Talking Data to the Fourth Pillar

DIGITAL EMPOWERMENT foundation

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Talking Data to the Fourth Pillar

Module 3

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

What are some practical steps journalists can take to protect their devices from attacks on their digital privacy?

Journalists can protect their devices and their sources' information from being hacked by following these steps:

Keep software up-to-date: Regularly update the operating system and all other software on your devices to ensure that security patches and bug fixes are installed.

Use antivirus software: Install antivirus software on all your devices to detect and prevent malware infections.

Secure your passwords: Use strong passwords and enable two-factor authentication whenever possible. Avoid reusing passwords across different accounts.

Encrypt sensitive information: Use encryption to protect sensitive information, both on your devices and in transit.

Be cautious of public Wi-Fi: Open Wi-Fi networks can be convenient for journalists who are on the go or do not have access to more secure Wi-Fi connections, but must be used very carefully. In situations where using open Wi-FI networks is unavoidable, journalists must be sure to avoid accessing sensitive information, such as login credentials or confidential files, while connected to an open Wi-Fi network, avoid public file sharing and decline to use open Wi-Fi networks to share large files, such as images or videos, as this can put their data at risk. Be wary of free Wi-Fi networks that are not provided by reputable companies, as they may be set up by hackers to steal personal information. Avoid using public Wi-Fi networks to access sensitive information. If you must use public Wi-Fi, use a VPN to encrypt your internet traffic.

VPN : A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over the internet. VPNs are useful for journalists

because they help protect sensitive information, both in transit and at rest, by encrypting all internet traffic. When a journalist uses a VPN, their internet connection is routed through a server operated by the VPN provider. The VPN provider encrypts the journalist's internet traffic, making it difficult for anyone to intercept or access sensitive information. Additionally, VPNs can help journalists maintain privacy and security while using public Wi-Fi networks. Public Wi-Fi networks are often vulnerable to hacking and eavesdropping, but with a VPN, the journalist's internet traffic is encrypted, reducing the risk of sensitive information being intercepted.

TOR: Tor (The Onion Router) is a privacy-focused network that allows journalists to browse the internet anonymously and access censored or restricted websites. Journalists can benefit from using TOR as it provides journalists with anonymity by routing their internet traffic through a series of servers, making it difficult for anyone to trace their online activity back to their device. It also allows them access to censored information: In some countries, the government censors or restricts access to certain websites. Tor allows journalists to bypass these restrictions and access censored information. TOR additionally offers protection from government surveillance by encrypting their internet traffic and routing it through a series of servers, making it difficult for anyone to intercept or monitor their online activity. TOR can also be used to access secure websites and communicate with sources in a confidential manner.

Educate sources on security: Advise sources on the importance of protecting sensitive information and provide them with guidance on how to do so.

In addition to using VPN and private internet connections, utilising strong passwords and anti-virus software, there are also several secure private messaging chat apps that journalists can use to conduct their work, including Signal, Telegram, Whatsapp, Wickr, Threema and others.

Whatsapp vs Signal vs Telegram

Whatsapp, Signal and Telegram are three of the most widely used encrypted messaging platforms in India. However, they offer different levels of security and data privacy.

Signal is fully open-source, and is a free app developed by the non-profit the Signal Foundation. Signal collects only your phone number, and does not collect or store any of your data outside of this. Through Signal, you can send fully encrypted text, audio, photo or video messages to individuals or groups on Signal after verifying your phone number. Besides its default powerful

