Internet Privacy

Before asking what the controversy over privacy is, you should know that people in the past have risked humiliation, faced exile and even lost their lives for it. Internet privacy is a battle ground, your information weapons, your personal space a battle field. In order to be decided you must consider aspects such as ethics, pros, cons, the ways anonymity can be used, organizations, policies and so much more.

In the past, anonymity has been used as a way for authors to surpass the stereotypes such as gender, age, family, name, and has allowed them to stand on the same playing field as every other author in the world. For instance the author of Alice in Wonderland used a pseudonym so he could preserve the modesty of his books. Another example was female authors throughout history who wrote under a pseudonym in order to avoid the scrutiny of being a female writer. (Cole 20-25)

Anonymity was also crucial for the sake of the author’s safety when he or she was expressing personal opinions or speaking of controversial issues; either factually or fictionally. For instance author John Twyn was humiliated, tortured and beheaded in punishment for writing that a monarch should be held accountable for their subjects they rule. Another horrifying example was John Stubbs hand being cut off for writing in opposition to the government. Even publishers would be killed and tortured for publishing information, if the author couldn’t be found, thus making it a good idea to publish and write anonymously (Cole 22-23). A defining moment in anonymous rights was found in the court case of *NAACP vs Alabama*. When Alabama requested the names of this anonymous organization, the group took them to the Supreme Court. The group won its anonymous rights, which proved invaluable to the preservation of freedom.

Another huge factor in internet privacy is the issue of ethicalities how it relates to the invasion of privacy. According to Judith Jarvis Thompson, the rights of privacy consist of the rights of a person and their personal property. Invasion of privacy only occurs when one of the two or both have been violated (Macnish). The fourth amendment also comes into play with its protection against unreasonable search and seizures; we have to ask ourselves, does this apply to internet privacy? (Shah).

The necessity of surveillance should also be considered in the ethical argument. The five questions that must be asked include: Is surveillance better than the alternative? Should it only be used in last resort? What is the point when you should stop or start using surveillance? Is it necessary for the security and safety of society? Is there a justifiable cause for the surveillance to be put in place? Does it discriminate on whom it targets? Is it overdone for its purpose? (Macnish) For instance if you place surveillance in public restrooms, it’s an invasion of privacy. However if there is a justifiable reason such as gang or criminal activities, it may become an option. If in some cases surveillance becomes necessary, it should be carried out in the most non-invasive way possible in order to protect the innocent party and their moral rights. (Macnish)

Pros and Cons of moralities must also be considered when carrying out surveillance. One of the many pros of surveillance is the promotion and feeling of public safety. It can help catch criminals, stop crime and problems existing. However when invasion of privacy does occur, it diminishes the feeling of personal safety and mentally forces the person to conform which leads to lack of need in trust but however may destroy the relationship between the person under surveillance and the person doing the surveillance. (Macnish) Surveillance may also have the possibility of discrimination if allowed under the right conditions. For instance if social sorting occurs and people only focus on one demographic, it creates the problem of discrimination and the occurrence of a stereotype which can cause that particular demographic to be rejected or alienated in society. (Macnish)

There are many pros in general to anonymity on the internet. For instance, anonymity is used online in order to allow people to be themselves, seek support on private issues, express opinions safely, change the world without worrying about disapproval from associates in real life and to prevent the paranoia of humiliation or retaliation. (Cole 218-221) When you have transparency and invasion of personal information, you create a threat to privacy, which is necessary to have a functioning ecosystem. (Macnish) Another pro of anonymity is the fact that what you say on the internet is permanent and could potentially come back to harm you in the future. This can be a terrible thing for people who changed their opinions over time, evolving into a different person. Yet they are still haunted by the stupidity of their ignorant past self. (Cole 233)

Another pro to anonymity is the fact that your personal information is safe. For instance there is a large amount of data stored on computers. If it’s not kept private you can have incidents where medical information is released to the outside world for all to know, destroying that person’s reputation. This is not only a HIPA breech but also an invasion of privacy upon that person. (Shah) This doesn’t only apply to confidential documents though; companies such as Google and Facebook want your name so they can connect your name to personal data about you. While this may not seem like such a big problem, what they want to do is control your mind; potentially leading to data release, blackmail and most obviously data about you to sell to other companies so they can successfully advertise. (Cole 164-166)

However, while there are several pros to anonymity and privacy, there are also many cons to consider. One of the biggest problems is the lack of accountability, which is needed to bring misbehaviors such as identity theft, credit card fraud, virus writers and hackers to justice. Anonymity can make the perpetrators harder to find, which can lead to severe consequence (Davenport). Another controversial point is cyberbullying, trolling and the protection of children. Facebook argues that anonymity can cause cyberbullying, which affects the children, thus leading to the rather controversial issue of being forced to use your own name (Cole 160-164). Facebook also claims through a quote of Randi Zuckerberg: “I think anonymity on the Internet has to go away. People behave a lot better when they have their real names down.” (Cole 11)

