**Forum:** U.N. Commission on Science and Technology for Development

**Issue:** Developing measures to regulate the use of personal data by social media companies

**Student Officer:** Chirag Jadhav

**Position:** President

## Introduction

In today's digital age, social media companies have become ubiquitous, amassing a vast trove of personal data from their users. This data, encompassing everything from names and ages to health records and political opinions, is collected, analyzed, and shared by social media companies, often without the full knowledge or consent of the individuals to whom it pertains. Despite the benefits of personalized services, targeted advertising, and market research, this pervasive data collection raises significant concerns about privacy, security, and individual autonomy. The lack of transparency and accountability surrounding social media companies' data practices leaves users vulnerable to potential misuse, abuse, or unauthorized access. This data can be exploited for nefarious purposes such as identity theft, fraud, blackmail, or espionage.

Furthermore, the ethical and social implications of using personal data for purposes that may not align with the expectations or interests of users are profound. Manipulating emotions, behaviours, or decisions or discriminating against individuals based on personal characteristics or profiles are just a few examples of how personal data can be misused. Addressing these challenges requires a comprehensive and multifaceted approach involving governments, civil society, the private sector, and the scientific community. The U.N. Commission on Science and Technology for Development plays a crucial role in providing policy advice and recommendations, fostering dialogue and cooperation, and examining progress made in regulating the use of personal data by social media companies.

The issue of data privacy and regulation is not only relevant and necessary but also timely and urgent. The rapid advancement of technologies like artificial intelligence, big data, and cloud computing has facilitated the collection and dissemination of unprecedented amounts of personal data. Simultaneously, users and society demand more excellent protection, access, and control over their data, alongside upholding human rights and fundamental freedoms in the digital era. A global and multilateral approach is essential to address this issue's cross-border and cross-sectoral nature, ensuring the coherence, consistency, and effectiveness of measures to regulate the use of personal data by social media companies. Striking a balance between the benefits and risks associated with personal data is a complex and ongoing challenge that must be addressed to safeguard individual rights and foster a just and equitable digital society.

## Definition of Key Terms

**Privacy**

The ability to control what information about oneself or one's activities, preferences, or behaviours is collected, used, or disclosed by social media companies and to prevent any harm or loss that may result from such practices. This information can range from simple facts such as one's identity or location to more complex data such as health, financial status, views, or emotions.

**Transparency**

The quality of being straightforward, open, and honest about how social media companies collect, process, and share personal data and how they obtain consent from users. This personal data can include basic details such as name, age, and gender, as well as more sensitive information such as health records, financial transactions, and political opinions.

**Accountability**

Social media companies must justify and explain how they collect, use, or disclose information about users or their activities, preferences, or behaviours and respect and comply with users' rights and obligations. Accountability is necessary for the responsible and beneficial use of personal data, as it ensures fairness, security, and confidence for users and society1.

**Data Minimization**

A *data protection principle* aims to limit personal data collection, processing, and retention to what is necessary and relevant for a specific purpose. Companies should only collect and use the data essential for providing services and enhancing user experience. They should only collect or retain what they need and not use data for purposes not disclosed or consented to by the users.

**Purpose Limitation**

A data protection principle requires social media companies to only process personal data for the specific, explicit, and legitimate purposes for which they have informed and obtained user consent. It also means that social media companies cannot use or share personal data for any new or different purposes incompatible with the original unless they have a legal basis or a public interest justification.

**Data Accuracy**

A quality criterion evaluates how valid the data is concerning the reality it describes. Therefore, the data obtained and used by companies should be error-free, coherent, and current.

## Background

The collection and use of personal data by social media companies has raised considerable alarm among many people across the globe. Personal data encompasses information about or identifying an individual, such as biometric data, behaviour, interests, preferences, location, email, and name. Social media companies employ personal data for diverse purposes, such as delivering customized content and services, examining user trends and behaviour, marketing targeted ads, and disseminating data with third parties. However, these activities also entail grave perils to the rights, security, and privacy of individuals, as well as to the democratic values and public interest.

