Internet Privacy

Name

[Institutional Affiliation(s)]

Author Note

# Internet Privacy

Internet privacy consists of subset of a larger set of data privacy that includes the use, collection and storage of confidential information. In the United States, privacy right of individual has always been cherished. This is due to the reason that the consequences of privacy intrusions for individuals can be disastrous. Cyber threats can come from many different sources that are related to the use of personal information for exploitation and benefits. There is a need for more regulatory safeguard measures regarding internet privacy. The internet privacy policy is mostly concern with how internet privacy is exposed over the web through data collection, tracking, cybersecurity and data sharing threat.

According to one research study, it is found that internet privacy is very important for almost 74% of the Americans and more than 86% of the Americans have taken different actions to maintain their internet privacy by adopting different procedures such as encrypting email, deleting cookies and IP address protection (Carlson et al., 2018). The invent of tracking technologies known as cookies brought a myriad of resources and helpful tools. Although the internet has achieved great popularity among the general public, most of the people are not familiar with the level of privacy and security on the internet.

According to a survey, 82% of the people showed dissatisfaction with "user profile". This paper will analyze certain policies related to internet privacy and ethical concerns for implementing these policies. A practice which different companies use to track and record data. Whenever a person visits website, enter his debit or credit card number, fill out online forms, sign up for new accounts, post on some social media site, store document or image in cloud storage release personal information and data into cyberspace (Tesfay et al., 2018). The definition of internet privacy differs across different cultures and individuals (*The coming privacy crisis on the Internet of Things | Alasdair Allan | TEDxExeterSalon*, n.d.).

The internet serves as the main means of communication and it is a platform of financial transaction and exchange of critical data. With the increasing use of the internet for different purposes, a new concept of internet privacy has evolved. It deals with addressing the user information security need and also the prevention of disclosure of web user personal information without their consent. In recent years' technology made it possible to view user information that is shared on the web (Gul et al., 2017).

The information can be leaked for the wrong reason by invading the internet privacy (Heimes, 2017). This gives rise to the concern of ethical issue regarding the protection of confidential information from unauthorized access. Internet privacy invasion can be avoided with the implementation of strict privacy laws; every act cannot be classified as illegal or legal, for example, monitoring of web user online habit to target potential customers by an advertiser is not illegal. It is ethics which draw the line between breaching user privacy and ensuring network security. In the United States, many laws cover data privacy and internet security. The internet privacy act was passed to create control over the maintenance, collection, dissemination and use of personal information by different agencies in the main branch of the United State government. The internet invention changed the privacy definition and made it important to legislate new laws concerning electronic security and communication. Sharing confidential and personal information through email and transaction means that information or data is no longer remain confidential. However, for ethical and technical reasons, providers of email service do not use information in the wrong manner.

# Ethical Guidelines

There are ethical issues regarding reading and storing of emails without the consent of users. With the help of an automated system, emails are scanned by Google. They use this to detect malware and spam and also to tailored advertising (Carlson et al., 2018). The content of the email, YouTube views, Google profile and map requests are all analyzed and information is further used to create the advertisement. The indexing and scanning cannot be turned off fully thus making it a serious ethical issue in information and data privacy (Carlson et al., 2018). During online shopping, people share their bank account details and credit card number on the shopping portal which increase the risk of these details being used for the fraudulent and unethical purpose (*The coming privacy crisis on the Internet of Things | Alasdair Allan | TEDxExeterSalon*, n.d.). On social networking sites, people through status update let everyone know about their location and personal life details. One of the main ethical concern is whether third parties are allowed to read or store emails without the consent of the person or track visitors on their website or not (Kernighan, 2017). Facebook has very little ways to restrict or protect others from accessing the profile information of a user.

The government holds very important information about people. National security can be threatened if the security of this information is compromised. Therefore, there is a great need that Federal websites maintain a high level of privacy standards to protect a large amount of critical information. The degree of government access to citizen personal information raises the ethical concern in data privacy. There are many organizations which store critical information and personal details of their users (Kernighan, 2017). These include medical facilities that contain medical record, banks that contain account holder's financial records, educational institutes that have the education and personal details of students and companies that contain a record of the employee.

