



The Dialogue™  
INFORM ENGAGE IDEATE

# HANDBOOK: HOW CAN JOURNALISTS EXERCISE THEIR RIGHT TO PRIVACY?

**Written By:** Kamesh Shekar, Manreet Khera  
**Designed by:** Kriti Singh



# HOW CAN JOURNALISTS EXERCISE THEIR RIGHT TO PRIVACY?

On August 24, 2017, a nine-judge Constitutional bench of the Supreme Court of India delivered its judgement on Justice K.S. Puttaswamy and others vs Union of India, declaring privacy as a fundamental right under Article 21 of the Constitution. Privacy as a constitutional value straddles various fundamental rights. It especially secures and strengthens the right to freedom of expression, which is the nut and bolt of well-functioning journalism.

As members of the fourth pillar of a democracy, journalists have a crucial role in informing citizens and making the government accountable. Journalists work under the constant threats from the state, which may carry out surveillance against them, or undertake other forms of abuse. Therefore, the fundamental right to privacy is integral to securing the integrity of journalism and information.

In the post COVID-19 scenario, journalists are now dependent on digital mediums to not only interact with their sources, but also to disseminate their work. How far can journalists exercise their right to privacy to secure information and maintain its integrity while extensively using the internet or internet-enabled technologies?

This handbook attempts to provide information on the statutory and legal protections that journalists have in securing their right to privacy. In addition, this handbook also lists various tools and practices for developing a secure end-to-end model of information sourcing and dissemination.

## 1. What do the courts have to offer?

Since 1954, the Supreme Court has tested whether the right to privacy should be a fundamental right under various cases. But Puttaswamy judgement collectively addressed the concerns of the privacy cases that preceded it, i.e. cases that fought for privacy against state excesses, unwarranted search and surveillance, against phone tapping, invasions of bodily privacy, restraints on freedom of speech, and even against methods of interrogation that invade the privacy of thought.

While the Puttaswamy judgement happened in 2017, different verdicts by the Supreme Court over time has set the contour for recognising the right to privacy as a fundamental right. These verdicts also found an exemplary connection between surveillance and fundamental rights, pushing back on surveillance measures to secure the fundamental right.

This section will discuss some of the surveillance measures targeted at journalists' and plug in the court verdicts that aid them in securing their right to privacy.

## 1.1. SEARCH AND SEIZURE

Law Enforcement Agencies (LEA) in India are empowered to perform search and seizure under various Indian legislation<sup>1</sup> to collect evidence in violation of the concerned legislation. LEA raids on media houses have increasingly become a significant concern for journalists because there is no clarity on what they are supposed to do and what they are not liable to do. For example, it is unclear whether any LEA can seize journalists' phones since they are just employees and their phones are their personal property. In a statement, the Editors Guild of India condemned the government raids and stated that they should not use coercive methods to crush the freedom of the press.

### How can journalists safeguard themselves?

The Maneka Gandhi case of 1978<sup>2</sup> allowed for wide interpretation of Article 21, which allowed privacy to find a place within the scope of Article 21. The verdict also provided that any restriction on Articles 14, 19 and 21 has to go through "due process of law" subjected to the triple test. This was re-emphasised by the Puttaswamy judgement of 2017<sup>3</sup>, where any interference on the right to privacy must meet the requirements of (i) legality, (ii) necessity, and (iii) proportionality.

As interference of the state in the form of search and seizure would violate journalists' privacy, it has to be subjected to the triple test. Therefore, the journalist must ensure that the respective LEA has a raid notice passed through "due process of law". As the first step the journalist must ensure the legality of the raid i.e., (a) if the subordinate authority has an approval of the Director or any officer not below the rank of Deputy Director authorised by the Director and (b) report has been forwarded Magistrate under Section 157 CrPC<sup>4</sup>. Second, journalists must look for necessity i.e., to check whether the order has a mention of scheduled offence<sup>5</sup> and appropriate evidence for the same. Thirdly, check if the evidence presented is proportionate to conduct search and seizure operations.

But the caveat to this protection is the reasonable restrictions like sovereignty, national security and public order.