### How Social Media Companies Gather and Utilize Personal Data

Social media companies gather and utilize personal data to offer users personalized and captivating platform experiences. A study by the Pew Research Center reveals that 81% of Americans use social media at least once a day, and 28% say they use it almost constantly. Social media platforms provide users with various features and functions, such as producing and disseminating content, communicating and interacting with others, accessing information and news, and joining online communities and groups.

Social media companies gather and utilize a large amount of personal data from users to facilitate these features and functions. This encompasses profile information, such as data that users voluntarily provide when they create and update their accounts, such as name, age, gender, location, contact information, education, work, and interests. Some platforms also enable users to link their accounts with other services, such as email, phone, or other social media accounts, which can supply additional data to the platforms. Another type of data that social media companies gather and utilize is content and communication data, such as data that users produce and disseminate on the platforms, such as posts, photos, videos, comments, likes, reactions, messages, and stories. Some platforms also gather metadata from users' content and communication, such as tags, captions, timestamps, locations, and device information.

Moreover, social media companies gather and utilize browsing and behavioural data, such as data that platforms gather and infer from users' online activities and interactions, such as pages, groups, events, and profiles they visit, follow, or join, links they click, products they buy, ads they view or click, searches they make, and preferences they express. Some platforms also employ cookies, pixels, and other tracking technologies to gather data from users' browsers and devices, such as IP address, browser type, operating system, screen resolution, and device I.D. Lastly, social media companies gather and utilize biometric and sensory data, such as data that platforms gather and analyze from users' biometric and sensory features, such as face, voice, fingerprint, iris, and gait. Some platforms use facial recognition, voice recognition, and other artificial intelligence techniques to identify, verify, and categorize users and provide them with filters, effects, and other functionalities. Some platforms also gather data from users' cameras, microphones, and sensors, such as location, motion, and orientation.

Social media companies utilize personal data for various purposes. One of the primary purposes is to provide and improve services and content, such as personalizing users' feeds, recommendations, notifications, and ads, as well as developing new features, functions, and products. Another purpose is to analyze and understand users and markets, such as measuring and evaluating their performance, user behaviour, and market trends, as well as conducting research and innovation, such as testing new algorithms, models, and systems. A third purpose is to sell and monetize data and advertising, such as generating revenue and profit, mainly from marketing targeted ads to advertisers and marketers, as well as from selling or sharing data with third parties, such as data brokers, analytics firms, and research institutions. A fourth purpose is to comply with legal and regulatory obligations, such as responding to requests from law enforcement and government agencies and enforcing their terms of service, policies, and standards, such as removing illegal or harmful content and accounts.

## How Personal Data Can Be Compromised and Misused by Social Media Companies

The handling and utilization of personal data by social media companies also involve significant hazards and obstacles to the privacy, security, and rights of individuals, as well as to the public interest and democratic values. Some of these hazards and obstacles are as follows.

### *Data Breaches and Leaks*

Data breaches and leaks occur when personal data is accessed, disclosed, or stolen by unauthorized or malicious actors, such as hackers, cybercriminals, or rogue employees. They can expose sensitive and confidential information, such as identity, financial, health, and political data, resulting in identity theft, fraud, blackmail, harassment, and other harm. According to the Identity Theft Resource Center, 2022 had the second-highest number of data compromises in the U.S. in a year, affecting over 422 million individuals.

### *Data Misuse and Abuse*

Data misuse and abuse occur when personal data is used for purposes that are incompatible, inconsistent, or contrary to the individuals' expectations, interests, or consent, such as profiling, discrimination, manipulation, and surveillance. Data misuse and abuse can undermine the autonomy, dignity, and rights of individuals, such as privacy, freedom of expression, and non-discrimination, as well as the public interest and democratic values, such as transparency, accountability, and participation. According to the Pew Research Center, 79% of Americans are concerned about how social media companies use their data, and 64% think the government should do more to regulate them.

