**Data Privacy**

The Internet has progressed from a decentralized and anonymous architecture to one in which data recording a variety of behaviors is uniquely and personally recognizable. New services, companies, and industries have evolved as a result of the value of such a large amount of personal data. Despite the advantages of data, internet users worries about personal privacy intrusions have grown as shared personal information becomes a non-rivalry, non-excludability public good. The value of protecting and sharing personal information is context-dependent and based on essentially unpredictable world conditions.[29]

**What Is Data Privacy, and Why Does It Matter?**

Data privacy is a set of guidelines for how sensitive and important data should be acquired and handled. Personal health information (PHI) and personally identifiable information (PII) are two examples of data privacy (PII). Financial data, medical records, social security or ID numbers, names, birthdates, and contact information are all examples. All sensitive information that firms handle, including that of customers, shareholders, and workers, is subject to data privacy concerns. This data is frequently crucial to corporate operations, development, and finances. Data privacy ensures that sensitive information is only available to those who have been given permission to see it. It helps guarantee that firms follow regulatory obligations and prevents criminals from using data for nefarious purposes.[30]

**Critical Best Practices for Ensuring Data Privacy**

The following best practices can help you ensure that the policies you create are as effective as possible.

* Inventory Your Data

Understanding what data you have, how it is managed, and where it is stored is an important part of protecting data privacy. Your policies should define how this data is gathered and used. For instance, you'll need to define how often data is scanned for and how it's classified once located. Your privacy policies should clearly outline what protections are needed for your various data privacy levels.   Processes for auditing protections should also be included in policies to guarantee that solutions are implemented correctly.[30]

* Minimize Data Collection

Ensure that your policies dictate that only necessary data is collected. If you gather more than you require, you increase your liability and can create an undue burden on your security teams. Minimizing your data collection can also help you save on bandwidth and storage. One method to accomplish this is using “verify not store” frameworks. These systems using third-party data to verify users and eliminating the need to store or transfer user data to your systems.[30]

* Be Open with Your Users

Many users are aware of privacy concerns and are likely to appreciate transparency when it comes to how you’re using and storing data. Reflecting this, GDPR has made user consent a key aspect of data use and collection. By incorporating privacy concerns into your interfaces, you can ensure that users and their consent are included in your processes. Having explicit user notifications describing when and why data is gathered.  You should also give consumers the ability to change or opt out of data collecting.[30]

**Data Localization**

Despite the significant benefits to businesses, consumers, and national economies that come from organizations' ability to easily share data across borders, dozens of countries at various stages of development have erected barriers to cross-border data flows, such as data-residency requirements that confine data within a country's borders, a concept known as "data localization." Data localization can be mandated by legislation or is the de facto result of a slew of other restrictive rules that make data transfer impossible, such as requiring enterprises to retain a copy of their data locally, process data locally, and demand person or government approval for data transfers.[26]

Legitimate global anxieties over surveillance and security are justifying governmental measures that break apart the World Wide Web, without enhancing either privacy or security. However, we contend that data localization will backfire, compromising privacy and security while still exposing data to foreign surveillance. Such a change poses a threat to the new type of international trade made possible by the Internet [27].

**Cross-border Data Flows**

Data is the current global economy's lifeblood. Digital trade and cross-border data flows are predicted to rise at a higher rate than global trade overall. Businesses utilize data to create value, and many of them can only maximize that value if data can move freely across borders. However, an increasing number of governments are imposing restrictions that make data transfer more expensive and time consuming, if not illegal.[26]

**Cross-border data flow regulation**

Although data protection regulations in different countries take different approaches to cross-border data transfers, they can be put together in a general taxonomy. A country may apply several different approaches to cross-border data flows depending on the nature of the data involved. For instance, there can be differences across sectors: while a country might apply a free-flow approach to movement of personal data across borders, it might condition the transfer of personal data that is health-related. Equally, a country might condition the transfer of personal data but apply a free-flow approach to all other types of data.[28]