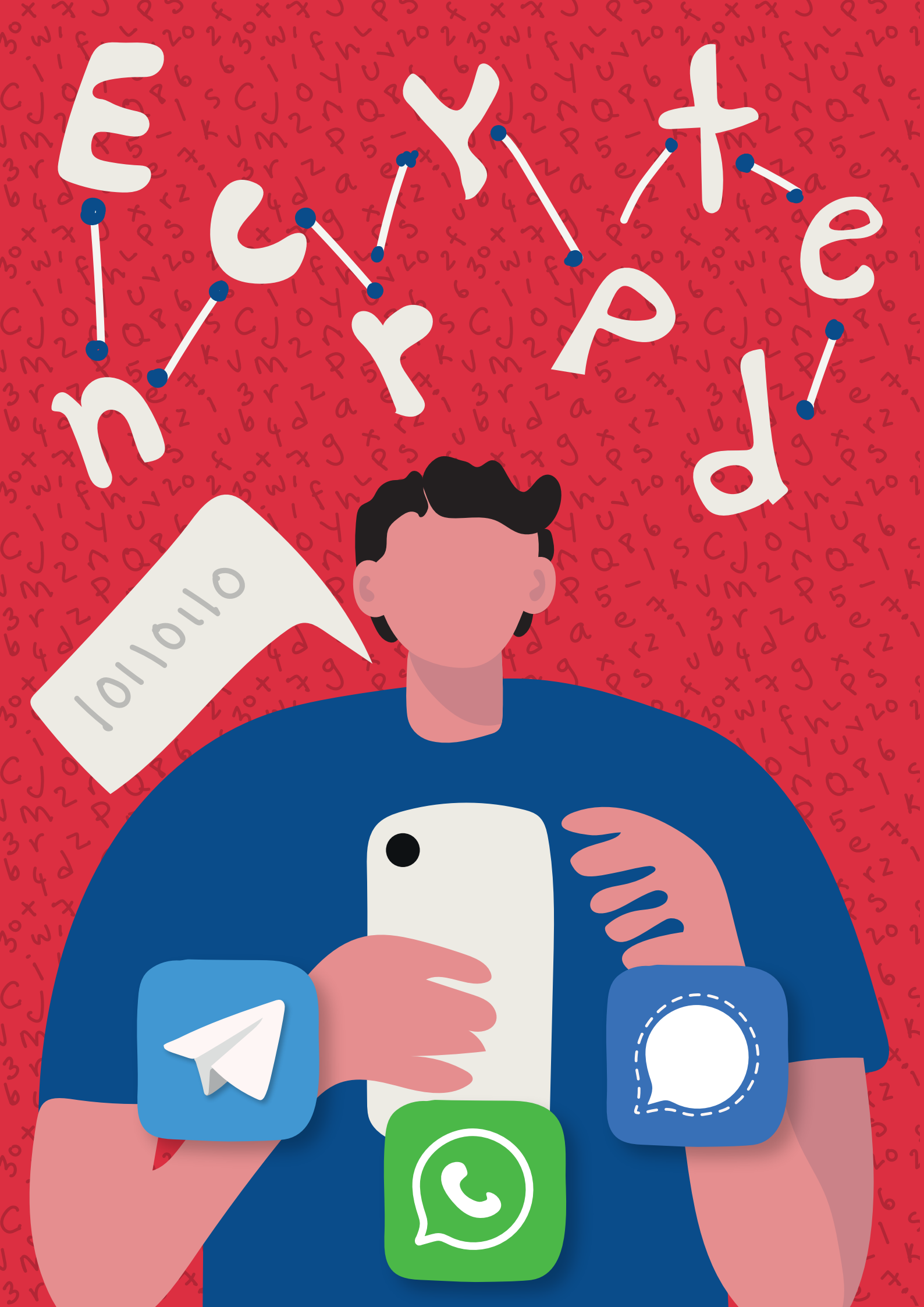
encryption, Signal offers in-app privacy extensions, such as an app-specific lock and face-blurring anti-surveillance tools. Compellingly, data privacy activist and US-whistleblower Edward Snowden uses Signal.

Telegram is a partially open-source messaging service that offers encryption. Telegram collects your name, phone number, contact list, user ID and IP address, which Signal does not do. Telegram, unlike Whatsapp and Signal, does not offer automatically encrypted one-to-one messages, but users can turn on the encryption function in their personal settings. You cannot send encrypted group messages on Telegram.

