use. The training date or the historical data. Right, what are the concerns of the origins of this? Well, here's the thing. Practitioners, experts, scientists are not always in control of the information the machine is considering when it is specializing itself. How might that be? Suppose a [machine learning](https://platform.qa.com/library/machine-learning/) system considers social media posts to assess, let's say, the marketing quality of some user, to asses their political party, to sell them a product or to advise them about a decision. Suppose because the machine is considering social media data, I, as a malicious agent, create social media posts that I know the machine will consider, will see, will process. And I create them so as to bias, or prejudice, or disrupt its future operation. With this system you could cause all kinds of chaos in people's lives. So if we have let's call it expert control and good faith on the data, then we're probably okay. And if we don't, then maybe we're not okay. Issue three then, and the final issue we will consider, is the system is not making a mistake, operating with high quality information, and in fact making the correct diagnosis, the correct prediction, the correct operation, there still may be concerns with its use. So we can call these moral concerns. Let me give you some examples. Let me give you some examples. So there ones around profiling a person with what we may call protected characteristics or let's say controversial features of a person. Now I don't mean to say-- Another kind of concern here, a moral concern, is lets call it perhaps even the empathetic one or... the automated one. What I mean here is that there is a question around whether were it possible for a machine to deliver a diagnosis, a health diagnosis to a person, whether we'd want to do that in automated fashion. Suppose the diagnosis was cancer. Would we wish to live in a society in which people went to vending machines to discover that they had cancer? There are arguments for such a society, but there are a large number of moral arguments perhaps against such a thing. And those arguments are things really to do with the emotional character of human beings. That people can actually be more stressed, people can feel more isolated, more alone, more ill, from engaging with automated systems that make no consideration for their state of mental health, for their state of emotional health and physical wellbeing. So we could even say perhaps there's a third little issue here following on from that is too specialized. If we build a machine to solve one highly specific problem, by doing so we may end up seeing that the problem we have asked the machine to solve was not the problem we originally had, or even really have. It is one mere piece of the puzzle. And in fact a human being might have performed to say across the board. So we have profiling. We have the empathetic concern, which kind of amounts the same as too specialized. Let's also perhaps say we have the automation concern. So yes, it's too specialized. What about it being automated? Are there concerns about job losses here, about replacing people? For the entirety of human [history](https://platform.qa.com/course/module-0-what-is-machine-learning/the-history-of-ai/) every single technological innovation has replaced human beings on that activity in which it was used. The automated loom replaced hand stitching of clothes. But what we see every time that that replacement is made, is that demand for what can now be automated increases many fold. In other words if we go back to 1800, or to 1700, or even earlier, there is a global demand in the year 1700 for everyone to have multiple shirts, more than one or two, many, like we have today. But there is no capacity whatsoever to deliver on that demand. The wish is there. If you ask anyone in the planet in the year 1700, "Would you wish to have multiple shirts?" They would say, "Yes." But they can't have them. But when the automated loom was invented, suddenly everyone could have them. And because that demand existed, more people are employed to serve it now it was there, than were it lost in the jobs which disappeared because of the automation. And the reliable thing about human beings is that the demand is effectively infinite. If you can create a new technology then the things that new technology allows will be wished for by everyone one.