**[Data-divide]**

In 1970, American researchers used the term "knowledge gap" to describe the unbalanced flow of information and the public's equal access to knowledge during the popularization of mass media. The National Telecommunications and Information Administration (NTIA) proposed the information divide in the report of “Falling through the Net: Defining the Digital Divide”. The information divide refers to the disparity between those who have access to information and those who do not. Those who lack the opportunity or ability to receive information are unable to participate in the creation and dissemination of social civilization achievements based on information and knowledge**.[31]**

**[Data-divide Challenges]**

**The Digital Infrastructure Divide among Cities and Rural Areas:** One of the key causes of the growing digital gap is a lack of infrastructure. Most rural and isolated villages lack the necessary telecommunication infrastructure to enable any significant ICT project aimed at the public.[24]

**Language Barrier and Digital Divide:**

Language is another hurdle that contributes to the Digital Divide. This barrier has hampered information in countries where English is not used as a medium of instruction. huge information resources are not fully accessible, due to the absence of motivation to learn a new language. One other factor for insufficient access is a lack of good translational software. [23]

**disability digital divide in developed contrary:**

according to the World Health Organization 80% of people living with a disability lives in developing countries, according to the different definitions it is indicated that this community is a disadvantaged group in the society ICT access by this community also considered as a common problem in the world. [23]

**The differences in usage of data resources (Digital skills**)**:** the use that people make of digital technologies is not the same. Individuals from various classes and groups may have equal access to the internet, but not everyone has the same skills and knowledge to use and apply them in the same way, and empirical studies have been showing the relevance of these differences (Van Dijk, 2006; Scheerder et al., 2017). More precisely, it has been noted that, due to differences in skills and knowledge, some individuals benefit from technology significantly more than others.[32]

**issue of access to the internet**: The digital divide was firstly associated with a socio-economic gap between those who have access to the computer and the internet, and those who do not.[32]

**Data-divide Solutions:**

Here some possible solutions to bridging the gap of digital divide

**Launch different internet connectivity projects**: Different projects, both in rural and urban regions, should be launched soon to provide access to all sectors of the population. such projects should include as Fiber optical link, for far and unreachable area wireless local loop could be an option. As a component of these projects, high Speed Internet connectivity should be subsidized to the less privilege individuals and offer them low-cost technologies so that they would be able to connect with global community, access open data, take benefits from the technologies, including emerging technologies, and raise their voices, and find the solutions to their problems.[25]

**Provide low-cost of Computer and Internet connectivity**

ICT has provided many technologies for disabled people globally including web services, mobile services, and computer devises but differently abled community has not used these tools and techniques due to the cost of computer and Internet connectivity Therefore, the solutions (e.g. Providing low-cost technologies, reuse recycled computers) need to implement at Government level, University level and other public and private sector authorities. [23]

**Providing Digital Training**: providing some assistive tools, ICT training, competence related elements (such as technological knowledge and internet abilities), and involvement in online learning communities.[33]

# **Sources**

[23] R. N. Wedasinghe, "Web, Mobile and Computer Related Model to Bridge," 2014. [Online].

[24] Narrowing the Digital Infrastructure Divide among Cities and Rural Areas, Hyong-Soon Kim, Eun-Young Lee, Seoul, Korea 2010.

[25] eGovernment and the digital divide, PhD Vujica Lazović MSc Tamara Đuričković,2012

[26] N. Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," ITIF, 2017

[27] Anupam Chander," Breaking the Web: Data Localization vs. the Global Interne",2014

[28] Francesca Casalini, Javier López González," Trade and Cross-Border Data Flows",2019

[29] "Managing privacy in the digital economy",2021

[30]"Data Protection and Privacy: 12 Ways to Protect User Data", https://cloudian.com/guides/data-protection/data-protection-and-privacy-12-ways-to-protect-user-data/#data-protection-privacy

[31] LI Jian, WANG Zhijin, "The Urban-rural Information Divide in China",2011

[32] " The three levels of the urban digital divide: Bridging issues of coverage, usage and its outcomes in VGI platforms" Daniela Ferreira a,\* , M´ ario Vale b , Renato Miguel Carmo c , Luis Encalada-Abarca b,d , Carla Marcolin e,,2021

[33] The digital divide: A review and future research agenda,2022