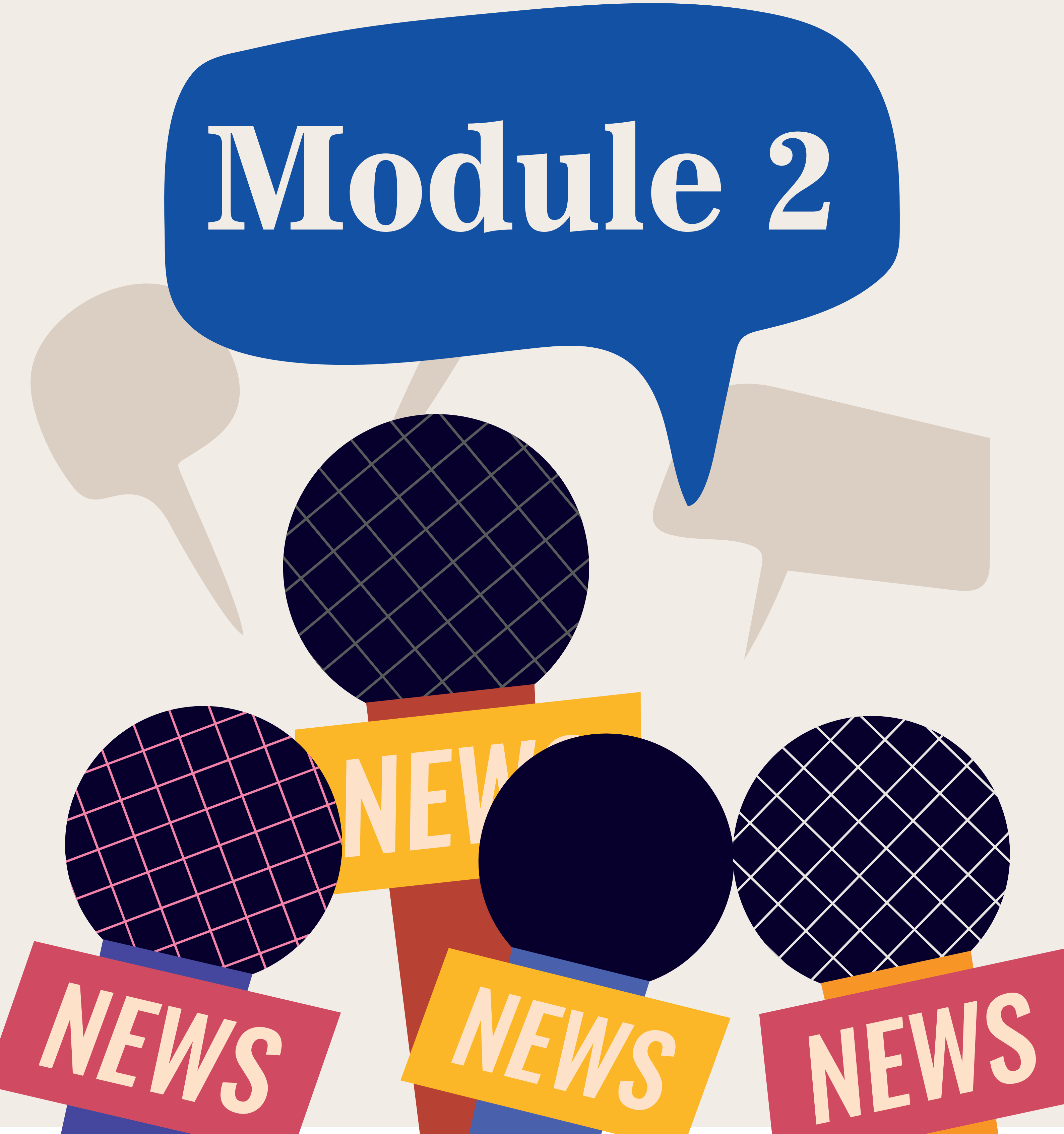
Talking Data to the Fourth Pillar

DIGITAL EMPOWERMENT foundation

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Talking Data to the Fourth Pillar



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 are journalists the particular target of threats, including to their privacy?