Of these three messaging services, **Whatsapp** collects the most information about you, including your unique device ID, your location, the products you've interacted with, your financial information, how often you use the app…the list goes on. Given that Whatsapp is owned by Facebook, this compounds concerns about privacy and usage of your personal information. Whatsapp uses the same encryption protocol as Signal, but most of its code, outside of encryption, is not open source. While Whatsapp encrypts conversations between people and groups, it does not encrypt metadata. Whatsapp is considered easier on the eyes and easier to use than the other two apps mentioned here. Signal, despite its strong privacy protocols, has not been widely adopted. Telegram offers data privacy features and collects less user information than Whatsapp, but does not provide privacy protections as robust as Signal.

In terms of handing over user data to third-parties or governments, Signal has the strongest privacy policies, with a stated commitment to resist demands for user data, while Telegram and WhatsApp have stated that they will only provide user data in response to valid legal requests. While Telegram and Whatsapp have said they will hand over data when presented with legal requests from governments in particular jurisdictions, this gives rise to grave concerns about government surveillance given that most countries have data privacy exceptions for governments working in the interest of national security or law and order. However, Telegram has stated that they have handed over 0 bytes of data to governments or third parties and do not intend to do so in the future. Signal has publicly stated that they do not store any metadata or user data that can be linked to a specific user, and that in the event that the company receives a request for user data from a government, they will evaluate it based on the jurisdiction, the validity of the request, and the legal basis for the request. The company has stated that they will resist demands for user data and will only comply with legally binding requests.

Journalists should also be careful to use secure email platforms to conduct their work. ProtonMail is widely accepted to be the best, most secure email


Encrypted
10110110

platform. ProtonMail was founded in 2014 at the CERN research facility by Andy Yen, Jason Stockman, and Wei Sun. The Switzerland-based platform also stores its servers in two locations in Switzerland, which is protected by some of the world's strictest privacy laws. is free if you send fewer than 150 messages a day, and open source, and provides end-to-end asymmetric encryption. All email data is stored with zero-access encryption, which means even ProtonMail employees can access your data.

How can journalists and journalism organisations protect against online harassment?

Gideon Sarpong, a media security professional and founder of iWatch Africa wrote in Reuters that she recommends a five point action plan for dealing with online harassment in newsrooms. These five points are:

Build digital rights literacy: This includes information journalists about the various threats that they can be exposed to, providing useful content to them that engages with the subject and having continual, frequent formal and unofficial discussions and conversations about online harassment and the forms it takes.

Establish safety practices: This includes making it clear that the organisation does not condone online harassment as a "rite of passage" for a journalist, and that it takes online harassment seriously. All instances and varieties of online harassment should be noted.

Conduct risk assessments: In each case of reported online harassment, the organisation should ask the risk level of the case, focusing on physical risks, psychological risk, and damage to the organisations reputation. In all cases, the subjectivity of the journalist should be taken into account: harassment on the basis of gender, sexual identity or religious status can be particularly damaging, and place such individuals at risk of being in need of professional support.

Implement support mechanisms: This includes providing legal or psychological support or funds for journalists to avail professional services.

Assign roles and tasks: The organisation needs to have a clear, compassionately set hierarchy of reporting and addressing online harassment. Those in such positions should be chosen carefully: would women journalists feel comfortable speaking to that individual about the harassment they face or the emotional repercussions of it?

Journalists can also rely on several international groups for safety, protection, and support, including:

Committee to Protect Journalists (CPJ): CPJ is an independent, non-profit organisation that promotes press freedom and defends the rights of journalists worldwide.

International News Services (INS): INS is a non-profit organisation that provides support to journalists in danger, including security training, legal assistance, and advocacy for their protection.

Reporters Without Borders (RSF): RSF is an international organisation that defends the freedom to inform and to be informed and provides support to journalists in danger.

International Federation of Journalists (IFJ): The IFJ is the world's largest organisation of journalists, representing over 600,000 journalists in more than 140 countries. It provides support to journalists in danger, including legal and financial assistance.

International Women's Media Foundation (IWMF): The IWMF is a non-profit organisation that promotes the participation of women in the media and provides support to female journalists in danger.