## 1.2. PHONE TAPPING

To secure the interest of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order, the government institutes various measures like Legal Interception and Monitoring of Communications.

Section 5 of the Indian Telegraph Act states that phone tapping is allowed only in public safety and public emergency cases. In the amended Indian Telegraph Act, 1885, Section 5(2) permits the Central Government, State Government and any officer specially authorised by the Central Government or a State Government to intercept in case of public emergency or in the interest of public safety<sup>6</sup>. The Rule 419A of Indian Telegraph (Amendment) Rules 2017 provides direction for the interception under Section 5 (2) of the Indian Telegraph Act, 1885. The rules state that the requirement for interception has to be approved by the head or second most officer of the LEA within three working days. Post the approval; the final confirmation is needed from the Union home secretary in case of Central agencies & State home secretary for State agencies<sup>7</sup>. Besides, the rule provides for setting up a Review Committee - a monitoring body for lawful interception headed by the cabinet secretary.

1 Like Criminal Procedure Code (CrPC), Narcotic Drugs and Psychotropic Substances Act, 1985, income tax act, 1961, Prevention of Money Laundering Act, 2002 etc.

2 Maneka Gandhi v Union of India AIR 1978 SC 597

3 Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. AIR 2017 SC 4161

4 <https://indiankanoon.org/doc/279174/>

5 [https://finindia.gov.in/files/AML\\_Legislation/scheduled\\_offences.html](https://finindia.gov.in/files/AML_Legislation/scheduled_offences.html)

6 Sharma, S. (2013). Sunday ET: All you wanted to know about phone-tapping. Retrieved 1 November 2021

[https://economictimes.indiatimes.com/sunday-et-all-you-wanted-to-know-about-phone-tapping/articleshow/18882226.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cppst](https://economictimes.indiatimes.com/sunday-et-all-you-wanted-to-know-about-phone-tapping/articleshow/18882226.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst)

7 Not lesser than joint-secretary in unavoidable situation

According to a 2013 report<sup>8</sup>, on average, 9000 orders for the interception of telephones were being issued by various LEAs of the Central government every month. This means the numbers are significantly higher when we count in the orders from state government agencies. A phone can only be tapped for 180 days at most. After the 60th day, the interception request must be renewed by the LEAs from competent authority i.e., Union home secretary in case of Central agencies & State home secretary for State agencies. However, in an emergency, "authorised agencies" can tap a phone without permission, but if permission is denied, all records of taped conversations need to be destroyed in 48 hours<sup>9</sup>. Intercepting the communication of a journalist can infringe on the right to privacy and have a chilling effect on the right to freedom of expression. Besides, this would also hamper the integrity of information as the anonymity (in case) of sources will be exposed.

### How can journalists safeguard themselves?

In the People's Union for Civil Liberties case<sup>10</sup> (often known as the phone tapping case<sup>11</sup>), the court ruled that whether a person's right to privacy has been violated depends on the facts and circumstances of the case. But, the right to privacy is also derived from Article 19 because "when a person is chatting on the phone, he is exercising his right to freedom of speech and expression". The case brought communications under the right to privacy and significantly impacted communications laws by laying down rules on how and why phones can be tapped. Thanks to this case, now, phones can be tapped only with permission of the court or concerned department. Therefore, an aggrieved journalist (as a citizen) can file an FIR<sup>12</sup> and move to the Human Rights Commission as unauthorised tapping violates the right to privacy.

Besides, post Puttaswamy judgement, Bombay High Court in Vinit Kumar Case adjudicated upon the law pertaining to phone tapping and surveillance, applying the principles in relation to the right to privacy to section 5(2) of the Indian Telegraph Act. The High court firmly clarified that the interception request under section 5(2) of the Indian Telegraph Act has to be in 'public emergency' or 'public safety' situations. In case of proven contraventions, the agency has to destroy the data, and the same data will not be considered evidence in the court<sup>13</sup>. Therefore, an aggrieved journalist in case of proven contravention can demand the agency to destroy the data.

## 1.3. EXPOSING SOURCES AND DATA

Professional journalists have a strong obligation to protect their sources because they are frequently the person most at risk. The source of information usually expects the journalist to understand how to keep the information they provide secure, which is critical for building trust. But there are instances, where state and non-state actors compel the journalist to disclose their source and, on refusal, put them behind bars.

