Talking Data to the Fourth Pillar

DIGITAL EMPOWERMENT foundation

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Talking Data to the Fourth Pillar

Module 1

Talking Data to the Fourth Pillar

April 2023

Author: Dushyant Arora

Concept: Vineetha Venugopal

Review: Vineetha Venugopal, Jenny Sulfath, and Arpita Kanjilal

Advisor: Osama Manzar

Design and Illustration: Yuvasree Mohan

Published and distributed by:

Digital Empowerment Foundation
House No. 44, 2nd and 3rd Floor (next to Narayana IIT Academy)
Kalu Sarai (near IIT Flyover)
New Delhi – 110016 Tel: 91-11-42233100 / Fax: 91-11-26532787
Email: def@defindia.net | URL: www.defindia.org

INTRODUCTION

The last few years have seen increasing digital surveillance on citizens by various national governments and corporates as evidenced by Cambridge Analytica and the Pegasus project. With existing legal provisions inadequate to ensure the privacy and autonomy of the citizenry in a digitalized world, many countries are legislating on digital data protection. However, with the rise of authoritarian politics and the digital economy, there is also the danger of these legislations prioritizing state surveillance and commodification of data over the rights of the people.

Particularly vulnerable are the journalists. Termed the fourth estate by the British parliamentarian Edmund Burke, the media would later be termed the fourth pillar of democracy meant to scrutinize the executive, judiciary, and legislature on behalf of the people. Due to the particularity of their profession, journalists need to protect not only their privacy, but also that of their sources, making them even more vulnerable. As such, it is important that journalists are equipped with the knowledge to safeguard themselves using digital and legal means.

India is currently on the 4th iteration of its data protection legislation having closed the public consultation for the draft Digital Data Protection Bill, 2022 as of January 2023. However, the draft bill has been critiqued for facilitating state surveillance without adequate safeguards. There are also fears that vague terms in the bill can be interpreted in a manner that would be detrimental to the freedom of expression, freedom of the press and privacy.

It was in this context that Digital Empowerment Foundation initiated the program 'Talking Data to the Fourth Pillar'. This cohort-based learning program was designed with the aim of discussing core concepts on privacy, data protection and online safety so that the trained participants can

- Educate and inform the citizenry through content/art pieces
- Use the legal knowledge acquired from training to safeguard journalistic freedoms
- Practice responsible reporting that is respectful of citizen's privacy and data
- Exchange best journalistic practices and collectively work towards securing online Privacy and safety

Additionally, women, queer individuals and other marginalized communities have been historically oppressed by surveillance and data processing. All these calls for nuanced understandings of privacy and data protection from an intersectional feminist perspective. It is our hope that the sessions and discussions will contribute to fostering such an understanding. We look forward to learning with you and learning from you.

- Vineetha Venugopal

Why is privacy a fundamental human right?

Privacy International describes privacy as a "fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built." It has also been defined as a "a state of affairs where information regarding an individual's life and conditions that are private in nature is beyond the reach and knowledge of others."

The Right to Privacy is mentioned in Article 12 of the Universal Declaration of Human Rights and Article 16 of the Convention of the Rights of the Child (CRC). It is mentioned in Article 8 of the European Convention on Human Rights and Article 17 of the legally-binding International Covenant on Civil and Political Rights (ICCPR), to which India is a signatory.

On August 24th, 2017, the Indian Supreme Court recognised that citizens have a right to privacy in a landmark judgement, Justice K. S. Puttaswamy (Retd.) & Anr. Vs Union Of India & Ors (Puttaswamy or the Right to Privacy case). In this case, the Supreme Court ruled that the right to privacy was a fundamental right under Article 14 (which deals with equality before the law), Article 19 (which deals with various Constitutionally protected freedoms) and most importantly and directly, Article 21 (the right to life) of the Indian Constitution. It also ruled that this fundamental right to privacy granted to individuals extends to digital spaces.

The 2017 Right to Privacy verdict stated that "privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level, privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty."

