Internet Privacy And National Security Concern Under Internet And The Onion Routing

Internet help connects people worldwide as a powerful communication and information sharing platform. However, as the internet “requires the collection of certain data from individuals who visit websites—such as Internet address—in order for the site to operate properly”, every data the users provide may lead to privacy problems. Meanwhile, with the development of social media, it’s now never a hard task to collect one’s personal data through simple search. To address these privacy problems, there comes a new information technology called The Onion Routing, also known as the “TOR”. It provides the new possibility for securing the user’s information could hardly be traced while the user could still access the content. The anonymity this service provide raised serious concern about national security since the criminals also use its feature for anonymous contact and illegal activities. It’s hard to take the balance between national security and privacy but it’s something worth exploring.

What is privacy and why do people have the rights to it? Privacy is a noun that means “freedom from unauthorized intrusion.” in the Merriam-Webster dictionary. For most liberal countries, privacy and freedom are part of the best human rights. According to “A fresh look at privacy”, Magi argued that privacy matters to all human beings that it “provide space for disagreement and allows tolerance”. Privacy allows individuals to avoid the so-called “anticipatory conformity” that adds diversity to our culture and society. Internet privacy, as the extension of this concept, have its influence in multiple aspects. Not only do the end users need the privacy of passwords security or communication security, but also government agencies’ “highly sensitive financial and health data”. The widespread internet also brings the problem of “privacy paradox”, which means people are actually sharing more personal data online while still wants to keep their privacy. Magi also mentioned that people would choose to trust the “privacy policy” which means their privacy is protected, but these policies are generally “disclaimers indicating all the ways their personal data can be used”. For instance, Robin Li, the CEO of the biggest search engine company in China BAIDU, claimed that “If they [Chinese] are able to exchange privacy for safety, convenience or efficiency, in many cases, they are willing to do that, then we can make more use of that data” in 2018 China Development Forum held in Beijing. This incident evoked massive opposition against BAIDU at that time, and many Chinese people were calling for information privacy and were seeking for alternating choices other than using BAIDU.

Therefore, the onion routing was created, with the anticipation to secure information privacy, avoiding so-called “traffic analysis”. The heading of the packets sent out in the normal internet revealed too much information to possible internet surveillance even with encryption , which may leak what people are doing. For the onion routing, unlike the packets flow between routers and sends directly to the user, it forms a “distributed, anonymous network” that sent the packets through several places on the internet. The service creates a special network that the user’s packets first sends to A, then A sent these packets to B, and it back forth a couple of times. Though the browsing speed is sacrificed and the possibility of getting traced down still existed, the price to track is greatly higher than normal internet surveillance, since nobody knows where all these packets are going to apart from the two middle servers.

Honestly, the onion routing sounds a promising project that fight for human rights and citizen

rights of privacy, but there's just one problem: all the criminals also want anonymity to hide from police trace. In the shadow of our daily internet, there exists the dark web, which are unreachable by normal browser but onion routing. The dark web doesn't use the ordinary DNS system, but a whole different system. On the dark web, crimes are committed in the example of hitman service, illegal drop and weapon sales, terrorism, child pornography, fake ids, data breach and so on. Apparently, none of these are legal, but the onion routing are offering them a great place to conceal. National security is under serious threaten by these crimes, and these crimes may affect any of our normal citizens. No one wants see the tragedy of 911 incident again anywhere, but the reality is cruelty. In fact, according to "Going Dark: Terrorism on the Dark Web", some terrorists are using the dark web as a plat form to share content about "Hiding the Extremist Identity," "Earning Money," "Internet Privacy," "Training," "Bomb-Making," "Transporting Weapons," and "What Happens When You Are Spied On And Get Raided." For instance, one of the most famous terrorist group, ISIS, use the onion routing for recruiting, fundraising, and coordinating actions. Obviously, the onion routing wasn't preparing for these, and these terrorist websites in the dark web could be very hard to shut them down, unlike the surface network.

Even though, there are plenty of people still choose to stand on the side of online privacy and it's certainly reasonable. They believe that people's privacy is one of the most valuable thing in the world. We humans, as millions of individuals with own cognition, may have different view on various things. It's important to respect these voices and minds as they create a diverse world. And thus, privacy gives us the space to freely express our own opinion, which is part of the basic human rights freedom of speech. Moreover, privacy is closely related to information censorship. According to "Upholding free speech and privacy online: a legal-based and market-based approach for Internet companies in China", it is said that "In China, anyone who provides information to the public through the Internet, publishes works online, posts news articles, distributes audio-visual materials, or operates an Internet bulletin board, message forum, or chat room must first receive a permit from the appropriate government agency. " This means that any content that the government determined violating the government's ideology, the one who sent out this message would need to be responsible for what they've said, no matter in what circumstances. To achieve that goal, the Chinese government has regulations that force mainland internet companies to cooperate with the government to do information censorship, which is totally intolerable to these looking for liberty and human rights. For these people, the onion routing is the right place for them, not for cybercrime, but a great place to hide for any possible personal data leakage. To sum up, this group of people are willing to have as less regulation as possible, which may lead to potential crimes risks, but ensuring their human rights.