8 Sharma, S. (2013). Sunday ET: All you wanted to know about phone-tapping. Retrieved from Economic Times: [https://economictimes.indiatimes.com/sunday-et-all-you-wanted-to-know-about-phone-tapping/articleshow/18882226.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cppst](https://economictimes.indiatimes.com/sunday-et-all-you-wanted-to-know-about-phone-tapping/articleshow/18882226.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst)

9 Ibid

10 People's Union for Civil Liberties vs. Union of India & ors. AIR 1997 SC 568

11 "telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."

12 When proven guilty authorities can take penal action against a person who taps phones illegally. It could be 3 years of imprisonment under Section 26 (b) of the Indian Telegraph Act.

13 Mangaldas, C. A. (2019). Right To Privacy: Surveillance In The Post-Puttaswamy Era. Retrieved from BloombergQuint: <https://www.bloombergquint.com/law-and-policy/right-to-privacy-surveillance-in-the-post-puttaswamy-era>

## How can journalists safeguard themselves?

There is no concrete solution to this problem as the legal lacunae is yet to be filled with the answer on maintaining source confidentiality while securing larger public interest<sup>14</sup>. But, from a privacy perspective, in the Aadhaar case of 2014 (UIDAI v. CBI<sup>15</sup>), the court upheld "consent" as an essential facet of informational privacy. It restrained UIDAI from sharing any biometric information from its database without the consent of the owner.

This verdict made a giant leap to protect anonymity, where the court implied that people own the data and information about themselves. Interpreting this in case of forced disclosure of sources, technically any information on the source of a story is owned by the source, not by the journalist. Therefore, the 2014 Aadhaar case verdict could potentially help journalists protect their sources.

## 2. What do statutes/draft statutes offer?

The Puttaswamy judgement of 2017<sup>16</sup> vested a positive obligation over the government to protect informational privacy, where the MeitY formed a committee on Data Protection Framework under the chairmanship of Justice Srikrishna. The committee submitted its report and draft data protection bill on July 27, 2018. The Personal Data Protection Bill, 2019 (after making some significant changes to the 2018 version) was tabled in the 2019 winter session of the parliament and referred to the Joint Parliamentary Committee (JPC) for further deliberations.

The PDP Bill 2019 (now Data Protection Bill, 2021) would aid journalists in securing their fundamental rights like the right to privacy and the right to freedom of expression. While the draft bill with JPC tabling its report is one step closer towards becoming a legislation, it is yet to be enacted. Meanwhile, the Information Technology (Amendment) Act, 2008 fills in the gap by legislating some aspects of informational privacy under section 43,<sup>17</sup> 43A,<sup>18</sup> 72A,<sup>19</sup> and 66E.<sup>20</sup>

This section will discuss some of the legislative safeguards provided to journalists through these statutes.

### 2.1. DATA PROTECTION

To strike a balance between freedom of expression and the right to informational privacy, the Justice Srikrishna Committee suggested that the proposed law should consider "journalistic purposes" and whether the disclosure of specific data served the "public interest." The draft bill emphasises the public interest, and it also argues for broad definitions of what "journalism" and "journalist" mean in the context of data protection.

14 Mitta, M. (2012). No legal cover for journalists refusing to divulge sources. Retrieved from Times of India:

<https://timesofindia.indiatimes.com/india/no-legal-cover-for-journalists-refusing-to-divulge-source/articleshow/12499518.cms>

15 Unique Identification Authority of India (UIDAI) vs Central Bureau of Investigation (CBI) SLP (CRL) 2524/2014

16 Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. AIR 2017 SC 4161

17 Penalty and compensation for damage to computer, computer system, etc.

18 Compensation for failure to protect data

19 Punishment for disclosure of information, knowingly and intentionally

20 Punishment for violation of privacy

According to the committee report, media persons invoking journalistic exemption from the law should be able to reject requests to implement a data principals'<sup>21</sup> rights, such as "access, confirm, and correct", which may obstruct the publication of a report or the collection of information, or lead to harassment of the data principals. It has proposed an exemption that would allow journalists to preserve data for future work as long as they have a clear rationale, which may be led by the relevance of a specific piece of news, the level of intrusion it requires, as well as the potential impact on the data principal and third parties. The draft bill also advocates for the installation of security safeguards for journalists' personal data. "They must take reasonable efforts to prevent data loss, theft, or misuse," the committee emphasises, adding that individuals who take advantage of the exemption must guarantee their published work is not deceptive and distinguishes facts from opinions.

