My groups summary:

Our group found 3 articles tackling different issues. In one article The CEO of TikTok, after his company was found violating multiple privacy policies, also mentioned how Temu and Shein were a risk to national security as well. Last year, Temu was the most downloaded app in the US with it currently boasting around 170 million users. What most don’t know is that Temu can collect data if the app is installed, and the users won't notice at all. Temu is also obligated to share information with the Chinese Government as well as being able to access private data and sell it to third party users. Scaringly, app store security scans don't flag Temu's risks because Temu can change its own code once it has been downloaded to a user’s phone. Our second article focused on the 2016 Wendys Point-of-sale scams. Wendys discovered that 300 of its stores were infected with malware intended on stealing customers credit card information. Wendy's caught wind of this when several credit card unions reported fraudulent payment activities being traced back to Wendys. One company estimated that the loss from this breach was 5 to 10 times that of Home Depot and Target. After considerable research, it was determined that more than 300 stores had been affected by these breaches. They mentioned that part of the problem was that the breach happened in two waves, with two different strains of malware. The last article we discussed was about how as of February, the CDC has changed their policies regarding molecular surveillance. Essentially, the CDC is collecting genetic data on HIV viruses found in patients. Collecting this information about a patient’s virus material violates a patient's privacy as they have no way to opt out of it. The patient does not need to be notified about this, and their information could be used in court cases or worse. They worry that with this information they could see exactly how the virus was spread through a population. These articles all connect because it involves so much more than large companies being attacked. Their customers and consumers are also being affected, even more than the company. With a multitude of people’s well-being at risk, this issue is national if these mishaps continue. These articles display how regular people are being used as a means to obtain money and information. This leaves people feeling unsafe and at a loss for money.

The other groups summary:

The other group wrote about 3 different large companies and their sketchy business practices. Firstly, they wrote about how Meta was doing UK data transfers, exposing their information possibly to the US government. The US violated citizens of Europe since their laws are different. Meta was possibly selling the data as well, so it was seen under the data protection policy, and they deemed it unlawful. A fine of $1.2 billion was associated for the damages. They also wrote about how the FBI violated the privacy rights of Americans. They breached FISA section 702, which lets them read foreign emails to defend from national security threats. Through this they found a loophole allowing them to legally look through American emails. This allowed them to collect heaps of American data. Their final article was about how in 2013, Yahoo had a data breach over all 3 billion users. It went unnoticed until 2014. They didn't announce them getting breached, which eventually came out in 2016, when yahoo tried to sell themselves to Verizon. Their value went down to $35 million due to the breaches. They were also fined $50 million since they didn't tell their users about the breaches. These articles show a common theme of using people as a means to stealing data. This causes people to become enraged that their personal information is in the hands of many others.

Summary of the privacy unit:

Over the course of our privacy unit, we’ve learned in depth the importance of privacy and the consequences of it. Our information, whether it be our card details or conversations, is immensely important to us. With this information comes dignity, stability and happiness. When information dear to us gets leaked, it’s extremely threatening of our privacy. We enjoy privacy in most everyday situations, as privacy is both physical and online. We all reserve the right to have “freedom to”, and “freedom from” any private situation we don’t desire, or do desire. Unfortunately, with the internet, privacy is at an extremely vulnerable point. Personal data is sold off constantly by companies and individuals for profit. This puts people’s personal privacy at constant risk, as well as leaving them unsafe. This makes the issue of online privacy an utmost risk that needs more attention. Too many people are being used for their information which could potentially harm their privacy.

Examples of the 8 types of privacy:

Bodily privacy: An example of bodily privacy is that friends and strangers have no right to touch you in any way. If someone were to attempt to touch you in a non-desirable way, you have the right to reject their notion.

Spatial privacy: An example of is that you are allowed to have a private sphere in which nobody can intrude. If I were to have a house and someone wanted to come in without me wanting them to, I can reject their want to come inside.

Communicational privacy: An example of this is that I have the right to reserve any information about myself in any situation. If I were in public and somebody had been listening in on my conversation, that would breach this form of privacy. I would have a right to converse away from all ears.

Proprietary privacy: An example of this is that I have the right to shield my information from the public sphere. My backpack contains many of my personal belongings as well as preventing any onlookers from seeing what’s in it.

Intellectual privacy: An example of this is that I have the freedom to develop my own opinions and beliefs. If somebody walked up to me and told me that the world was indeed flat and that I’ve been wrong my entire life, I would still have the right to continue to believe that the earth isn’t flat.

Decisional privacy: An example of this is that one can make personal decisions whenever they want. If I were to want an ice cream cone, nobody has the right to say I cannot, as it doesn’t affect their own personal well-being.

Associational privacy: An example of this is that I have the freedom to choose who I interact with. If I saw someone who I thought was cool, I would have the right to hang out with them. However, if somebody was really annoying me, I would have the right to stop hanging out with them.

Behavioral privacy: An example of this is that I have the right to be both reserved and myself in public areas. If one day I were feeling chipper, I could be energetic in the public sphere. If one day I were tired, I could be slow in the public sphere. In either circumstance, I’m allowed to act the way I please in the public sphere.