In contrast, there are other groups of people believe that nation security would be more important than individual privacy, since it's related to every single one of us. As I mentioned before, everyone could still recall what happened in September 11th, 2001, and I believe no one would it happen again. As these people would like to sacrifice more privacy to establish a better anti-terrorism world, they believe that individuals could hardly shape a better world with their own force. Thus, they choose to give this power to the government and merge this individual power to the power of the whole nation. They also hold the opinion that the privacy they gave up was actually protecting them and protecting society. According to a survey of Chinese's opinion towards current privacy problem in China mentioned in "Upholding free speech and privacy online: a legal-based and market-based approach for Internet companies in China", there are plenty of Chinese internet user prefers the internet getting managed or controlled by the government. In their opinion, "given the historical and cultural context that the government is

the most natural and trusted source of control", together with their doubt on the credibility of other online resources, especially from western media, they choose to trust information from the government. Cybercrime and fake news made "a sizable number of Chinese wary", particularly the dark web and the onion router, which could be explained why this group of people stands at the side of the government. Meanwhile, considering the internet companies in China mainlands that are required to take information censorship, controlling some information and taking some user privacy not only meet the government's requirement to do business in China but also satisfy the needs of a number of citizen's needs. The onion routing and the dark web is more likely a place for criminals in their eyes, since there are so much illegal activities happening on the dark web and could hardly be controlled. The overpower of individual freedom may lead to someone hiding behind the invisible mask, saying or doing some illegal activities with almost no harm. The onion routing means no good but great harm to their value. To sum up, they think the loss of some user privacy would gain these people less harm to fake information and cybercrime. For internet companies, they could tell users the privacy problem is because of the government regulation and do their business without harming their benefits.

There are also plenty of people choose to stand in between, like me, choose to hold a more neutral idea. The balance between individual rights and national security needs to be found, and laws and regulation need to be established. The technology itself could almost never be harmful, just like one couldn't tell a knife or a gun is harmful. What is important is how the knife or the gun, in our case, the onion routing is being used. In fact, "The Digital Underworld: Combating Crime on the Dark Web in the Modern Era." told us that the statistics have told us there are more people choose to use the onion routing for anonymous but not for crime-related activities. To be honest, the different opinions towards this privacy problem is also because a diverse view of this privacy problem and people need to respect all different voices. As mentioned in "Upholding free speech and privacy online", though the control of the internet and privacy may contribute to stability, realizing the benefit bring by a more opening internet and why it would not threaten society stability is critical.

Early in 1948, the Universal Declaration of Human Rights (UDHR) gave the standard of international human rights agreements. "Upholding free speech and privacy online" suggested that in article 12 of the UDHR outline, stated about privacy, telling that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence….". There are long agreements of why human rights matters and what to do to protect human rights. On the other hand, police and government agencies all over the world are taking a close eye on the onion routing, being prepared to fight against cybercrime at any time and place. According to "Going Dark: Terrorism on the Dark Web", various kinds of efforts are made to regulate the onion routing service, through Web mining technology, identify users and other ways to monitor the dark web. These have shown that both the government and the normal people have raised great attention and concern to the national security the onion routing brings. Interestingly, the user of onion routing is gaining at the same time. I suppose this could be a sign of people are caring the national security while still keep human rights in their minds, for both of them are equally important.

In conclusion, onion routing is providing people with a cheap and convenient solution to secure their online privacy and human right of freedom, it may lead to national security concern. While extreme privacy would make cybercrime no cost, and extreme regulation would harm the human rights, finding the right middle place is thus particularly important. There're reasons from a different perspective for both side, but fortunately, more people are realizing the core conflict,

choosing to utilize the onion routing technology while caring national security regulations.

Reference:

1. Dwyer, Catherine; Hiltz, Starr Roxanne; and Passerini, Katia, 'Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace' (2007). AMCIS 2007 Proceedings. 339.
2. Privacy(2019). In Merriam-Webster dictionary. Retrieved from https://www.merriam-webster.com/dictionary/privacy (//TODO)
3. Greengard, S. (2008). Privacy matters. Communications of the ACM, 51(9), 17-18.
4. Magi, T. (n.d.). A Fresh Look at Privacy - Why Does It Matter, Who Cares, and What Should Librarians Do about It? Retrieved from http://journals.iupui.edu/index.php/IndianaLibraries/article/view/4229.
5. Shen Xinmei. (2018, Mar 28). Chinese internet users criticize Baidu CEO for saying people in China are willing to give up data privacy for convenience. Abacusnews. Retrieved from https://www.abacusnews.com/big-guns/chinese-internet-users-criticize-baidu-ceo-saying-people-china-are-willing-give-data-privacy/article/2139313
6. Scherer, L. (2014). Privacy (Introducing issues with opposing viewpoints). Farmington Hills, Mich.: Greenhaven Press, a part of Gale, Cengage Learning.
7. United States. General Accounting Office. Accounting Information Management Division. (2000). Internet privacy : Comparison of federal agency practices with FTC's fair information principles. Washington, DC: The Office.
8. Vogt, Sophia Dastagir. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, 15(1), 124.
9. Weimann, G. (2015). Going Dark: Terrorism on the Dark Web. Studies in Conflict and Terrorism., 39(3), 1-12.
10. Yutian Ling. (2011). UPHOLDING FREE SPEECH AND PRIVACY ONLINE: A LEGAL-BASED AND MARKET-BASED APPROACH FOR INTERNET COMPANIES IN CHINA. Santa Clara Computer and High Technology Law Journal, 27, 175-793.