Besides, section 72A of the Information Technology (Amendment) Act, 2008 can be extended to secure the privacy and anonymity of the sources, as the service providers (journalists) are obliged (through contract) not to disclose information of an individual without consent.

## **2.2. PROTECTION FROM CYBERSTALKING AND CYBERBULLYING**

The cyberbullying and cyberstalking of journalists have become a common practice of intimidation. If people do not like a particular journalist, they will dig up everything personal and put it up or threaten them in digital spaces. While India lacks a separate statute for tackling cyberbullying and cyberstalking, some of the provisions within the Indian Penal Code (IPC) and Information Technology (Amendment) Act, 2008, can be interpreted to extend safeguards against the same. Section 353–357 of the Indian Penal Code provides safeguards and punishment for stalking, especially the criminal law (Amendment) Act, 2013 includes "Stalking" as an offence under Section 354D.<sup>22,23</sup> Therefore, journalists can protect themselves from cyberstalking by lodging a complaint under these appropriate sections of the Indian penal code.

---

21 Under the PDP Bill 2019, Data Principal means "the natural person to whom the personal data relates"

22 <https://www.indiacode.nic.in/show-data?>

[gclid=AC\\_CEN\\_5\\_23\\_00037\\_186045\\_1523266765688&sectionId=46125&sectionno=354D&orderno=398](https://www.indiacode.nic.in/show-data?gclid=AC_CEN_5_23_00037_186045_1523266765688&sectionId=46125&sectionno=354D&orderno=398)

23 However, it is noticed that provision on "stalking" is not gender-neutral law

Besides, section 499-507 of the Indian Penal Code provides criminal provisions for defamation. Journalists can specifically use section 500 (which makes defaming publishable) and section 503 (which makes threats through email into criminal intimidation) to lodge their cyberbullying complaints.

In addition, safeguarding data that can be easily hacked is critical for preventing cyberstalking and cyberbullying. Until the enactment of the Personal Data Protection bill, 2019, Section 43A of the amended Information Technology (Amendment) Act, 2008 allows for compensation in the case of a firm or a company that causes any wrongful losses or gain to any person by way of transmitting any sensitive information. Using the words sensitive information instead of obscene or salacious material makes this section somewhat relevant to journalists as any entity that discloses sources or sensitive data can then be held accountable. Besides, there are various provisions like section 66C, 66E and 67 in the Information Technology Act that protects journalists against cyberbullying.

### **2.3. IMMUNITY FROM ARREST**

Journalists can be targeted through imprisonment when they state the truth to power. But journalists can partly protect themselves against defamation laws if they take precautions to publish what they are sure of and can back it up with evidence. The best defence against defamation is truth, so it cannot be termed defamatory. Still, the Unlawful Activities (Prevention) Act, 1967 and Section 124A (Sedition) of the Indian Penal Code (IPC) have been used to arrest<sup>24</sup> many journalists who have spoken against the government using the exception of "compelling" state interest.

While there are no separate statutes that provide immunity to journalists from unlawful arrest, still they can reach out to courts to step in and enforce the constitutional right to free speech, free press and verify whether the compelling state interest holds up.