### *Data Inequality and Injustice*

Data inequality and injustice occur when personal data is collected, used, and distributed in ways that create or reinforce social and economic disparities, disadvantages, and discriminations, such as digital divide, exclusion, and exploitation. Data inequality and injustice can affect the access, opportunity, and empowerment of individuals and groups, especially those who are marginalized, vulnerable, or underrepresented, such as minorities, women, children, and low-income people. According to the World Economic Forum, data inequality and injustice are critical challenges for achieving a fair and inclusive digital economy and society.

## How to Safeguard and Regulate Personal Data in the Digital Age

Data protection and regulation encompass the legal and ethical frameworks and mechanisms that aim to safeguard and regulate the handling and utilization of personal data by social media companies and other actors, such as governments, businesses, and organizations. Data protection and regulation can consist of various elements.

First, data protection principles and rights are the fundamental norms and rules that govern the handling and utilization of personal data, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. Data protection rights are individuals' entitlements and remedies regarding their data, such as access, rectification, erasure, restriction, portability, objection, and consent.

Next, data protection authorities and agencies are the public institutions and bodies that oversee and enforce data protection laws and regulations and assist data controllers, processors, and subjects. Data protection authorities can have various powers and functions, such as issuing rules and standards, conducting audits and investigations, imposing sanctions and penalties, and resolving disputes and complaints.

Thirdly, data protection laws and regulations are the legal instruments and measures that establish and implement data protection principles and rights, as well as data protection authorities and agencies. Depending on the jurisdiction, sector, and context, these laws and regulations can vary in scope, level, and approach.

### *The General Data Protection Regulation (GDPR)*

The GDPR is the comprehensive and harmonized data protection law of the European Union, which governs the handling and utilization of personal data of individuals in the E.U. by any actor, irrespective of their location. The GDPR establishes high standards and requirements for data protection, such as data protection by design and by default, data protection impact assessment, data protection officer, data breach notification, and data transfer rules. The GDPR also confers substantial rights and remedies to individuals, such as the right to be forgotten, the right to data portability, the right to object to automated

decision-making, and the right to complain with a data protection authority. The GDPR also enforces severe sanctions and penalties for data protection violations, up to 4% of the global annual turnover or 20 million euros, whichever is higher.

### *The California Consumer Privacy Act (CCPA)*

The CCPA is the comprehensive and pioneering data protection law of the state of California, which regulates the handling and utilization of personal data of consumers in California by any business that meets specific criteria, such as having annual gross revenues of more than 25 million dollars or collecting or selling the personal data of more than 50,000 consumers, households, or devices. The CCPA confers broad rights and remedies to consumers, such as the right to know, the right to delete, the right to opt out, and the right to non-discrimination. The CCPA also enforces civil penalties and damages for data protection violations, up to 7,500 dollars per intentional violation or 750 dollars per consumer per incident.

### *The American Data and Privacy Protection Act (ADPPA)*

The ADPPA is the proposed and pending data protection law of the United States, which aims to provide federal protection of the personal data of individuals in the U.S. by any actor, irrespective of their location. The ADPPA would establish and implement data protection principles and rights, such as transparency, choice, access, correction, deletion, and security. The ADPPA would also create and empower data protection authorities and agencies, such as the Federal Trade Commission and state attorneys general, to oversee and enforce data protection laws and regulations and provide guidance and assistance to data controllers, processors, and subjects. The ADPPA would also impose civil penalties and damages for data protection violations, up to 5% of the annual revenue or 25 million dollars.

## Major Parties Involved

### The European Union (E.U.)

The EU spearheaded data privacy regulation by enacting the General Data Protection Regulation (GDPR) in 2018. The GDPR aims to empower EU citizens to regulate how and when their data is gathered and disseminated. It levies severe penalties on companies that fail to obtain users' consent or disclose how their data

will be utilized. The EU also has other legislation and initiatives to safeguard consumer privacy, such as the ePrivacy Directive and the Digital Services Act.