Human Rights Watch (HRW): HRW is an international human rights organisation that provides advocacy and support to journalists and media workers who face safety risks and threats to their freedom.

In India, there are several journalist organisations that journalists can rely on for help, including:

Press Institute of India (PII): The Press Institute of India is a non-profit

organisation that provides training, research, and support to journalists.

Indian Women's Press Corps (IWPC): The Indian Women's Press Corps is a forum for women journalists in India to address issues related to gender and the media.

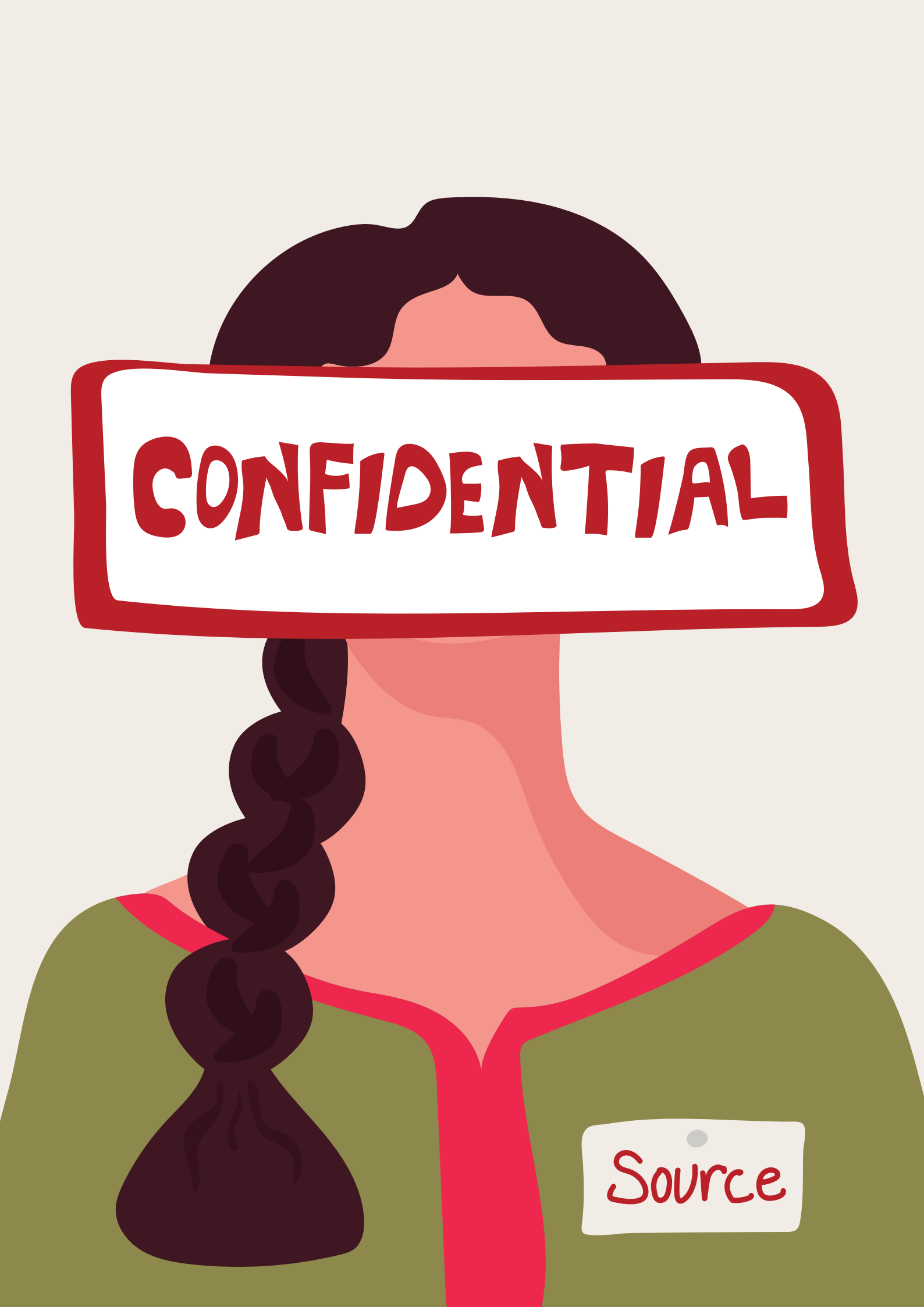
The Editors Guild of India: The Editors Guild of India is an organisation of senior editors and journalists that works to promote media freedom and ethical journalism in India.