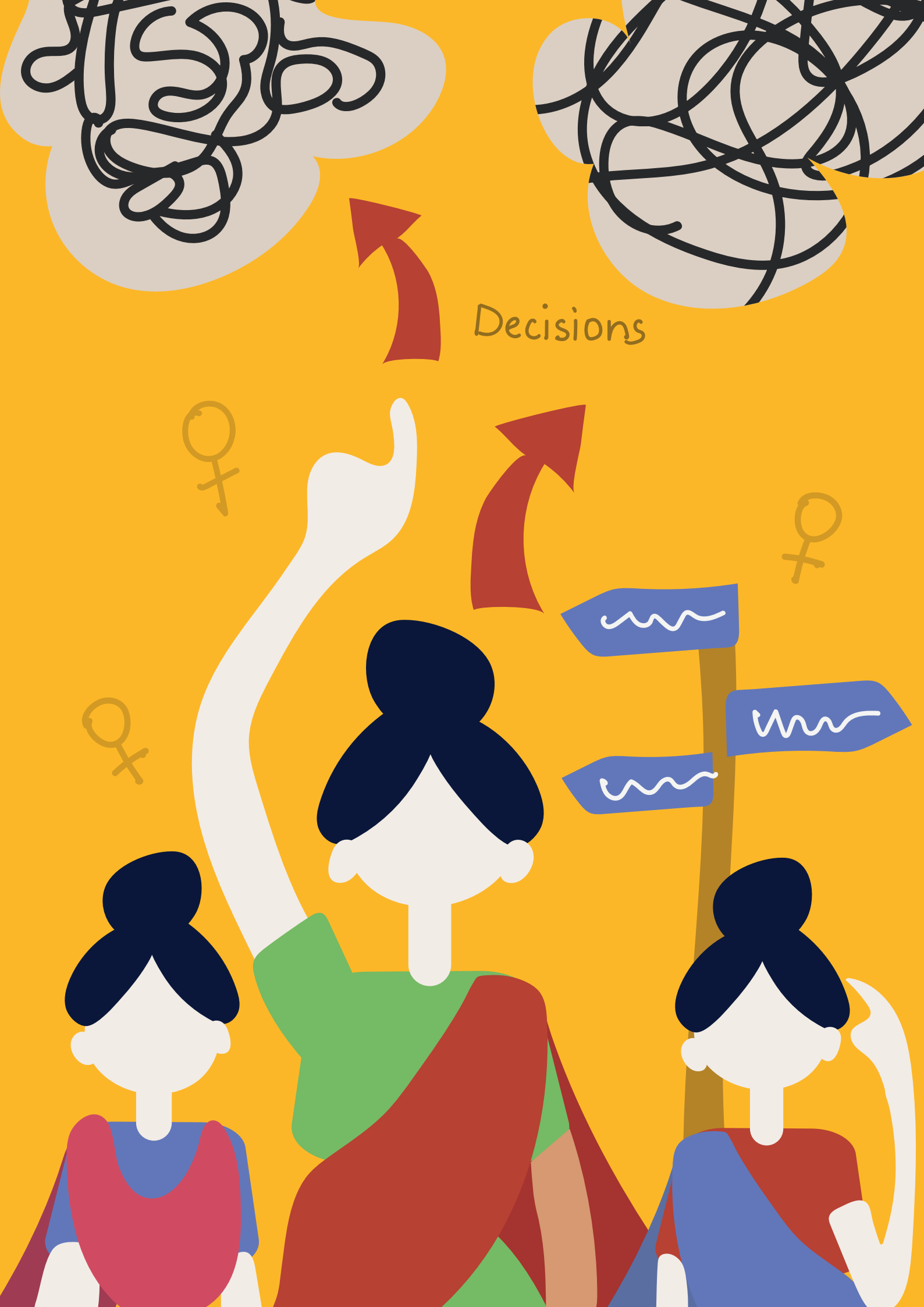
It also stated that "Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurali-

ty and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being."

The Right to Privacy being recognised as a fundamental right was a direct result of data privacy concerns raised around the country's Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The Unique Identification Authority of India (UIDAI) is entrusted with issuing AADHAAR cards and storing the data collected from citizens. These cards can be linked to citizens' bank accounts, Unified Payment Interface IDs, and various government portals. Given the wealth of crucial information that the UIDAI is entrusted with storing and protecting, many concerns were raised about protecting this massive online information database from invasions of data privacy and allowing for the creation of mass surveillance systems. In this case, the Court recognised the need to protect citizens' data from being intercepted, used for mass surveillance or otherwise misused by ruling that citizens had a right to privacy which the State was bound to protect.