The very nature of the work of journalism often puts journalists at odds with those who want to keep information secret, hold on to power or silence critics. While the killings of journalists are showing a declining trend, UNESCO still refers to journalism as a "deadly" profession, and states that "the global rate of impunity for killing journalists is worryingly high: nine times out of ten, the case remains unresolved." Journalists continue to be prime victims of threats, violence, murder, physical, sexual and mental harm and harassment.

Due to the particular nature of their work and the fact that journalism is increasingly being conducted through and published on digital platforms, journalists are particular targets for threats to or invasions of their digital privacy.

This is because journalists:

a) Have access to sensitive information: Journalists often have access to sensitive information and are privy to confidential sources and documents that others do not have access to. This can make them a target for those who want to keep information secret or who want to silence critical reporting.

b) Report on sensitive issues: Journalists may report on sensitive issues such as corruption, human rights abuses, and political violence, which can make them a target of privacy breaches due to the strong reactions they evoke, or the powerful entities they provoke.

c) Hold power to account: Journalists play a crucial role in holding powerful individuals and organisations accountable for their actions. Such individuals and organisations often have the motivation and ability to silence or intimidate journalists without facing immediate or massive repercussions.

d) Lack of legal protection: In many countries, including India, journalists lack legal protection when it comes to protecting the privacy of their sources and themselves, which can make them more vulnerable to attacks.

Which countries legally protect journalistic sources?

United States: The U.S. has a strong tradition of protecting freedom of the press and the First Amendment of the Constitution guarantees freedom of the press. There is no federal shield law in the U.S, however, some states like California and Colorado have shield laws, which offer some protection to journalists from being forced to reveal their sources in court.

Canada: The Canadian Charter of Rights and Freedoms protects freedom of the press and freedom of expression, and many provinces have shield laws that protect journalists from being forced to reveal their sources in court.

France: The French Constitution guarantees freedom of the press, and the Civil Liberties Act of 1881 provides protection for journalists' sources.

Germany: The German Constitution guarantees freedom of the press, and the Federal Press Law provides protection for journalists' sources.

Australia: The Australian Constitution guarantees freedom of the press, and some states and territories have shield laws that protect journalists from being forced to reveal their sources in court.

South Africa: The South African Constitution guarantees freedom of the press and the Promotion of Access to Information Act of 2000 provides protection for journalists' sources.

The Constitutions of Spain, Sweden, Portugal and Andorra all mention the need to protect the confidentiality of journalist’s sources.

Legality of protecting journalistic sources in India:

India does not have a specific Act or law protecting journalistic sources. While the Indian Constitution guarantees freedom of speech and expression, including freedom of the press, there is no unqualified protection for journalists' sources in Indian law.

Furthermore, journalists are increasingly turning to digital mediums to contact sources and collect information from them.

However, the Indian courts have recognized the importance of protecting journalistic sources in certain cases. The courts have held that the right to protect sources is an integral part of freedom of the press and that journalists have a qualified privilege to protect their sources. The restrictions on protection of journalistic sources can, however, easily be misread, misinterpreted or misused.

Indian courts have recognized the importance of protecting journalistic sources in certain cases and have upheld the protection of sources as an integral part of freedom of the press. Here are some examples of cases where Indian courts have upheld the protection of journalistic sources:

In the case of Romesh Sharma v. State of Uttar Pradesh (1997), the Supreme Court of India held that the right to protect sources is an integral part of freedom of the press. The court also recognized that journalists have a qualified privilege to protect their sources, which can be overridden in certain circumstances, such as when the information is necessary to prevent a crime or to protect the public interest.

In the case of Indian Express Newspapers (Bombay) Pvt. Ltd. v. Union of India (1985), the Supreme Court of India held that the government cannot compel a journalist to disclose their sources unless there is a strong public interest in doing so.