---

<sup>24</sup> <https://infogram.com/covid-19-ipi-tracker-on-press-freedom-violations-linked-to-covid-19-coverage-lh7z2lg0mqog4ow>

### 3. HOW CAN A JOURNALIST DO A PRIVACY HYGIENE CHECK?

While legal frameworks and statutes act as ex-post remedies, journalists should actively test their privacy hygiene using the below tools and checklist to ensure their functions are secured at an ex-ante level. It is important to understand that there are different perceptions of 'threat'. For instance, threats to a journalist will be different from threats to a lawyer. Similarly, it will be different for a business-beat journalist and a photojournalist. The simple way to determine your 'threat-model' to be able to tackle it efficiently is by figuring out the worst nightmare you can face digitally as an individual w.r.t to your both professional and personal life. Further, how it may impact your organisation and loved ones, respectively. After establishing your 'threat-model' you can tailor your practices and tools according to the needs:

1. **Awareness & education:** Journalists can educate themselves and become more aware of their rights and tools through the Digital Training Module On How To Protect Privacy Of Sources & Self<sup>25</sup>, released by Reuters. Alternatively, for context-specific queries feel free to reach us out at [editor@thedialogue.co](mailto:editor@thedialogue.co)
2. **Talking to sources:** Journalists should first determine whether encrypted communication is legal, technically and practically feasible (without attracting unnecessary attention). Databases containing contacts or sources should be password-protected, and interview notes and recordings should be stored securely<sup>26</sup> using technological tools discussed in section 4.3.
3. **Keep checking:** Journalists must have their phones checked for malware and for account breaches. Besides, journalists can also use tools and platforms like Have I Been Pwned?<sup>27</sup> to check if their personal information is compromised through data breaches.
4. **Take help:** If a journalist is stuck and not tech-savvy, should reach out for help. For instance, Tactical Tech's Data Detox Kit<sup>28</sup> lays out a solid and straightforward plan to keep all parts of digital life in check, make better and wiser choices and change online habits to best suit the life of a journalist.

25 <https://www.reutersagency.com/en/media-center/reuters-launches-the-reuters-digital-journalism-course-in-partnership-with-the-facebook-journalism-project/>

26 Journalist must beware of the fact that not anything online is liable to compromise

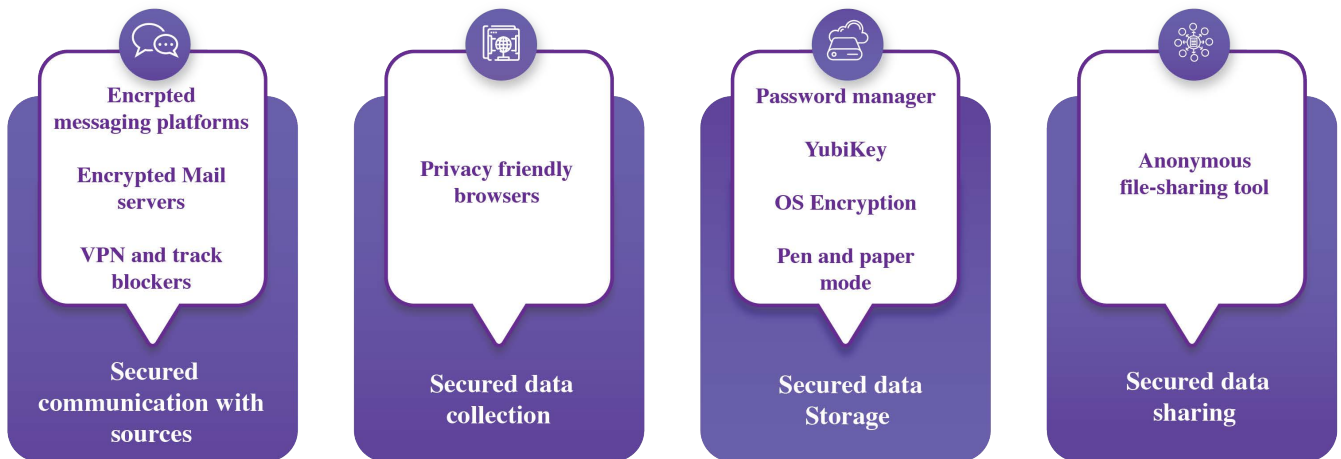
27 <https://haveibeenpwned.com/>

28 <https://datadetoxkit.org/en/home/>

## 4. WHAT DOES TECHNOLOGY OFFER?

Despite having a checklist for making journalists privacy-conscious, it has been noted that privacy consciousness and awareness does not translate into privacy-securing behaviour due to bounded rationality and lack of awareness. Therefore, this section maps various functions of the journalist to privacy enabling technological tools (as illustrated below) to secure their informational privacy without much effort.

