POSITION PAPER

Committee: United Nations Human Rights Council (UNHRC)
Topic: The Right to Privacy in the Digital Age
Country: The Kingdom of Denmark
Delegate: Parth Gurjar (Delhi World Public School, Noida Extension)

In the digital age, privacy refers to the protection of an individual's information that is used or created while using the Internet on a computer or personal device. In other words, digital privacy is the information available online about a given person is within his or her comfort zone. It can be classified as

1. Information Privacy
2. Communication Privacy
3. Individual Privacy

The right to privacy in the digital age demands a united, multinational alliance that will ensure all individuals in the world share an inalienable right to protect their identities or personal information. Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the current focus on the right to privacy is based on some new realities of the digital age. Personal spaces and safeties that were previously granted simply by physical separation are no longer protected. When it comes to digital data like photos, conversations, personal information, health information and finances, nothing can be perfectly private. Internet users are increasing aware of this, and increasing wary of institutions charged with protecting their data.

Digital technologies do not exist in a vacuum. They can be a powerful tool for advancing human progress and contribute greatly to the promotion and protection of human rights. When it comes to privacy in digital age nothing is private It can be hacked or possessed by hackers.

Right to privacy in digital age

Individual privacy is an important dimension of human life. The need for privacy is almost as old as the human species. Definitions of privacy vary according to context, culture, and environment.

Generally, privacy is viewed as a social and cultural concept. With the ubiquity of computers and the emergence of the Web, privacy has also become a digital problem. In particular, with the Web revolution, privacy has come to the fore as a problem that poses a set of challenges fundamentally different from those of the pre-Web era. This problem is commonly referred to as Web privacy. In general, the phrase Web privacy refers to the right of Web users to conceal their personal information and have some degree of control over the use of any personal information disclosed to others.

Digital privacy is simple to understand but difficult to keep track of. The more a user shares over the social networks, the more he will be prone to losing his privacy. All the information and data shared is connected to clusters to similar information. As the user keeps sharing his productive expression, it gets matched with the respective cluster and his speech and expression is no longer just with him or with his social circle. This is a consequence of bridging social capital as we create new and diverse ties on social networks, data becomes linked. This decrease of privacy continues until bundling appears. No one shall be subjected to arbitrary or unlawful interference with

his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Country Policy:

The Data Protection Agency is the central independent authority that makes sure the Act on Processing of Personal Data is obeyed in Denmark. Amongst other things it provides counselling, advice, treat complaints and perform inspections of authorities and companies. It comprises The Data Council and a secretariat. Anyone can complain to The Data Protection Agency if they feel Act on Processing of Personal Data is not obeyed in Denmark.

- According to the Danish law, all Internet traffic must be logged, registered and stored for one year.
- The Danish Ministry of Justice suggest a 10 years post-mortem data protection which contains the details of citizen's understanding of digital privacy.
- Denmark's Data Retention Law, which was passed in 2007, exceeds the requirements of the European directive in several respects, making it the most comprehensive law of all the member states.
- Provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, implementing the General Data Protection Regulation. The Data Protection Act repeals the previous Act on processing of personal data, which had implemented the data protection directive.
- The Danish Surveillance law is the ratification of the European Union's Directive, which requires all providers of communication like telephones and internet to log certain data regarding the communication through their systems.

Possible Solutions:

We categorize solutions to the Web privacy problem based on the main enablers of privacy preservation. The two main categories are technology and regulation-enabled solutions. The implementation approach further refines this taxonomy.

Technology-enabled solutions
A typical Web transaction involves a Web client and a Web server. We classify technology-enabled solutions according to the type of Web entities that are responsible for their implementation: clients, servers, or clients/servers.

Regulation-enabled solutions
Regulation-enabled solutions encompass two types: self and mandatory regulation solutions. Self-regulation refers to the information keepers' ability to voluntarily guarantee data privacy. Mandatory regulation refers to legislation aimed at protecting citizens' privacy while they transact on the Web.

Conclusion:

The internet was not designed with privacy and security at top of mind. It was built to spread information, not contain it, and has in succeeded at this central objective in spectacular fashion. As the internet and digital economy mature, however, privacy and security are now rising on the list of priorities for consumers and increasingly for policy makers as well.

We hope that the situation might improve for the right to privacy, but the future appears bleaker. Since the advent of a digital society with online accounts, organizations that harvest user data have amassed tremendous powers. While certain merits can be argued for collecting user data, an equivalent responsibility remains to regulate and secure any stored personal data. Our identities are the most valuable thing we own. They are a form of wealth: identity capital. We should expect our identities to be protected from embezzlement and exploitation.

The UN must be proactive and provide a forum for those whose privacy is threatened. It is the responsibility of the international community to foster privacy-enhancing technologies that will protect all individuals equally.