### China

China's data protection regime is rigorous and extensive, encompassing the Cybersecurity Law, the Personal Information Security Specification, and the Data Security Law. Social media companies must secure user consent, safeguard user data, and adhere to data localization and cross-border transfer regulations. The Cyberspace Administration of China, a formidable internet regulator, can levy fines, revoke licenses, and close websites for breaching data privacy rules.

### India

India's first data protection law, the Personal Data Protection Bill, is expected to be enacted in 2023. The bill draws inspiration from the E.U.'s GDPR, but also has some distinctive features, such as requiring data localization for certain types of data, establishing a Data Protection Authority, and granting the government the power to exempt itself from some data privacy obligations for national security and public interest purposes. The bill would cover social media companies that process the personal data of Indian users, irrespective of their location.

### United States of America (USA)

The USA needs a comprehensive federal data privacy law and instead has a mosaic of state and sector-specific laws. Some of the most prominent ones are the California Consumer Privacy Act (CCPA), which grants Californians the right to access, delete, and opt out of the sale of their data, and the Children's Online Privacy Protection Act (COPPA), which mandates parental consent for collecting data from children under 13. The U.S. government has also taken some measures against social media companies for infringing user privacy, such as the Federal Trade Commission (FTC) imposing a $5 billion fine on Facebook in 2019 for the Cambridge Analytica scandal. However, the U.S. public is split on whether the government should or should not regulate how social media companies protect the personal data of their users, with 49% saying it should and 47% saying it should not, according to a 2023 survey.

## Previous Attempts to Resolve the Issue

In 2013, the U.N. General Assembly adopted resolution 68/167, which reaffirmed the online and offline applicability of the right to privacy and expressed grave concern over the human rights implications of electronic surveillance and data collection. The resolution urged all states to respect and safeguard the right to privacy and to revise their policies, practices, and laws on monitoring communications, their interception and the gathering of personal data. It also mandated the U.N. High Commissioner for Human Rights to produce a report on protecting and advancing the right to privacy regarding domestic and extraterritorial surveillance and interception of digital communications and collection of personal data, including on a large scale.

In 2015, the U.N. Human Rights Council adopted resolution 28/16, which acknowledged the High Commissioner's report and supported its suggestions, such as ensuring that any intrusion on the right to privacy adheres to the principles of legality, necessity, and proportionality and that any gathering of personal data is in line with international human rights standards. It also resolved to appoint a Special Rapporteur on the right to privacy, with a mandate to oversee and report on issues pertaining to the right to privacy in the digital age.

In 2017, the U.N. Human Rights Council adopted resolution 34/7, which reiterated the previous resolutions and acknowledged the need for more efforts to tackle the challenges posed by the digital age for the right to privacy. It also asked the Special Rapporteur to produce a report on the role of the private sector in the digital age and its effect on exercising the right to privacy.

## Possible Solutions

Strengthen User Control and Transparency:

Give Users Fine-Grained Data Access and Control: Provide user-friendly dashboards and settings to give users fine-grained control over their data, enabling them to easily access, review, modify, and delete it.

Enforce Clear and Transparent Data Practices: Obligate social media companies to provide clear and accessible privacy policies that explain how they collect, use, and share user data. Acquire explicit consent from users before collecting or using sensitive data.

Ensure Data Portability: Enable users to quickly transfer their data between social media platforms, stimulating competition and promoting data ownership.

Set Up Robust Data Protection Standards:

Apply data minimization principles: Require social media companies to limit data collection to what is necessary for specific purposes and delete data promptly when no longer needed.

Enforce Data Security Measures: Implement encryption, access controls, and regular security audits to protect user data from unauthorized access, breaches, and misuse.

Regulate Data Sharing and Third-Party Access: Establish strict guidelines for sharing user data with third parties, require explicit consent before sharing sensitive data, and ensure transparent data-sharing agreements.

Foster Responsible Data Use and Algorithmic Accountability:

Prohibit Misleading or Deceptive Data Practices: Prohibit social media companies from employing deceptive or manipulative data practices to influence users' behaviour or preferences.