In the case of Outlook Magazine v. Registrar of Companies (2002), the Delhi High Court upheld the protection of journalistic sources, stating that the media

What causes journalists to increasingly fall prey to digital Attacks ?

has a right to protect its sources and that the source should be protected unless there is a compelling public interest in disclosing the source.

In the case of Samir Jain v. Union of India (2007), the Delhi High Court held that a journalist has a right to protect his source and that the source should be protected unless there is a compelling public interest in disclosing the source.

The Press Council of India (PCI) has also issued guidelines for the protection of sources, stating that journalists should not disclose their sources unless they are compelled to do so by a court of law or unless the information is already in the public domain.

There is a marked absence of a specific, clear shield law protecting journalistic sources in India, combined with the legal uncertainty and lack of clear guidelines. There are also overriding qualifications or exceptions to the protections of journalistic sources in the face of court or government orders.

Given that the Indian IT Act allows the government or government officers to ask social media and messaging platforms to hand over requested information for a variety of reasons, including the investigation and prevention of any crime, some courts having stated that journalists should be allowed to protect their sources is inadequate protection to journalists and sources operating in an increasingly digital environment. Invasions to privacy are difficult to rectify after the fact, and in the space of government and intelligence agencies, it is difficult to ensure that matter once accessed has been destroyed.

This leaves journalists and their sources particularly vulnerable to different threats to their work, lives and privacy. The lack of robust legal protection to journalistic sources, and the lack of a special provision protecting the confidentiality of journalistic sources in India’s existing legislation around IT services, is particularly concerning in an increasingly digital world and journalistic workspace.

What causes journalists to increasingly fall prey to digital attacks in today's world?

Technological/economic challenges: Digital attack software and methods of digital surveillance are becoming increasingly common, easy to purchase and less expensive than in previous years, particularly for governmental actors.

On the other hand, digital security tools are often difficult to understand or operate, leading to inefficient usage by journalists. Open-source digital security tools tend not to be updated at a pace that keeps up with newer and more sophisticated emerging technologies and attacks. There is also not enough real-time information about the kinds of attacks and threats journalists have been or can be potentially exposed to. While more journalistic work than ever is being carried out on digital messaging platforms, journalists and their sources are largely not up-to-date with encryption software and the platforms that support them, and other measures to protect their digital privacy. Journalists are also often not well-acquainted with technological best-practices around digital privacy, nor are they generally necessarily acquainted with technologists who can assist them in these matters in a timely way.

Legal/political reasons: There is a lack of political will to take action against threats to journalists, especially threats to their digital privacy. This is unsurprising, given that governments and government actors are often alleged to be the ones who carry out sophisticated surveillance and data privacy attacks against journalists. Furthermore, most legal provisions protecting data privacy also carry exceptions around national security and protecting law and order, which can be read conveniently by governments in power to allow invasions of data privacy in the name of fighting against terrorism or other crimes.

Psychosocial challenges: A report prepared for UNESCO's Division for Freedom of Expression and Media Development postulates that "decision-fatigue" may cause journalists to choose not to opt for digital security measures.

Decision fatigue refers to the phenomenon of being mentally and emotionally drained from making too many decisions over a short period of time. Journalists are often required to make a large number of decisions on a daily basis, from deciding on story angles and sources to determining how to present information in a fair and accurate manner.

They also have to make quick decisions in high-pressure situations, such as covering breaking news stories, meeting deadlines, and balancing competing demands from editors, colleagues and audiences. Journalists also have to make ethical decisions on a regular basis, such as whether to reveal a source's identity or not, whether to cover a story or not, whether to publish a story or not, whether to use a certain source, etc. Working in this kind of high-stress environment where the stakes are consistently high can lead to journalists experiencing decision-fatigue, or just fatigue in general, leading them to make poor choices around digital safety.