Having a right to privacy is essential for several reasons. It prevents other people, entities or even the government from spying on citizens or monitoring them without due cause. Knowing citizens have the right to privacy is one of the critical foundations of several essential services and industries, including banking, financial services and healthcare. Having a robust, well-protected and meaningful right to privacy should ensure that your data isn't used for ends that you aren't aware of or do not consent to and that those who do the same are held accountable.

As Privacy International states, establishing and protecting the boundaries around an individual and deciding the limits of their autonomy is simultaneously an exercise in discussing "the ethics of modern life, the rules governing the conduct of commerce, and the restraints we place upon the power of the state."


Decisions

What is autonomy and why is it important to women and queer individuals?

Autonomy of individuals in a society refers to the freedom and ability of individuals to make their own choices and decisions, without interference from others. This can include personal autonomy, which relates to an individual's personal choices and decisions, as well as political autonomy, which refers to the ability of individuals to participate in the political process and make decisions about their government. Autonomy is considered an important aspect of a free and democratic society, as it allows individuals to have a say in the direction of their own lives, and the life of their community.

Historically, women and queer individuals have often been denied the ability to make their own choices and decisions, and have had their autonomy restricted by societal norms, cultural expectations, and laws that discriminate against them. Personal autonomy allows individuals to reclaim control over their own lives and bodies and make decisions that align with their own values and beliefs without facing negative repercussions.

Personal autonomy allows women and queer individuals to have agency in making social, aesthetic, sexual and reproductive choices, and to be free from discrimination and oppression. It allows them to pursue their own goals, aspirations and live their lives as they see fit, without interference from others. Having personal autonomy promotes self-esteem, self-respect and self-worth.

Personal autonomy must be protected as a human right, and also a socially upheld moral value. Personal autonomy being protected by law has no meaning to individuals if their autonomy is curtailed in spaces that are traditionally left unregulated by law, such as the domestic space.

Privacy in the South Asian context

Can you think of the word for privacy in your native language? Does such a word exist? How long did it take you to recall it?

Many believe that the notion of privacy appeals more intrinsically to individualist societies, such as in Europe or the United States of America, rather than to collectivist cultures, such as India, South Korea, Bangladesh or Pakistan. Studies have shown that internet users in individualist countries and societies are more concerned with data privacy issues than users from collectivist countries or cultures. It has been observed that users from individualist versus collectivist societies have different kinds of data privacy concerns. While users from individualist countries are more concerned with their data privacy as individuals, users from collectivist countries were found to be more concerned with how their usage of the internet or certain apps could affect the privacy and exposure of their peers or group members and in discussing ways in which they could restrict their own usage to protect the privacy of their peers.

Given that much of our lives involve using the internet, which consequently involves putting personal information onto the internet, digital privacy is an aspect of privacy that allows individuals to have control over the information about themselves that exists in the digital domain.

What is digital privacy?

Digital privacy is defined as the "protection of the information of private citizens who use digital mediums". Using the internet leaves a digital footprint in the form of geolocation tracking, IP address, search history, social media posts and activity, likes and dislikes, in addition to a variety of personal information such as a user's name, gender and country of origin. A user typically

expects this information to be kept private and used only in contexts to which the user has understood and consented. Using social media and communications applications also creates a vast digital trail of various communications between groups and individuals.

There are two significant facets to digital privacy. These are information privacy and communication privacy. Information privacy is the freedom to decide how your personal information will be used. Communication privacy is the freedom to use digital platforms with the assurance that digital communications will be kept private.

Why is the protection of digital privacy important?

Much as you would not like to be surveilled when alone in your home or see billboards displaying photographs from your personal family photo albums, digital privacy ensures that your activities online, where you would like them to remain private, remain so. Digital privacy ensures that your digital identity is protected from bad actors, the State, or companies seeking to profit from behaviour you could reasonably expect to be kept private.

Protecting digital privacy is important because it allows individuals to maintain control over their personal information and how it is used. Without protection, this information can be accessed, shared, and used without an individual's knowledge or consent, potentially leading to negative consequences such as identity theft, discrimination, or manipulation. It is also vital for protecting freedom of expression and freedom of association.