Another problem with anonymity is the destruction of trust and relationships. The problem is that it’s hard to have trust built if you don’t know the people. You may also seem suspicious if you are anonymous and be held accountable under law in certain countries (Davenport). The other problem is hackers and other trouble makers. In fact 2011 was considered “the year of the hacktivist” due to cyber attacks on Sony, Google, Sega Corp, Citabank, CIA, government organisations and many other corporations. People blame anonymous hackers for this while others blame faulty coding and negligence. The final argument is that if you have nothing to hide, then you have nothing to fear about your invasion of privacy (Cole 147-150).

Another thing to consider is invasion of your privacy through government programs. Most recently and notably, an NSA program called PRISM has been revealed to the general public. PRISM allowed the NSA to obtain information such as email, photos, chat, videos, social networking, stored data, logins and much more from multiple companies such as Google, Apple, Yahoo, Skype, YouTube, Microsoft, AOL, Facebook and more. This was able to be obtained without a court order, nor warrant or consent from the public (Greenwald). According to the NSA leaks, surveillance had reached an extremely high invasive level including tapping everyone from American citizens to foreign countries. (Shah) Companies had to comply with these data requests under US law, leaving us to question how private our data really is and how much we are willing to accept the invasion of our privacy.

Another organisation that would be affected by transparency would be the highly controversial Wikileaks. Wikileaks is an organisation for whistleblowers who want to anonymously leak information in order to uncover ethically wrong or potentially controversial things that they want to be known to the world (Cole 93). Creator Julian Assange was a hacktivist earlier on whom infiltrated the Canadian communication system, leading to the invasion of his property and several charges, which may have contributed to his anti-authoritarian views. (Cole 88-89). Julius supported cyberpunks love of freedom, ideas of anonymity, hatred of a surveillance state and doing good in the world which led to the creation of the site for whistleblowers to unveil the wrongdoings of government organisations (Cole 90).

By far the most controversial group was an organisation called Anonymous or (ANON’s). This group portrays the sides of anonymity including mischief makers and activists and their potential to change the world with ever shifting principles and no main goals (Cole 56). WIth no true leaders, Anonymous is a group made out of mostly hackers with varying principles. The first stages were people whom loved to create mischief and wreck havoc through Online Drama to Real life attacks on the people they were opposing (Cole 46). Anonymous would troll people or entire groups, usually to teach them a lesson to them. (Cole 40) Another group called LulzSec carried out high profile attacks. The problem was that if anyone tried to report them, or discover them it would usually be found as fake and the reporter would be ridiculed. (Cole 36)

However, Anonymous began to evolve into a much bigger group, which much bigger intentions and a serious activist side advocating the freedom of speech, the case against internet surveillance, racial profiling and the war on drugs (Cole 61). One of their most famous missions and achievements was against the Church of Scientology whom were notorious for suppressing critical information, releasing false information and censoring the internet. Through a video ending with “We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.” (Cole 50-51) Anonymous started project Chanology which started a revolution by posting videos, blocking off the site, prank calls, real life attacks and fighting on so many fronts that they conquered and won for freedom rather than oppression online. (Cole 52-53). Other ANON’s use their anonymity for good and fighting evil in the world. They unearthed animal abusers, handed information on child pornographers to authorities, brought down websites containing illegal materials and leaked data on 190 people participating in these activities (Cole 46-47). Another example of their protests was Occupy Wall Street, a peaceful protest on Wall Street about abuse and corruption of banks and governments (Cole 87).

Another example on how people became activists through anonymity was demonstrated in SOPA. Though the GOFA targets authoritarian or repressive governments, it fails to solve the problem of democratic governments abusing internet surveillance and censorship. (Mckinnon) Anyways, SOPA was an insidious legislation that would have allowed service providers to shut down entire websites if they were found hosting illegally even one piece of copyrighted material. The opposition was so massive, it caused websites such as Tumblr, Wikipedia, Reddit and over 7000 other websites to host a blackout, Google to collect 7 million signatures against it and Anonymous attacks on industries supporting the bill. The internet won and the bill was never passed (Cole 222-223)

Internet privacy is a topic that won’t be settled without serious debate. As you can see, you must consider all aspects of pros, cons, ethics, group interests and so much more and deal with the consequences of whichever side you go against. Now it’s up to you and the rest of the world, whether you are for or against anonymity is for you to decide and act upon.