In the United States, most of the people are employed in handling, collection, distribution and use of information. Mason stated four ethical issues that are related to the information age: accuracy, privacy, access and property. Privacy is a main part of ethics and data accuracy. The internet privacy protection is the main principle of this current age of technology. More than half of the Americans think that their personal information is not secure than it was 5 years ago. In 2017, there was a disastrous breach at Yahoo admission that result in billions of compromised email account.

Over the years the potential for breach of internet privacy has significantly increased. There is no single law that regulates online privacy. In the United States, many laws regarding internet data security and privacy are available with the privacy act 1974 being the base for all. A patchwork of state and federal law regarding internet privacy include different laws related to internet privacy. The new technologies and internet continually raise new privacy and policy questions. There is a need to address these privacy issues on a priority basis (Carlson et al., 2018). The lawmaker’s documents state laws regarding the personal information held by providers of internet service, website privacy policies, email monitoring, online marketing and reader browsing information.

# Current Laws and Policies

The California Consumer Privacy Act (2018) allows the consumers to request the disclosure of specific personal information that is collected. According to this act, the consumer can request business to delete the personal information (Carlson et al., 2018). This law puts greater restriction on collecting and using information and data by companies. The Federal Trade Commission Act (1914) regulates deceptive and unfair commercial practices. This act is a primary federal regulator in the area of privacy and brings actions and enforcement against companies. This usually includes failing to comply with protection of personal information and privacy policies. The Electronic Communication Privacy Act (1986) protects electronic, wire and oral communications from unauthorized access disclosure and interception (Carlson et al., 2018). The Computer Fraud and Abuse Act makes some computer-related activities unlawful. This includes the involvement of unauthorized and illegal access of a computer to get access to certain information, transmit harmful items and obtain data or passwords by wrong ways (*The coming privacy crisis on the Internet of Things | Alasdair Allan | TEDxExeterSalon*, n.d.). The Children Online Privacy Protection Act requires that online service providers and some websites obtain consent before using, collecting and disclosing any data from minors under 13 years of age (Carlson et al., 2018). Under this act, websites are required to collect only the necessary information, post online privacy policy and maintain and create security measures.

Two types of privacy issues raised with the use of internet. First, the aggregation and posting of personal information on the websites violate privacy sometimes. Websites contain all kind of personal information that is made available publicly often without the consent of the person such as a personal address, phone numbers, pictures and video clips. The second ethical issue includes internet user online monitoring (Carlson et al., 2018). The ethical issue related to internet privacy is the use of malicious software and spyware to commit cybercrime and to steal private information. In the US, most of the cybercrime has been outlawed which reflects a consensus that information stealing is wrong.

In the US, Federal laws against the internet privacy covers credit card fraud, deceptive and unfair law against cybercrimes, fraud in relation with computers, access devices and identification of information and documents. According to these laws, it is illegal to invade the person privacy to steal their information (Carlson et al., 2018). In 2014, according to the Guardian, some of the best security investigators were under the indictment threat to expose the internet infrastructure. The United States, Computer and Abuse Act makes illegal the breaking and hacking of private system and networks (Carlson et al., 2018). Threats to internet privacy do not only come from criminals and information can be leaked from Google and Facebook. In the last few years, it is reported that user's private information on Facebook has been shared on different websites and applications that are further use for data mining.

# Challenges in Implementing Ethical Guidelines

It is very easy for hackers to hack into any system or computer as long it is connected to the internet. They can use an IP address to access the computer of the user and collect information for the wrong purpose (Kernighan, 2017). The widespread use of internet cookies also makes it easy to collect any information and exposed internet users to high risk of conflicting and fraud interest. Most of the companies and organizations use these cookies to found which service or product they can advertise to us (Carlson et al., 2018). In online banking, hackers can transfer money into their account which affects both customer and bank who is using online technology of banking. Although the internet has enabled people to share and find relevant information, it also exploited the freedom of privacy (*The coming privacy crisis on the Internet of Things | Alasdair Allan | TEDxExeterSalon*, n.d.). There are different ways in which privacy is exploited such as the use of webcams.