Keeping your digital information private protects you from your personal information being exposed. It allows details you share on online platforms and services, such as your banking information, debit or credit card details, and location, to be kept private. Digital privacy protects your information from being accessed and sold to bad actors who could use it to perpetrate various cyber crimes, including financial crimes or crimes with real-world physical consequences. It protects your private communications from being made public. It protects you from being profiled or persecuted for your sexual orientation, gender identity or socio-political views.

What are the challenges to digital privacy?

One of the most intriguing challenges when addressing privacy rights is that most privacy violations occur without the individual's knowledge. When dealing with other rights, an individual is usually aware of who is violating their right and of the fact that that right is being infringed or compromised. Breaches of privacy occur in a manner that the user is usually completely unaware that they are being surveilled, or that their data is being viewed, or has been compromised. This unique aspect of data privacy breaches makes it still more important to ensure that robust data privacy frameworks are in place.

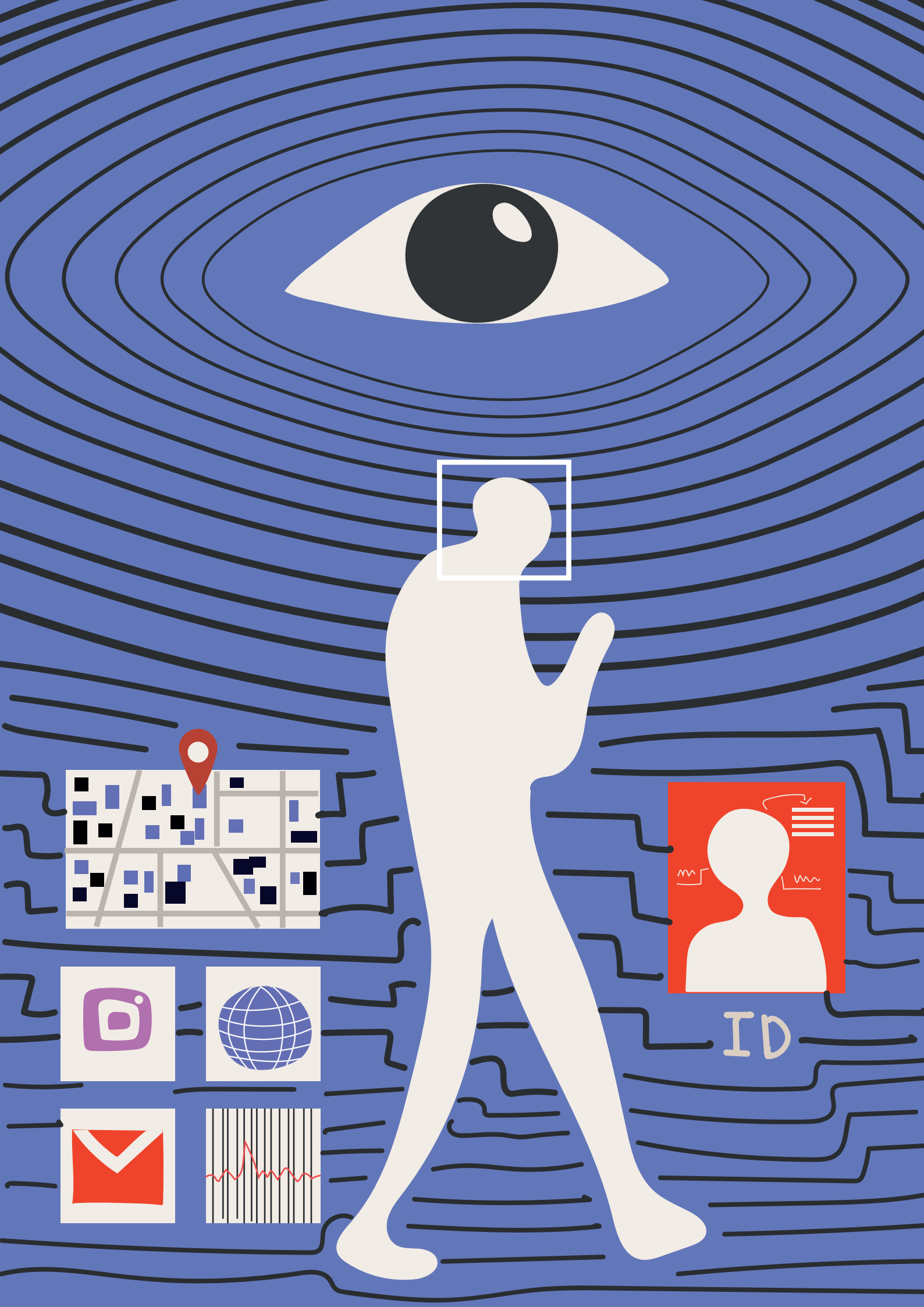
Some of the keenest threats to digital privacy include:

1. State-based surveillance techniques

Mass surveillance:

Mass surveillance can be defined as the "broad, arbitrary monitoring of an entire or substantial fraction of a population (EFF 2015)". States and governmental organisations can easily undertake mass surveillance of vast swathes of the population by placing taps on fibre optic cables. They can monitor and surveil the internet activity of any number of internet users by gaining access to their email IDs and telephone numbers and thereby have an overview of internet activity associated with certain websites. Governments can install surveillance equipment, such as internet monitoring systems, in critical locations (e.g. internet exchange points, cable landing stations) to indiscriminately collect data on a large number of internet users or conduct targeted surveillance of specific groups. Governments may use sophisticated data analysis techniques such as artificial intelligence and machine learning to sift through and make sense of the vast amounts of data collected.

Back in 2013, Edward Snowden, a former American National Security Agency (NSA) contractor, revealed a vast amount of classified information that exposed the extent of mass surveillance being conducted by the United States government.
:


ID

Some of the key revelations made by Snowden included

PRISM: a top-secret program run by the NSA that collects data on individuals from major internet companies, including Google, Facebook, and Apple. This data includes emails, chats, images, and other forms of communication.

Tempora: a program run by the British intelligence agency GCHQ, which collects vast amounts of internet data from undersea fibre-optic cables.

XKeyscore: a program that allows the NSA to search through vast amounts of internet data, including emails, chats, and browsing history, without a warrant.

BULLRUN: a program that attempts to weaken encryption and security protocols used on the internet to allow the government to access data it would otherwise be unable to.

Boundless Informant: a tool used by the NSA to track and map data collection worldwide, including by country.

Collection of metadata on US citizens: Snowden revealed that the NSA was collecting metadata on millions of American citizens' phone calls and emails.

There have been reports that the Indian government has used mass digital surveillance to monitor ethnic minorities, particularly in regions with separatist movements or tensions between ethnic groups. For example, in the state of Jammu and Kashmir, the site of a long-running conflict between the Indian government and separatist groups, the government has been accused of using digital surveillance to monitor and control the online activities of the Muslim-majority population. This includes internet shutdowns, tracking cookies, and surveillance software to limit the population's freedom of movement and communication.

Targeted surveillance

Targeted surveillance can be used to silence, intimidate or collect information on political opponents, human rights activists, and others that are critical of the government. Additionally, targeted surveillance can also be used to discriminate against certain groups, for example, ethnic or religious minorities, or to monitor and control the activities of particular citizens. Governments can use GPS tracking to track the movement of individuals using their cell phones or other GPS-enabled devices.

Governments have been known to install software on people's computers, smartphones, and other devices that allow them to monitor and collect information on the user's online activities, searches, and communications.

In 2018, it was reported that the Indian government had used the spyware Pegasus, developed by the Israeli cyber intelligence company NSO Group, to target individuals involved in the Bhima Koregaon case. The case relates to an incident in which Dalit (formerly known as "untouchable") rights activists were arrested for alleged involvement in inciting violence at a public event in the Bhima Koregaon village in Maharashtra state.

The use of Pegasus was reported to have been used to target human rights activists and lawyers, to spy on their phone calls, text messages, and other forms of communication. It was also alleged that the Indian government had used the spyware to hack into the activists' phones and gain access to their personal information, including contacts, messages and location data.

These kinds of privacy breaches are often undetectable, given that governmental and intelligence agencies enforce them.

2. Third-party intermediaries (ISPs, social media companies, search engines, telecom companies)

Third-party intermediaries, such as internet service providers (ISPs), search engines, and social media companies, collect user data through various means. Some of the ways they collect data include:

Logging user activity: ISPs, search engines, and social media companies may log user activity, such as websites visited, search queries, and clicks.