Journalists may also face unintentional leakages of information from well-meaning friends and family members, through the social media accounts or conversations of friends and family members.

What are the ways in which journalists (intentionally or unintentionally) pose threats to the privacy of their sources?

1. Lack of security: Journalists may inadvertently expose sources to harm by not properly securing their communications or by failing to take appropriate measures to protect their identity, such as the use of encryption.

2. Unauthorised disclosure: Journalists may accidentally or intentionally publish or reveal the identity of a source without their consent, which can put the source at risk of retaliation.

3. Negligence: Journalists may fail to take appropriate steps to protect the identity of a source, such as redacting sensitive information, using pseudonyms or blurring out the faces of at-risk persons on television. This can happen due to the journalists negligence, lack of care or hurry to break a story before a competing outlet.

4. Exploitation: Journalists may use a source's identity or personal information to further their own interests or to sensationalise a story, which can put the source at risk of retaliation or harm, or cause the source to be depicted in a way that is offensive to their dignity or privacy. Journalists may do so to further a political or social aim, or to increase their own popularity or professional success.

What are some common cyber attacks that journalists need to be particularly wary of?

Doxxing: The term "doxxing" comes from the phrase "dropping dox," or "dropping documents", which refers to the practice of publicly releasing PII ("documents") about someone. Doxxing is the act of publicly revealing or publishing private information about an individual without their consent, typically with the intent to harm or intimidate the individual. This information can include the person's full name, address, phone number, email address, and other personal details. Doxxing can be particularly dangerous when the person being doxxed is a woman or member of a minority community, as they are at increased risk of violence, physical intimidation and harassment.

Phishing attacks: Phishing attacks are a type of cyber attack where the attacker attempts to trick the victim into providing sensitive information, such as login credentials or financial information, by disguising themselves as a trustworthy source. This is often done through email, where the attacker sends an email that appears to be from a legitimate source, such as a bank or a government agency, and requests the victim to click on a link or enter their information into a fake website.

Journalists may be particularly susceptible to phishing attacks because they often receive emails from sources they are not familiar with. Additionally, journalists may be targeted by attackers looking to gain access to sensitive information related to their reporting.

DDoS attacks: A DDoS *(Distributed Denial of Service)* attack is a type of cyber attack in which an attacker attempts to make a website or network resource unavailable to its intended users by overwhelming it with a flood of traffic from multiple sources. This traffic can come from compromised computers and devices that have been infected with malware, as well as from networks of compromised devices (such as IoT [Internet of Things] devices) that have been taken over by the attacker.

DDoS attacks can be harmful because they can cause a website or online service to become unavailable, resulting in lost revenue and damaged reputa

DATA Mining

tion for the affected business. Additionally, DDoS attacks can be used to distract and divert attention away from other cyber attacks that may be happening simultaneously.

DDoS attacks can make a journalist's website or online platform unavailable, preventing readers from accessing their content. This can result in lost readership and revenue for the journalist or media organisation, as well as damage to their reputation from users who assume that their site is no longer properly functional.

MitM (Man in the Middle) attacks: A man-in-the-middle (MITM) attack is a type of cyber attack in which an attacker intercepts and alters the communication between two parties without their knowledge or consent. The attacker essentially "eavesdrops" on the conversation and can modify, read or inject new data into the conversation. This can happen in various ways, such as by using a rogue wireless access point, intercepting network traffic, or compromising a device on the network.

There are several types of MITM attacks, such as:

IP spoofing: the attacker alters the source IP address in a packet so that the targeted device believes the packet is coming from a trusted source.

ARP spoofing: the attacker alters the ARP (Address Resolution Protocol) table on a device, so that the device sends traffic to the attacker's device instead of the intended recipient.

SSL/TLS spoofing: the attacker intercepts and alters the SSL/TLS certificate of a website, allowing them to intercept and read encrypted communications.

MITM attacks can be particularly dangerous because they can give the attacker access to sensitive information such as login credentials, financial data and personal information. They can also be used to spread malware and perform other malicious activities.