Network of Women in Media, India (NWMI): The Network of Women in Media, India is a forum for women journalists in India to address issues related to gender and the media.

The Indian Journalists Union (IJU): The Indian Journalists Union is a national organisation of journalists in India that works to promote media freedom and protect the rights of journalists.

How can journalists undertake their work in a way that is respectful of sources, their dignity and their privacy?

Given the nature of journalistic work, journalists are often privy to exceedingly sensitive or private information provided by sources, and the personal data of the sources themselves. When collecting personal information for a story from different kinds of sources, journalists must be cognizant of their responsibility to conduct research and reporting in a way that is empathetic and respectful to the source.


CONFIDENTIAL
Source

Journalists should conduct ethical reporting that respects the privacy of sources by following these steps:

Obtain informed consent: Before conducting an interview or using information from a source, make sure the source is aware of the purpose of the interview and the intended use of the information. Obtain the source's informed consent before proceeding.

How does one obtain informed consent? Explain the purpose of the interview or information gathering: Before conducting an interview or gathering information, make sure the source understands the purpose of the interview and how the information will be used. Inform the source of any potential risks associated with providing information, such as the possibility of their name or information being published or shared with others, or being identified in other ways, and the consequences of that revelation being made public. Does the source still want to speak after fully understanding the real and potential risks associated with it? If the source requests anonymity, make sure to respect their request and not disclose their identity without their consent. When dealing with people who may not be fully aware of the implications of speaking to a journalist, show them examples of previously published stories and story formats to demonstrate how their inputs will be presented in the completed product.

Protect the source's identity: Consider the potential consequences of publishing a source's identity and take appropriate measures to protect their privacy and safety, such as using a pseudonym, withholding their name, or blurring out their faces. The journalist also shares a responsibility to ensure that no one in the immediate vicinity of a confidential source is aware of the source's identity. This may mean limiting communications with the source, and meeting the sources at locations that are safe and comfortable for the journalist, but also secret and private for the confidential source.

Avoid disclosing confidential information: Do not disclose confidential information obtained from a source without their consent. If a source provides sensitive information that could harm them or others, weigh the public's right to know against the potential harm before deciding whether to publish it.

Verify information: Ensure that the information you receive from a source is accurate and verify it through multiple sources before publishing it. Speak to several sources to understand various angles and nuances of a story.

References:

https://reutersinstitute.politics.ox.ac.uk/protecting-journalists-online-abuse-guide-newsrooms
https://datajournalism.com/read/longreads/privacy-day-security-guide#:~:text=It%20is%20recommended%20that%20journalists,else%20has%20access%20to%20it.
https://www.forbes.com/sites/forbestechcouncil/2018/10/03/10-data-privacy-tips-for-journalists-and-reporters/?sh=6692d990272c
https://www.comparitech.com/blog/vpn-privacy/protection-of-journalistic-sources/
https://cpj.org/2021/11/digital-physical-safety-protecting-confidential-sources/#digital
https://ethics.journalists.org/topics/interviewing/
https://ethics.journalism.wisc.edu/files/2020/07/33-Journalist-Interview-Assignment-Walsh-Childers.pdf
https://www.cnet.com/tech/services-and-software/signal-whatsapp-and-telegram-heres-which-secure-messaging-app-you-should-use/#:~:text=Data%20collected%20by%20Telegram%20that,aren't%20encrypted%20by%20default.
https://beebom.com/whatsapp-vs-telegram-vs-signal/
https://www.tandfonline.com/doi/full/10.1080/15405702.2018.1548019

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