Cookies and tracking: These intermediaries may use cookies and tracking technologies to collect data on users' browsing habits and preferences.

Location data: Many social media and mobile apps collect location data from users' devices, which can be used to track their movements and infer their interests and habits.

Personal information: Many social media and other online services require users to provide personal information, such as their name, age, and contact information.

Metadata: Intermediaries may also collect metadata, which is data about the data, such as the time and location of a message or call, but not the content of the message or call itself. Once collected, this data can be used for various purposes, including targeted advertising, personalisation of services, and analytics. However, this data can also be exposed through data breaches, hacking, or due to the intermediaries being compelled to share it with government agencies for surveillance or other purposes. The data can also be sold to third parties, such as data brokers, which can be used for various purposes, including targeted marketing.

3. Backdoor access requirements by law enforcement:

The existing laws that govern the use of the internet have sweeping exceptions that allow government entities and officials to legally obtain personal information if required in the interest of national security or investigation of crimes. Social media platforms in India, such as Whatsapp and Facebook, are governed by the IT Act. This Act states that authorised government bodies and officers have the right to intercept data from these platforms "if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence relating to above or for investigation of any offence." This sweeping exception leaves individuals and groups keenly exposed to a breach of their privacy that could be used maliciously or unintentionally. Most countries have laws that sacrifice digital privacy at the altar of national security, but these exceptions create enormous opportunities for the State to gain unnecessary access to private data.

Such legal provisions demand that journalists take particular care to protect the PII and communications of their sources, especially when reporting on politically or socially sensitive issues. This requires journalists to adopt conscious, informed and responsible choices when deciding what platforms to contact and collecting information from sources, and how they store the confidential information obtained from their research.

What does digital Privacy mean to Women in South Asia

What does digital privacy mean to women in South Asia?

In 2017-2018, an NGO called Nitya, in partnership with Google and several universities, surveyed 103 women participants from India, 52 from Pakistan, and 44 from Bangladesh, on various issues related to women and data privacy. The survey spoke to a total of 199 participants who identified as women, including 11 participants who identified as queer, lesbian or transgender. This survey threw up some interesting results.

Their survey revealed that participants had widely differing views on what privacy was and who it was for; many low-to-middle-income participants expressed the belief that privacy was a concept that did not seem natural to them or living situations and that it was a dubious Western import meant for upper-class women.

Many participants also shared that they were expected to share their mobile devices. This could be through sharing their devices with other family members, having other family members help them use their devices due to their inability to navigate their devices or monitoring or checking their devices and usage by other family members.

While the women surveyed had differing opinions on the meaning of privacy and the importance it held for them, all of the participants practiced some measures to safeguard their privacy on their devices. These measures included using screen locks, PIN locks for specific apps, deleting their data or pictures, or, for more tech-savvy participants, using a private mode or profile while using their devices.

It becomes clear from this study that South Asian women face not only threats to privacy from outside actors such as the State, hackers or third-party attackers but also family members or actors within their own homes.

Given the crucial and sensitive nature of the kinds of stories that journalists report on, the fact that journalists are increasingly turning to digital tools to carry out their work, and the fact that sources speak to journalists often on the assumptive condition that their identity and data will be kept private, data privacy is of particular importance to journalists.

What are the different types of information that require privacy protection as a journalist?

Personal data refers to any information related to a person. This can include information such as a person's name, address, phone number, email address, and other details that can be used to identify them.

Personally identifiable data (PII) is a subcategory of personal data that specifically refers to information that can be used to directly or indirectly identify a specific individual. Examples of PII include a person's social security number, driver's licence number, passport number, and biometric data such as fingerprints and facial recognition data.

In summary, all PII is personal data, but not all personal data is PII.

single piece of personal data, such as a person's name, say Ankita Lalwani, may not be PII, as there may be multiple people with the same name. But various pieces of personal data, such as their full name and the address of the specific branch of the multinational company they work at, can constitute PII, as the two pieces of personal data accessed in conjunction can identify the particular individual.

Journalists are tasked with protecting the personal data and PII of their sources and keeping communications between themselves and sources safe. Journalists are often entrusted with deeply personal, confidential information revealed to them by sources. It is a journalist's duty to keep the information being shared with them, in addition to the PII of that source, private.

Why do journalists have a duty to protect the PII of sources?