Fake domain attacks: Fake domain attacks, also known as typo-squatting or domain spoofing, are a type of cyber attack in which an attacker creates a domain name that is similar to a legitimate domain name, in order to trick users into visiting a malicious website or providing sensitive information.

For example, an attacker may create a fake domain name such as "newslaundry.org" that is similar to the legitimate domain name "newslaundry.com" in order to phish for login credentials or steal sensitive information.

Journalists can be affected by fake domain attacks in a number of ways. For example, an attacker may create a fake domain that is similar to a legitimate news website and use it to spread disinformation or fake news. This can damage the reputation of the legitimate news organisation and undermine the public's trust in journalism in general.

Shadow banning: Shadow banning is a form of censorship in which a social media platform or online forum limits the visibility of a user's content without informing them. The content is not removed outright, but instead is made less visible to other users. This can include hiding posts from a user's followers, hiding comments, or reducing the visibility of a user's account in search results.

For journalists, shadow banning can have a significant impact on their long-term ability to reach their audience and share their content. If a journalist's posts are shadow banned, their followers may not see their content, and their reach may be greatly reduced in a way that can be nearly impossible to recover from due to the nature of social media algorithms. This can make it more difficult for them to build and sustain a following and continue to establish themselves as credible sources of information.

Journalists who cover sensitive political or social issues may be targeted by a coordinated campaign to silence their reporting through mass reporting of their accounts or flagging their content as inappropriate, leading the social media platform they operate on to shadow ban them.

Data mining: Data mining attacks are a type of cyber attack in which an attacker attempts to extract sensitive information from a large dataset. This can include personal information, financial data, and confidential business information. Data mining attacks can be performed using a variety of methods, including SQL injection, phishing, and malware.

Journalists are susceptible to data mining attacks because they often handle sensitive information, such as confidential sources and classified information. An attacker may target a journalist's personal devices, email accounts, and other online platforms in order to extract this information.

In addition, data mining attacks can be used to target news organisations, where the attacker can extract information from the organisation's databases and use it for their own purposes. This can include information about employees, financial data, and confidential information about ongoing stories.

Intimidation: Journalists may be intimidated, particularly by governmental authorities, into giving up their social media account passwords or other sensitive digital information that compromises their own digital privacy, or the digital privacy of their organisation, when arrested or detained. While the intimidation of journalists and activists has been practised for decades, advancements in technology pose new kinds of challenges to journalists and media organisations.

