Forum: Youth Assembly

Issue: Measures to protect personal privacy on the internet

Student Officer: Sofia Sajjid

Position: Head-Chair

Introduction

The issue of invasion of personal privacy on the internet is, simply put, a threat to our safety and security.

Internet privacy is primarily concerned with how private information is exposed on the Web through tracking, data collection, data sharing, and cybersecurity threats. These threats come from various sources, all seeking to obtain personal information for their own gain or exploitation.

The majority of criticism from privacy activists has been directed at marketing firms, who stand to profit as much as anyone from the acquisition of personal data. More internal and regulatory precautions are required in response to the more powerful breaches.

Definition of Key Terms

Internet of Things

Computer gadgets which are installed into common objects and are connected via the internet to exchange data.

Internet Service Provider (ISP)

A service that gives customers access to the internet.

Privacy Enhancing Technologies (PETs)

Systems that uphold core data protection principles by maximizing data security and minimizing the use of personal information.

Key Issues

Cookies and Clickstreams

Cookies are a type of small text file that is frequently used to collect user data from websites discreetly. During online transactions, websites save these files on users' computer hard drives. Because they might violate a person's online privacy by gathering data about the user and his or her activity, cookies have the potential to have a dual nature.

Websites are not the only entities that keep tabs on you. Web publishers only have access to user information from their own websites, however ISPs (Internet Service Providers) keep a complete log of all of your internet activity. User data may be compiled into anonymous logs and sold to other businesses for use in marketing analysis, trend research, and other purposes.
This clickstream data poses a major threat to one’s privacy if it falls into the wrong hands.

Biased Systems

The economics of privacy continue to reward those who violate privacy laws. On the one hand, business models may be restricted by the cost of developing Privacy-enhancing Technologies (PET), their enforcement, and audits of privacy protection measures. In contrast, abuses of privacy laws either go unpunished or simply result in minor fines, and there isn't yet enough public awareness of the issue to cause unbearable harm to the public's reputation.

Corporations may deliberately breach their own privacy policies and prioritize other commercial objectives over their agreements with clients. People face the burden of proof and have no alternative for establishing wrongdoing because they are unaware of how their personal data may be distributed.

Thus, disregarding privacy legislation, for example, Google deliberately circumventing Safari's user tracking protection, seems profitable. Over this incident, Google paid a

record fine of $22.5 million in a settlement with the Federal Trade Commission, but it is conceivable that the earnings more than compensated for this loss.

Data Mishandling

Hoarding data is becoming more of a hazard than an asset. Users must provide personal information to a number of websites on the internet in order to use their services. This data is frequently not encrypted and thus accessible to anyone.

The improper management of personal information could have serious repercussions. The threats related to online privacy have increased as a result of the modern trend of e-banking and e-business portals. By posting your bank account information and other sensitive information online, you open the door for thieves and expose yourself to hackers.

According to a 2015 Perspecsys report, 57% of IT experts are unsure of exactly where sensitive data is located. For instance, in their development and quality assurance environments, software engineers use production cardholder data (i.e., debit and credit card information) spread across unsecured systems. Additionally, sensitive production data is transferred to third-party cloud services and disaster recovery servers, which most likely do not adhere to the same security standards as the production environment.

Major Parties Involved and Their Views

United States Of America

A private company's ability to gather personal information via the Internet is not currently covered by any extensive legislation protecting Internet privacy.

As per accusations, the US government purchased location information from a prayer app. Apps for treating opioid addiction have been identified by researchers to share sensitive information. Additionally, a recent data breach at T-Mobile affected at least 40 million customers, some of whom had no prior connection to the company.

At the moment, privacy laws are a confusing mess of many sectoral regulations. Historically, there have been several different federal laws in the US that control certain aspects of specific populations or specific sorts of data, such as credit or health

information. The privacy of all sorts of data is not covered by a single law in the United States. As an alternative, it consists of a variety of legislations, such as the Health Insurance Portability & Accountability Act (HIPAA), Childrens' Online Privacy Protection Act (COPPA) and Video Privacy Protection Act (VPPA).

Likewise, No national legislation also specifies when (or whether) a business must let you know if your data is compromised or disclosed to unauthorized parties.

Peoples Republic of China

Controversy surrounds China when it comes to online privacy. . According to data from the Internet Society of China, 54 percent of Chinese internet users believe that privacy violations are a serious issue in their nation.

For instance, Ant Financial, a unit of Alibaba that oversees payments, was forced to issue a public apology after enrolling consumers in a credit-scoring program without their permission. Researchers have noticed an increase in various types of personal records from China showing up on cybercriminal markets since the data of about 1 billion Chinese individuals became available for auction on a well-known dark website in June 2022. A spotlight has been focused on the enormous amount of information that government officials gather through Beijing's extensive surveillance network as a result of the interest in leaked Chinese data.

