Anonymity on the internet argumentative essay

Law, Criminal Justice

Introduction

The Edward Snowden scandal exposed massive electronic surveillance operations by the National Security Agency, which may have involved considerable violations of individual rights to privacy (Puddephatt, et_al, 2012). Privacy is an inalienable human right, whose meaning has, however, defied cross-generational efforts to understand and assert. It underpins other fundamental human dignity, integrity, freedoms and rights, including the freedom to belief, association and expression. Despite the difficulties in defining and understanding privacy as a construct, especially in the context of constantly changing technologies, it is easily acceptable that it amounts to the ability to communicate/live with/in anonymity, without governments or other third parties prying into the identity or content of the communications and personal life. Indeed, it will be impossible to safeguard the personal and political space guaranteed by constitution without a fiercely guarded right to privacy. This paper argues that unless otherwise limited by established law and the need to protect legitimate collective good, the right to privacy must be safeguarded at all times. It argues that anonymity protects the vulnerable and protects individuals' rights to free expression and democratic participation.

Background

The right to, and ability to exercise is essential to open, liberal and democratic societies (Puddephatt, et al., 2012). Prior to the digital revolution, the right to privacy could not only be easily defined, by it could be similarly enforced. However, modern communications technology has made it

relatively easy to infringe on the individuals' rights to privacy, often without them noticing. The internet resulted in multiple tools for gathering and processing new types of personally identifying information, which was unfeasible a few decades ago. It facilitates the surveillance, collection, location and processing of information, which can be easily traced back to the sender/receiver. As perhaps best emphasized by the NSA's PRISM program and hacking scandals, the internet has created new technologies for governments and private actors to gain possession of private communications and data, for commercial, criminal or law enforcement purposes. Further, the nature of the internet also makes it difficult to define and enforce clear boundaries between the right to privacy and legitimate infringement of the right to privacy. Further, efforts by governments to fight crime and terrorism have seen the enactment of laws such as the PATRIOT Act (2001), which give law enforcement agencies sweeping surveillance capabilities to the detriment of privacy.

Definitions

- PATRIOT Act (2001) - It is an acronym for a law enacted after 9/11 to allow law enforcement agencies to prevent and investigate threats to the nation.
- IP Address- Stands for Internet Protocol and it refers to a unique numerical address assigned, and used to identify every computer connected on the internet.

Right to Anonymity

Protecting individual citizen's rights to privacy extends to ensuring that they remain anonymous while surfing or sending communications over the

internet. According the United States Supreme Court in McIntyre v. Ohio held that the anonymous free speech is protected under the First Amendment. The Court argued that protections for free, anonymous speech are critical to the democratic discourse. It ensures that dissenters are able to protect their identities, effectively freeing them to express important minority views. Anonymity ensures that the tyranny of the majority does not infringe upon the minority's democratic and other rights. This embodies the very purposes envisaged by the First Amendment. Further, access to, use and disclosure of personal and personally identifying information amounts to search and seizure as defined under the fourth amendment, requiring a subpoena and/or warrant by a competent court, Katz v. United States (1967). Effectively, ensuring the anonymity of internet users simply amounts to safeguarding their rights to privacy in the context of a new technology. It ensures that individuals are free to exercise their freedom to free speech, expression and association in dignity and with integrity. This premise is perhaps best emphasized by the fact that in the most repressive nations in the world such as China and North Korea, governments often resort to electronic communications to deter free expression (Puddephatt, et_al, 2012). Further, internet anonymity is necessary to protect vulnerable members of society (Puddephatt, et_al, 2012). In a recent study, the European Network and Information Security Agency established that the protection of young people is critical to preventing abuse (e. g. cyber bullying) and grooming. Properly designed internet platforms that are simple ensure that young people can safely use the internet. The need to use true identities or use platforms that readily reveal personally identifying information such as IP

addresses only exposes the most vulnerable members of society to bullying, fraud and exploitation. In this way, the internet would be more productive and valuable to all members of the population (Landau, 2005).

Ironically, crime and fraud are the main reasons behind the aggressive limitations on the right to privacy and anonymity on the internet. The internet has become extremely critical in commerce and as a communication tool. It is prone to fraud and can even be used to finance or facilitate terrorism. Anonymity will impede efforts by law enforcement agencies to discharge their responsibilities effectively. Indeed, this is the very motivation behind legislation such as the Patriot Act and the Communications Assistance for law Enforcement Act. With the current setup, individuals can enjoy their rights to privacy, but such rights may be infringed upon through a legitimate court-warranted process, only when there is a probable cause to warrant such an infringement. The difficulty with this assertion stems from the fact that this system is open to massive abuses by governments and criminals as perhaps best emphasized by the NSA PRISM program. Fraud is also possible because of their ability to access personally identifying information because of flawed encryption and other security mechanisms (Gates & Privacy Working Group, 1995).

Further, it argued that data and information gathered from internet uses finances the internet and allow innovation and service provision. Companies such as Facebook, Twitter and Instagram thrive on the back of their ability to mine, process and sell user data to marketers and others businesses. Without this incentive, the business models of most internet companies will collapse. If this happens, the incentive for internet companies to offer

valuable services and innovate may decline, leaving them with the necessity to charge for their services or wind up (Gates & Privacy Working Group, 1995). However, this argument is self-defeating, because it defines the very problem with privacy infringement. Revenue models that rely on capturing and passing on user information to third parties are in themselves an infringement. It is still possible to legitimately mine and use user data even with user anonymity.

Conclusion

Protecting people’s rights to privacy extends to ensuring their free exercise of anonymous speech. This ensures that they not only have dignity and integrity, but perhaps most importantly, this underpins the ability of individuals to exercise a range of other rights are freedoms. The First and Fourth Amendments envisaged the right to privacy in terms of the ability to communicate anonymously, and in a manner that is free from political or other repression. Effectively, in order to achieve this purpose, it is necessary to ensure that people remain anonymous on the internet. There are legitimate arguments that this may render law enforcement impossible, but this assertion is undermined by rampant abuses by both governments and private parties (Puddephatt, et al., 2012).

References

Bellovin, S. M., Blaze, M., Clark, S., & Landau, S. (2013). Going Bright: Wiretapping without Weakening Communications Infrastructure. IEEE Security & Privacy, vol. 11, no. 1, 62-72.

Doyle, C. (2012). Privacy: An Overview of the Electronic Communications

Privacy Act. Congressional Research Service.

Gates, J., & Privacy Working Group (1995). Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information. New York: Information Policy Committee, Information Infrastructure Task Force.

Landau, S. (2005). CALEA and Network Security: Security, Wiretapping, and the Internet. New York: EEE Security and Privacy.

Landau, S. (2005). Security, Liberty and Electronic Communications. Seattle: Sun Microsystems.

Puddephatt, A., et_al. (2012). Global Survey on Internet Privacy and Freedom of Expression. Paris: UNESCO Publishing.