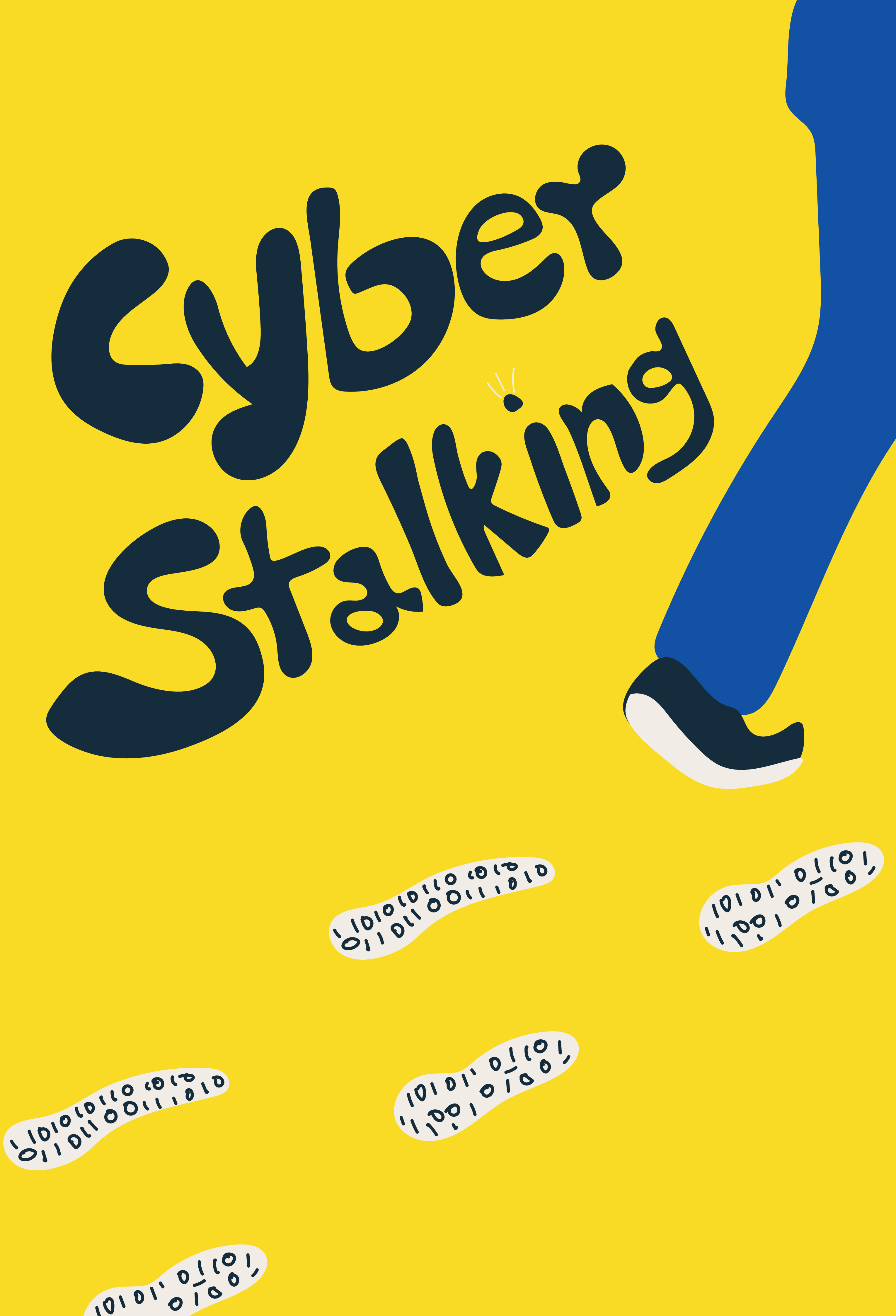
Surveillance: Journalists may be subject to some of the above attacks, or other methods of surveillance, by government actors acting as bad agents, or using legal methods or tools (such as court orders or exemptions to digital privacy laws) to surveil them. Governments and state actors often use the sweeping exceptions to privacy laws in order to conduct mass or targeted surveillance, including upon journalists and activists.

he ethical and legal debates around surveillance and press freedom centre around the balance between the right to privacy and the right to freedom of expression, and the journalistic ethic of preserving the confidentiality of journalistic sources.

On one hand, governments and other actors may argue that surveillance is necessary to protect national security and maintain public safety. They may also argue that it is necessary to investigate and prosecute crimes, and to identify and neutralise terrorist threats.

On the other hand, journalists and press freedom organisations argue that surveillance can have a chilling effect on the free flow of information, as it can make sources and journalists afraid to speak out for fear of reprisals. They argue that free and independent journalism is essential for the functioning of a healthy democracy, and that surveillance can be used to silence critical voices and repress freedom of speech.

Cyber Stalking



What are the kinds of online harassment journalists may experience?

Troll armies: Online trolling has been defined as "the deliberate provocation of others using deception and harmful behaviour on the Internet which often results in conflict, highly emotional reactions, and disruption of communication in order to advance the troll's own amusement". Increasingly, online trolling also serves to advance a troll's social or political agenda, or that of a political party or ideology it subscribes to. Troll armies are groups of such individuals who use social media and other online platforms to deliberately spread misinformation and incite disruption. They often target journalists and news organisations in order to spread false or misleading information and to undermine the credibility of their reporting.