Confidentiality and anonymity of sources are often integral to the meaningful practice of journalism and for journalists to fulfil their role as the "public watchdog". Keeping journalistic sources confidential helps journalists properly uncover and investigate stories and protects whistleblowers or sources of information from suffering the negative consequences of exposure.

Not protecting the data, identities and privacy of sources can have long-lasting negative repercussions. These repercussions can be felt by the journalist, the source, the media organisation for which the journalist is collecting information, and the culture of journalism as a whole.

The leaking of information between a journalist and a source can lead to pre-publication cover-ups of sensitive events being investigated by the journalist. It can lead to intimidation and harassment of the source or even legal action being taken against them. It can lead to the "chilling" effect of that source or other sources refusing to communicate further with journalists, leading to self-censorship or the "drying up" of sources in general for the journalistic community.

What are the exceptions to the confidentiality of source data?

While journalists do have a paramount responsibility to keep data about their sources safe, there are exceptions to this practice. These include situations where there is a real threat to human life, where the journalist's own life may be in danger, the journalist witnessing a grave crime, or when the journalist herself is being accused of a crime. When considering revealing a journalistic source, there should ideally be no other viable option than to reveal the source, the value of revealing the source should result in greater public good than protecting the source, and as little information about the source should be revealed as is absolutely necessary.

Women and queer journalists and sources are at particular risk of negative repercussions of data leakages.

Women journalists are susceptible to more significant physical harm and sexual harassment in their work and are more likely to become targets of online harassment campaigns. Women journalists and those belonging to gender or sexual minorities often have to use digital platforms to safely gather information in situations that pose additional risks to their safety, especially in cases where the journalist's safety would be compromised if they were physically present at the scene. Female sources and sources belonging to sexual or gender minorities also face more significant risks of harm, threats to their physical or mental safety, and threats to their livelihood and places of shelter if their identities are made public. Thus, women and queer journalists are compelled more than others to use digital platforms to communicate safely.

Furthermore, privacy breaches can lead to the leaking of different kinds of information about different groups. Queer individuals have been reported to use online platforms to access safe spaces, communities, romantic partners and health information. The consequences of this kind of sensitive information being leaked can have severe physical, psychological, or practical harm to queer individuals, including loss of life, livelihood, shelter and other threats to safety. Breaching the data privacy of queer individuals also risks exposing their networks and contacts.

The protection of data privacy between women and queer journalists and sources is an additional concern that needs to be kept in mind when conducting journalistic work. Journalists have an additional duty to keep the information of women and queer individuals particularly safe as there exist further consequences to such individuals' privacy being compromised. This becomes even more relevant in countries where certain gender or sexual identities or activities are criminalised.

References:

https://www.unesco.org/en/articles/unesco-releases-new-publication-protecting-journalism-sources-digital-age
https://link.springer.com/article/10.1007/s11205-020-02565-8
https://staysafeonline.org/online-safety-privacy-basics/data-privacy-crucial-lgbt-community/
https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/
https://privacyinternational.org/explainer/56/what-privacy
https://www.britishcouncil.org/voices-magazine/what-stops-girls-south-asia-getting-online
https://www.okta.com/identity-101/pii/
https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/source-protection-and-the-protection-of-journalistic-materials/
https://link.springer.com/chapter/10.1007/978-3-030-82786-1_12#:~:text=People%20in%20collectivistic%20cultures%20consider,coordination%20with%20their%20group%20members.
https://privacyinternational.org/explainer/56/what-privacy
https://www.econstor.eu/bitstream/10419/168531/1/Omrani-Soulie.pdf
https://www.ifamilystudy.eu/what-is-autonomy-and-why-does-it-matter/
https://internetdemocracy.in/reports/whats-sex-got-to-do-with-it-mapping-the-impact-of-questions-of-gender-and-sexuality-on-the-evolution-of-the-digital-rights-landscape-in-india
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3113158
http://138.25.65.17/au/journals/UNSWLRS/2018/11.pdf
https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/10/data-protection-and-journalism-media-guidance.pdf

Notes

Notes

Notes

Talking data to the fourth pillar

defindia.org

No# 44, 2nd & 3rd Floor, Kalu Sarai,
Near Naraina IIT Academy, Delhi 110017
info@defindia.org

Talking data to the fourth pillar