Some data protection laws are established under Chinese legislation, but when the interests of the Communist Party of China (CPC) are at stake, these rights will be eradicated. On November 1st, 2021, the Personal Information Protection Law (PIPL) of China took effect. The PIPL is the third of three Chinese laws—along with the Cybersecurity Law and the Data Security Law—that take a comprehensive approach to cybersecurity, data security, and data privacy. Therefore, China's regulations on data security and personal information have evolved to be more in agreement with other international standards after the implementation of the DSL and the PIPL in 2021.

European Union

The European Union passed its comprehensive Data Protection Directive ("Directive") in 1995, making it significantly more proactive than the United States in terms of safeguarding personal data online. The European Union's member countries are

subject to the Directive, which went into effect in October 1998 and does not distinguish

between online and offline settings.

The act achieves the following goals:
- the information collector must seek the user's permission before collecting and using personally identifiable information;
- the information collector must obtain the individual's permission before transferring the information to a third party.
-the information collector must give people full access to the information they have about themselves; and
-the information collector must declare the reason for collecting the data.

However, on May 25, 2018, the EU General Data Protection Regulation (GDPR), which controls how people's personal data may be handled and transmitted in the EU, was implemented. It replaces the provisions of Directive 1995/46 on Data Protection. Establishing guidelines for the protection of personal data and data migration is the overarching goal of all the initiatives.

Development of Issue/Timeline

Date	Event Outcome

1914	The Federal Trade Commission Act The FTC, which brings enforcement actions against businesses, is the main federal regulator in the field of privacy. This includes not adhering to privacy policies that have been posted and not effectively protecting personal data.
1986	The Computer Fraud & Abuse Act The United States passed the Computer Fraud and Abuse Act (CFAA) in 1986, making it illegal to access a protected computer without the required authorization.

2000	Children's Online Privacy Protection Rule Requires parental approval before gathering, using, or disclosing personal information from children under the age of 13 from specific websites and internet service providers.
2018	EU General Data Protection Regulation The Data Protection Law Enforcement Directive, the General Data Protection Regulation (GDPR), and other regulations pertaining to the protection of personal data. It was put into place to regulate how individuals' personal data may be handled and sent within the EU.

Previous Attempts to Solve the Issue

The Federal Trade Commission Act

The Federal Trade Commission Act is the primary regulation of the Commission. This law, as amended, gives the Commission powers, among other things, to - Seek financial and other legal remedies for acts harmful to consumers; - Prescribe rules specifically defining unfair or misleading conduct or practices and establish requirements designed

to prevent such conduct or practices; - Collect and compile information and conduct research on the organization, operations, practices, and controls of companies engaged in business;
- Present reports and legislative recommendations to Congress and the public.

To reiterate, The FTC, which brings enforcement actions against businesses, is the main federal regulator in the field of privacy. This includes not adhering to privacy policies that have been posted and not effectively protecting personal data.

Possible Solutions

Adoption of EU Directive on a global scale

Implementation of the EU Directive is one of the suggested resolutions to the Internet privacy concern. Although implementing the EU mandate remains a viable alternative for the cyberspace data collecting problem, Congress has been reluctant to pay the price.

The Directive, however, sets strict conditions that must be met by enterprises and that the government must enforce. As the environment shifts from inadequate to excessive protection of private rights, these standards may be overly demanding, leading to inefficiencies and burdening e-businesses.

Licensing

Some analysts advocate licensing of personal data. Individuals would be granted property rights in personal data under this suggested method. However, by discouraging transactions, encouraging fraud, and raising transaction costs, this method can have a negative effect on business. Additional challenges include figuring out what information belongs to a person and how to handle data that is already stored in databases.

Privacy Enhancing Technologies (PETs)

Yet another suggestion is based on technology itself. Technology-based safeguards are

used in privacy-enhancing methods (PETs), which are frequently based on pseudonyms or remailers to conceal the identities of Internet users, to prevent unauthorized data collection when browsing the Web.

However, relying on PETs and other comparable methods has drawbacks as well. Due to the rapid advancement of technology, the widespread usage of PETs could result in a cat-and-mouse game between businesses and individuals where each side is trying to outwit the other in order to gain the upper hand.

Bibliography

"Data Protection". European Commission - European Commission, 2022, https://ec.europa.eu/info/law/law-topic/data-protection_en.

Yong Xiong, Nectar Gan. "China Data Leak | CNN". Edition.Cnn.Com, 2022, https://edition.cnn.com/2022/07/05/china/china-billion-people-data-leak-intl-hnk/index.html.

"How To Protect Your Digital Privacy". Nytimes.Com, 2022, https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy.

Mckinneylaw.Iu.Edu, 2022, https://mckinneylaw.iu.edu/ilr/pdf/vol36p827.pdf.

YA