In the last few years, many people have become a victim of an online stalker. The ethical guidelines regarding internet privacy should recognize the personal freedom and autonomy. The ethical guidelines also provide a framework of actions regarding the handling of private information. In the view of the law, once the private information of a person has made public, it's no longer consider as private. The freedom and autonomy of a person should be regarded as confidential therefore person information must be handled with confidentiality (Carlson et al., 2018). This implies control and security of the information access and the right to use it. Privacy policy regarding the internet privacy should be formulated consisting of elements such as confidentiality level, use and purpose of information, and the procedures to ensure the information accuracy based on the norms of truth, freedom and human rights (Kernighan, 2017). Private and personal information or data that is no longer necessary must be collected and destroyed. No unnecessary personal and private information must be collected. This should not only for the logistics aims but also to prevent the unnecessary exposure and violation of person privacy. The companies must notify the user about the use of their private information.

The privacy policy should be posted on all websites. Websites that specifically directed at children under 13 years of age must post a notice that includes type of information collected from children, information dissemination plan, the intended use of data and information and involvement of third parties (Carlson et al., 2018). Different companies are hired specifically to watch which websites are mostly visited by people and then use the information available on these websites for different purposes (Carlson et al., 2018). The directly observed behaviour such as the content of the profile on Facebook, search queries and browsing logs can be processed automatically to infer details of an individual's such as religious and political views, sexual orientation, personality, intelligence, substance use and race.

The concerns associated with internet privacy usually cite different privacy risks and events that can compromise privacy that can be encountered through use of the internet (*The coming privacy crisis on the Internet of Things | Alasdair Allan | TEDxExeterSalon*, n.d.). These range from collection of user statistics to the spread of spyware and exploitation of different kinds of bugs. Different websites protect the personal information of their users. For example, on Facebook, the privacy setting is present to all registered users. People can block some individuals from viewing their profile and limit access to their pictures and videos (Carlson et al., 2018). The privacy setting is also available on some other social networking sites such as Twitter and Google Plus. The Electronic Frontier Foundation has formulated different guidelines for users regarding the use of these privacy setting

Various ethical concerns need to be considered during application of these laws for the use of these websites or applications. The laws should be more complex and strict for such applications that store private information data. The Abuse Act make some computer-related activities unlawful counting the unauthorized and illegal access of a computer to get access to certain information, transmit destructive items and obtain data or passwords by wrong ways (Carlson et al., 2018). Most of the websites take consent before using, accumulating and revealing any data from minors under 13 years of age. Under different acts, websites and applications are required to assemble only the essential information, post online privacy policy and preserve and generate security measures. Certain applications and websites require all of the essential details and it remains to save on clouds. The paper has significantly identified certain policies and ethical guidelines to establish privacy laws. These laws need specific privacy concerns to be maintained to protect data and information of communities.

# References

Carlson, E., Goldberg, R. M., McHenry, G., Lewis, M., & Romzek, W. (2018). Trends in Internet Privacy and Security Perceptions and Online Activity. *Available at SSRN 3142220*.

Gul, S., Asif, M., Ahmad, S., Yasir, M., Majid, M., & Malik, M. S. A. (2017). A survey on the role of internet of things in education. *IJCSNS*, *17*(5), 159.

Heimes, R. S. (2017). Internet privacy law, policy, and practice: State, federal, and international perspectives. *Maine Law Review*, *54*(1), 95.

Kernighan, B. W. (2017). *Understanding the digital world: What you need to know about computers, the internet, privacy, and security*. Princeton University Press.

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018). PrivacyGuide: Towards an implementation of the EU GDPR on internet privacy policy evaluation. *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, 15–21.

*The coming privacy crisis on the Internet of Things | Alasdair Allan | TEDxExeterSalon*. (n.d.). Retrieved January 5, 2020, from https://www.youtube.com/watch?v=yG4JL0ZRmi4

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258.