Internet Privacy

Matthew N. O. Sadiku, Sarhan M. Musa, Osama M. Musa

***Abstract*— The benefits of the Internet have come at some cost, one of which is a loss of privacy, which is often regarded as a moral right or a legal right. Internet privacy is primarily concerned with protecting user information. It is widely acknowledged as the top consideration in any online interaction. New threats to privacy and civil liberties are emerging daily and privacy practices are not one size fits all. This paper provides a brief introduction to online privacy.**

***Index Terms*— Internet privacy, online privacy, information privacy, database privacy**

I. INTRODUCTION

The concept of privacy is deeply rooted in modern civilizations. It has been a sensitive issue even before the advent of computers. Now the Internet is invading private space and
it is having a profound impact on aspects of our lives, patterns of work, the means
whereby we interact, with whom we interact, and the cultures within which we live.
Privacy can be classified into four types: privacy of personal data, physical privacy, territorial privacy, and the privacy of communications [1].

New technologies are making it easier for governments and corporations to monitor our online activities like never before. These infringements on personal privacy have devastating implications for our right to privacy. Privacy protects us from abuses by those in power. China, for example, is well known for its policy of censorship when it comes to the spread of information through public media channels.

Privacy can be understood as a specific form of freedom and therefore the same measures apply to both. Privacy is the right to an inviolable private life. Internet privacy (or online privacy) consists of privacy over the media of the Internet: the ability to control what information one reveals about oneself over the Internet and to control who can access that information. Protecting information privacy in the United States is largely the responsibility of individuals who are expected to guard their personal information and minimize the risk that it will be used in an unauthorized way [2]. However, it is difficult for individuals to police their privacy violations.

Matthew N. O. Sadiku, Roy G. Perry College of Engineering Prairie View A&M University Prairie View, TX 77446
Sarhan M. Musa, Roy G. Perry College of Engineering Prairie View A&M University Prairie View, TX 77446
Osama M. Musa, Ashland Inc. Bridgewater, NJ 08807

II. PRIVACY BREACHES

There are many ways in which people can divulge their personal information. For example, sending bank and credit card information to various websites. Using a social network such as Facebook and MySpace can automatically provide intrusive details about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality. Social networking sites have received a lot of attention concerning breaches of privacy of their users. Privacy settings are available on other social networking sites and the user can apply such settings when providing personal information [3].

Internet of Things (IoT) are everywhere - at homes, in cars, in hospitals, etc. IoT connects everyday objects such as thermostats, door locks, webcams, televisions, alarms, garage openers, power outlets, sprinklers, etc. However, all those benefits can come of the risks of privacy loss and security issues.

Today teenagers will spend the equivalent of 23 years of their lifetime on the Internet; I0 years of that span will be spent on social networking sites. Most these teens are unaware and unconcerned about protecting their privacy online [4]. As privacy invasion among teens increases, there is a need to develop effective privacy education for teens and their parents.

Data snooping (an electronic version of eavesdropping) is the process of legally or illegally using technology to gain access to personal information about you. Government uses cybersurveillance to monitor criminals or people they want to track. Organizations implement workplace surveillance to ensure that there is no misuse of time and computing resources. Crackers spy on your personal data and use it for malicious intent. For example, an identity theft would snoop to get credit card number and bank account and use them for their own gain.

III. ACHIEVING PRIVACY

Achieving privacy online is hard. Fulfilling customer privacy requirements is often difficult. Academia, business, and governments have proposed a range of solutions for information privacy and security problems which currently plague the Internet. A number of technologies have been developed in order to achieve information privacy goals. Some of these Privacy Enhancing Technologies (PET) are described as follows:

- *Virtual Private Networks* (VPN) are extranets established by business partners. As only partners have access, they promise to be confidential and have integrity.
- *Transport Layer Security* (TLS), based on an appropriate global trust structure, could also improve confidentiality and integrity.
- *DNS Security Extensions* (DNSSEC) make use of public-key cryptography to sign resource records in

order to guarantee origin authenticity and integrity of delivered information.