Cyberstalking: Cyberstalking is the use of technology, such as the internet, social media, and electronic devices, to harass, threaten, or intimidate someone. It can include actions such as sending persistent unwanted messages or emails, spreading false information about the person, or using their personal information to stalk them.

Women journalists and journalists from minority communities are especially vulnerable to cyberstalking, as their work often involves reporting on sensitive or controversial issues that can elicit strong reactions from individuals or groups who are more likely to direct their ire to women and members of social, sexual or gender minority groups. Cyberstalking can have a significant impact on journalists, both professionally and personally. It can lead to fear, anxiety, and stress, and affect their ability to do their job effectively or live their lives normally.

Sexual harassment: A 2017 survey by Norton of Symantec of Tier-1 Indian cities found that 41 percent of Indian women who use the internet reported facing online sexual harassment. Women and queer journalists are often particularly subjected to sexist, misogynistic, and violent language and threats, which can be particularly damaging and traumatic. Women journalists are also often targeted for their appearance, and their photographs and personal information are shared without their consent, leading to further harassment. Online sexual harassment can be amplified by the anonymity and lack of accountability on the internet, making it difficult for victims to seek justice.

Smear campaigns and disinformation campaigns: A smear campaign is a coordinated effort to damage the reputation of an individual or group by spreading false or deeply personal, professionally irrelevant information about them. A disinformation campaign is a similar effort, but specifically refers to the spread of false or misleading information with the intent to deceive.

Types of smear and disinformation campaigns targeted at journalists include:

Spreading false or misleading information about a journalist's reporting or personal life in order to discredit them.

Using social media and other online platforms to amplify false or misleading information and make it appear more credible.

Creating fake social media accounts or websites to spread false information and impersonate journalists.

Amplifying conspiracy theories about journalists in order to make their reporting appear biassed or untrustworthy.

References:

https://unesdoc.unesco.org/ark:/48223/pf0000379589
https://unesdoc.unesco.org/ark:/48223/pf0000232358
https://mouillere.com/universconvergents/wp-content/uploads/2015/06/An-International-Survey-of-Protections-and-Threats-to-Journalists%E2%80%99-Sources.pdf
https://weishenlawproject.wordpress.com/shield-law-in-other-countries/#:~:text=Countries%20like%20Austria%2C%20Norway%2C%20Belgium,(Article%2019%2C%202013).
https://www.theguardian.com/world/2013/aug/07/australia-journalist-protection-shield-laws
https://homes.cs.washington.edu/~franzi/pdf/JournoSec-PETS2016.pdf
https://feminisminindia.com/2023/01/20/cyber-harassment-trolls-and-cancel-culture-a-lingering-threat-to-women-and-queer-in-journalism/
https://journals.sagepub.com/doi/pdf/10.1177/1464884918769462
https://thewire.in/media/pegasus-project-spyware-indian-journalists
https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/
https://scroll.in/latest/974778/hathras-row-over-phone-tapping-as-india-today-reporters-conversation-with-womans-family-leaked
https://www.nytimes.com/2021/12/16/technology/harvard-job-scam-india.html
https://fraudwatch.com/common-cyber-attacks-what-are-mitm-dos-ad-ddos-attacks/
https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#SQL%20injection%20attack
https://intellipaat.com/blog/types-of-cyber-security/
https://blogs.blackberry.com/en/2017/11/all-about-the-cia-triad
https://www.imperva.com/learn/application-security/phishing-attack-scam/
https://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328
https://www.jdlasica.com/journalism/why-cybersecurity-should-be-front-of-mind-for-journalists/
https://www.orfonline.org/expert-speak/decoding-gendered-online-trolling-in-india/#_edn17
https://www.business-standard.com/article/current-affairs/eight-out-of-10-indians-suffer-cyber-harassment-norton-study-117100400643_1.html
https://www.shethepeople.tv/news/indian-female-journalists-facing-online-threats/

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