Definition: Privacy

Different sections of privacy

-How to define privacy?

-Technological Advancements in the internet has caused more and more information to circulate

- Interestingly,

 Privacy is defined under law: To quote Prosser

https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/what-is-privacy/

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.
* How private is the internet actually?
	+ Despite the thought of internet security, there is always the threat of security breaches and hackers
		- Breaches in confidential information, for example, Target’s massive credit card breach
			* <http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit>
		- Notably confidential information leak was the 2013 leak of confidential government global surveillance files
			* Edward Snowden was behind this
			* Revealed that data was being collected of domestic and global surveillance; caused some fear in Americans of how private is the internet and is the US government spying on them
	+ Lots of information is now permanently on the internet because of things like social media
		- Social networks now have information like birthdays, addresses, relationship status, etc that are readily accessible to anyone
		- So much so that social media is now a form for investigators and police to search for suspects
		- <http://www.cnet.com/news/the-internet-a-private-eyes-best-friend/>

The definition of privacy varies on different degrees. Certain information may be considered private by one, but not by others.

Notable stats:

-68% of internet users believe current laws are not good enough in protecting privacy

-86% of internet uers have taken steps online to remove or mask their digital footprints

-55% of internet users have taken steps to avoid observation by specific people, organizations, or the government

-50% say they are worried about the amount of personal information about them that is online

http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Storyboard of Events:

-Meet main character named “Ted”

-Introduce the rise of technology, and how more and more information is being uploaded to the web

-Begin discussion of what piracy is

-Formal definitions of piracy

-Discussion of privacy vs. security

**Script:**

Hey guys, my name is Teddy and I’m here to talk to you guys about privacy.

Privacy is a term that’s drastically changed over the past couple of years, and is a term that’s holding more and more significance as the spread of information has become facilitated by the rise of the internet.

Privacy in the Merriam-Webster dictionary is defined as “the state or condition of being free from being observed or disturbed by other people.” But privacy has become much more than just staying in your room, hiding away from other people. In this age of digital technology, people are closer than ever, with more and more information on the internet that ANYONE can access. So what has privacy become in this modern world, and why is it so controversial?

Firstly, we can take a look at the legal aspect of privacy. Privacy on the internet has become so vague and highly disputed that a legal definition of privacy has been written up. According to William Prosser, American common law has recognized four types of actions for which one can be sued in civil court for invasion of privacy:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

A perfect example of such was the massive Target leak that occurred in 2013. Target’s internal database with all of it’s customer’s personal information was breached, and an estimated 42 million people had their credit/debit card information stolen from them.

Another example of a breach in privacy on a much grander and significant scale was the Edward Snowden Wikileaks scandal. Snowden was a contractor for the US Federal Government, and upon finishing his work there, he released thousands of classified files to news reporting agencies. The files revealed that data was being collected of domestic and global surveillance; caused some fear in Americans of how private is the internet and is the US government spying on them.

However, breaches of this magnitude are rare, and hardly pertain to our average daily lives, so the legal definition of privacy seems a little disconnected and far too specific. Privacy, as its core, is a very simple concept; how can you keep your important information to yourself. But privacy varies in degree, and it is this, that makes privacy a complex term to define. Hence, the definition of privacy changes from person to person. One may think a particular piece of information is private, while others may not. The easiest way to see this is simply going on social media, like FaceBook. Some people have made their accounts public so ANYONE can see all their personal information like address, age, etc, while others have set up their security to the fullest.

This is what makes privacy such an important term in today’s world. Information on the internet is there to stay, and this is something people are starting to realize. In a study done by the PewResearchCenter, 50% of people say they are worried about the amount of personal information about them online. This number is up from 33% which was surveyed in 2009. Moreover, a whopping 86% of people say they have taken steps to remove their digital footprints, which may include clearing their browser’s cache/cookies, encrypting emails, and using virtual networks to mask their IPs.

Script:

The Three Sector of Privacy.

Privacy is a term that’s drastically changed over the past couple of years, and is a term that’s holding more and more significance as the spread of information has become facilitated by the rise of the internet. Privacy, at its core, is a simple term that expresses our desire and tendency to want to keep certain information private. However, it’s no longer simply limited to storing our privacy documents in a locked chest. As society and technology have gradually developed, the world has become more and more connected. Hence, I have broken privacy into three sectors: Corporations, Government, and Peers.

Sector 1: Corporations

Corporations play a major role in modern society. With online shopping now becoming a dominating sector of the market, companies are collecting more and more information about their customers. Take Amazon for example. Amazon collects a plethora of data from its customers, including some highly personal data like credit card numbers and addresses. As a result, much of one’s privacy becomes invested in the corporation. In the majority of the cases, corporations do a good job of keeping private information secure, however there are of course the occasional breaches in security. Take the massive Target breach in 2013 for example, Target’s internal database with all of it’s customer’s personal information was breached. An estimated 42 million people had their credit/debit card information stolen from them. Furthermore, much of this information that companies collect from their customers reveal much more than what is on the surface. In a New York Times article written by Charles Duhigg, it was revealed that a Target statistician had found patterns so strong in Target’s massive collection of customer data, that he could not only predict if a customer was pregnant, but also when the baby was due.

Sector 2: Government

The government is the ultimate overseer of information in the United States. Privacy is hugely controversial topic when it comes to government, as the balance between privacy and security comes to question. A major event that strongly demonstrates this balance was the Edward Snowden Wikileaks scandal. Snowden was a contractor for the US Federal Government, and upon finishing his work there, he released thousands of classified files to news reporting agencies. The files revealed that data was being collected of domestic and global surveillance; caused some fear in Americans of how private is the internet and is the US government spying on them. Particularly, the National Security Agency became highly scrutinized. One of the leaked documents revealed that the NSA was practicing “warrantless surveillance.” “Warrantless surveillance” allowed the NSA to monitor and digitally clone, without warrant, any communications in the United States. So phone calls, emails, text messages all fell within that category. Naturally, when this was leaked, it caused great outrage amongst the American people. This measure, however, was put in place under the presidency of George W. Bush, following the terrorist attacks of 9/11, in order to help with the war against terror. Thus, despite this order being highly beneficial towards the security of the nation, the American citizens were outraged by the huge breach in privacy. Ultimately, because of this, the “warrantless surveillance” was ended shortly after Wikileaks.

Sector 3: Peers

Peer privacy is the sector that we are probably the most connected to. With social media playing such a dominating role in modern society, people are more connected than ever. As a result, personal information is easier to access than ever. Forget someone’s birthday? Want to know where someone’s from? Well, most likely all that information will be one-click away on someone’s Facebook, or some other social media. The scariest part? All this information is to stay, or as the axiom goes, “Once on the web, always on the web.” This is something people are starting to realize. In a study done by the PewResearchCenter, 50% of people say they are worried about the amount of personal information about them online. This number is up from 33% which was surveyed in 2009. Moreover, a whopping 86% of people say they have taken steps to remove their digital footprints, which may include clearing their browser’s cache/cookies, encrypting emails, and using virtual networks to mask their IPs.