Promote Algorithmic Transparency and Fairness: Obligate social media companies to disclose the underlying algorithms that govern content moderation, targeted advertising, and other user experiences. Ensure algorithms are fair, non-discriminatory, and free from biases.

Establish Independent Oversight Mechanisms: Create independent oversight bodies to monitor and enforce data privacy regulations, conduct regular audits of social media companies' data practices, and address user complaints.

Empower Users with Privacy-Enhancing Tools:

Develop Privacy-Preserving Technologies: To enable personalized experiences while minimizing data exposure, encourage the development and adoption of privacy-preserving technologies, such as differential privacy and federated learning.

Promote Privacy-Enhancing Browser Extensions: Support developing and deploying privacy-enhancing browser extensions that empower users to control their data, block tracking, and enhance their online privacy.

Raise Public Awareness and Digital Literacy: Implement public awareness campaigns and educational programs to promote digital literacy, teach users about data privacy risks, and empower them to make informed choices about their online data.

Encourage International Cooperation and Harmonization:

Promote Cross-Border Data Flow Agreements: Encourage international cooperation to establish harmonized data privacy standards and facilitate the secure flow of data across borders while protecting user privacy.

Engage with International Organizations: Collaborate with international organizations, such as the OECD and the Council of Europe, to develop global guidelines and best practices for regulating social media companies' use of personal data.

Foster Cross-Border Enforcement Mechanisms: Establish mechanisms for cross-border enforcement of data privacy regulations to ensure consistent application and protection of user rights across jurisdictions.

## Bibliography

Avvo. "Consumer Privacy: How Your Personal Social Media Data Is Used." Avvostories, 1 Dec. 2020, stories.avvo.com/consumer-protection/2020-12-1-consumer-privacy-how-your-personal-social-media-data-is-used.html. Accessed 28 Nov. 2023.

Electronic Privacy Information Center. "Social Media Privacy." Electronic Privacy Information Center, 2020, epic.org/issues/consumer-privacy/social-media-privacy/. Accessed 28 Nov. 2023.

General Assembly. "Privacy and Data Protection: Increasingly Precious Asset in Digital Era Says U.N. Expert." United Nations Human Rights Office of the High Commissioner, United Nations, 19 Oct. 2022, www.ohchr.org/en/press-releases/2022/10/privacy-and-data-protection-increasingly-precious-asset-digital-era-says-un. Accessed 28 Nov. 2023.

Human Rights Council. "OHCHR and Privacy in the Digital Age." United Nations Human Rights Office of the High Commissioner, 4 Aug. 2021, www.ohchr.org/en/privacy-in-the-digital-age. Accessed 28 Nov. 2023.

Kaoudahhan, Ahmed Fadel. "How Social Media Companies Collect and Use Your Data." Medium, 29 Jan. 2023, medium.com/digital-reflections/how-social-media-companies-collect-and-use-your-personal-data-d677ce4ae469. Accessed 28 Nov. 2023.

MacCarthy, Mark. "Transparency Is Essential for Effective Social Media Regulation." Brookings, Brookings Institution, 1 Nov. 2022, www.brookings.edu/articles/transparency-is-essential-for-effective-social-media-regulation/. Accessed 28 Nov. 2023.

Petrosyan, Ani. "Annual number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022." Statista, 29 Aug. 2023, www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. Accessed 28 Nov. 2023.

Rahnama, Hossein, and Alex Pentland. "The New Rules of Data Privacy." Harvard Business Review, Harvard Business Publishing, 25 Feb. 2022, hbr.org/2022/02/the-new-rules-of-data-privacy. Accessed 28 Nov. 2023.

Reality Check team. "Social Media: How Do Other Governments Regulate It?" BBC, 12 Feb. 2022, www.bbc.com/news/technology-47135058. Accessed 28 Nov. 2023.

U.N. News. "U.N. Chief Calls for New Era of Social Media Integrity in Bid to Stem Misinformation." U.N. News Global Perspective Human Stories, United Nations, 13 June 2023, news.un.org/en/story/2023/06/1137562. Accessed 28 Nov. 2023.