- *Privacy Enhanced Mail* (PEM), using cryptographic algorithms, represents a major effort to provide security. The message is protected against attacks such as wiretapping [5].

Software for computer surveillance includes spyware and adware, which reside on your computer and work like electronic spies.

Internet users may protect their privacy through controlled disclosure of personal information – sex, age, account, physical address, IP address, email address, etc. They can protect themselves by updating virus protection, using security settings, installing a firewall, and using encryption.

Information privacy refers to the claims of individuals that data about themselves should generally not be available to other individuals and organizations without their permission, and the individuals must be able to exercise a substantial degree of control over that data and its use. They should be given the ability to choose whether they want to share their information with an entity or not. Failure to do this will result into privacy breaches.

A. CHALLENGES

There are a number key challenges policy makers must consider when determining action related to online privacy.

The lack of consumer confidence in information privacy is a major problem hindering the growth of e-commerce. Many privacy advocates and activists are concerned about the dangers of government control and related political problems. They argue that ethical approaches must incorporate fairness, transparency, participation, accountability, and legitimacy in the collection and handling of data. In order for Internet privacy initiatives to be successful, they must be accompanied by tools and procedures to provide strong security.

Cultural differences have been shown to affect individuals' expectations and privacy concerns. Digital literacy plays a crucial role in promoting information privacy. Legislature is important in establishing incentives that encourage compliance and disincentives that discourage inappropriate online behavior.

Although Federal regulations exist to mandate how sensitive information of individuals can be used by organizations, there is need to establish Information Privacy Principles that impose responsibility and conform with a comprehensive set of privacy protection principles [6]. Open and democratic processes are necessary for meaningful protection of values such as freedom and privacy. Standards efforts should create mechanisms for inclusion of input from a wide range of Internet users.

IV. CONCLUSION

Governments are often expected to preserve Internet privacy. Most states in the US have enacted legislation that increases employee and job candidate privacy rights by limiting employer access to their personal online information. But governments are among the main privacy violators, in pursuit of criminals.

Although the Internet has emerged as a significant marketing tool, privacy concerns could drastically affect e-commerce or purchasing online. Given that teenagers are constantly exposed to temptation from commercial web sites and they are not protected by federal laws, it recommended that children under the age of 18 must be protected from privacy violations [7]. Software engineers and project managers should make sure that the system functionality matches the privacy statement's claims.

REFERENCES

[1] S. Smirnov, "Privacy on the Internet," *Russian Politics & Law*, vol. 39, no. 5, 2001, pp. 52-63.

[2] J. P. Nehf, "Shopping for privacy on the Internet," *The Journal of Consumer Affairs*, vol. 41, no. 2, Winter 2007, pp. 351-375.

[3] "Internet privacy," From Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Internet_privacy

[4] G. D. M. and C. Linda, "A call to action: the privacy dangers adolescents face through use of facebook.com," *Journal of Information Privacy and Security*, vol. 6, no. 2, 2010, pp. 17-32.

[5] S. T. Kent, "Internet privacy enhanced mail," *Communications of the ACM*, vol. 36, no. 8, August 1993, pp. 48-60.

[6] R. Clarke, "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, vol. 42, no. 2, February 1999, pp. 60-67.

[7] F. Krohn, X. Luo, and M. K. Hsu, " Information privacy and online behaviors," *Journal of Internet Commerce*, vol. 1, no. 44, 2002, pp. 55-69.

AUTHORS

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.

Osama M. Musa is currently Vice President and Chief Technology Officer for Ashland Inc. He also serves as a member of the Advisory Board at Manhattan College's Department of Electrical and Computer Engineering as well as a member of the Board of Trustees at Chemists' Club of NYC. Additionally, he sits on the Advisory Board of the International Journal of Humanitarian Technology (IJHT).