FIGURE 1: MAPPING TECHNOLOGICAL TOOLS



### 4.1. SECURING COMMUNICATION WITH SOURCES

**Encrypted messaging platforms:** Signal<sup>29</sup> and Telegram<sup>30</sup> are widely used by the Journalist community. These are encrypted messaging apps that do not keep or share any data (or even meta data) of your conversations. In addition, these messaging platforms also provide opt-in features like disappearing messages, where any conversation between the journalist and the source will automatically get deleted post stipulated time.

Calls can also be made and recorded over Signal. Recording calls for transcription and later reference purposes is expected, but these recordings must be stored safely. Some people store them in pen drives, but rarely anyone trusts cloud services.

29 <https://signal.org/en/>

30 <https://telegram.org/>

**Encrypted mail servers:** ProtonMail<sup>31</sup> and Tutanota<sup>32</sup> provide extra encryption and protection for journalists who need an encrypted and secure email provider, enabling them to turn off logs, especially when dealing with more sensitive information. While usage of these mail servers is yet to pick up, journalists can still explore and use these resources wisely.

**VPN and tracker blockers:** VPNs<sup>33</sup> were used for protection, especially for conversations with sources. Journalists could, for example, use an avatar instead of their real identity, use a VPN to encrypt their connection and secure IP address, change PC address to disguise the device, and so on. Journalists could also use the assistance of Surveillance Self-Defense<sup>34</sup>, which the Electronic Frontier Foundation<sup>35</sup> developed. By implementing these measures, journalists can achieve some level of anonymity and make themselves a bit harder to track online or identify. However, it is essential to note that VPNs are not invincible and can still be breached. Besides, there are also less used alternatives like Zero-trust Security Network Access<sup>36</sup>, Secure Access Services (cloud-based)<sup>37</sup> etc.

In addition, track blocking browser extensions help journalists block the secret tracking orchestrated by third parties in terms of what they search, and which pages they visit. For instance, Electronic Frontier Foundation's Privacy Badger<sup>38</sup> is a free browser extension, which helps journalists block the third party from secretly tracking and posting advertisements on whichever page they end up on.

## 4.2. SECURING DATA COLLECTION

**Privacy-friendly browsers:** Journalists who browse for sensitive data and need anonymity could mask their identity online using privacy-friendly browsers like Tor<sup>39</sup>, which detaches any identifying information from your computer from websites you access. It can be installed<sup>40</sup> and used across several operating systems. Apart from Tor, you can use a secure, privacy-conscious browser such as Firefox<sup>41</sup>, Chromium<sup>42</sup> or Brave, and the extension HTTPS Everywhere<sup>43</sup> to make websites use a more secure connection, and uBlock Origin<sup>44</sup>, an extension to filter content.

---

31 <https://protonmail.com/>

32 <https://tutanota.com/>

33 The government is looking to ban VPNs, which will majorly affect Journalists.

34 <https://ssd.eff.org/en>

35 <https://www.eff.org>

36 <https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-37>

37 <https://www.mcafee.com/enterprise/en-in/security-awareness/cloud/what-is-sase.html>

38 <https://privacybadger.org/>

39 <https://www.torproject.org/download/>

40 <https://securityinabox.org/en/tools/>

41 <https://www.mozilla.org/en-GB/firefox/>

42 <https://www.chromium.org/Home>

43 <https://www.eff.org/https-everywhere>

44 <https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/>

### 4.3. SECURING DATA STORAGE

**Password manager:** Passwords must be strong and complex. Multi-factor authentication adds an extra layer of security. This is vital not only for cloud storage but also for securing internet accounts and gadgets. Even if a hacker cracks a journalist's password, they will still require a code to access the file. Therefore, to secure passwords, journalists can use a password manager that generates strong, distinct passwords and manages them. (e.g., KeePass<sup>45</sup> or Bitwarden<sup>46</sup>)

Restricting linked accounts and apps through password managers will help journalists' protect their cloud data. However, the very existence of cloud data is risky. The authorities and hackers can try to access cloud data on conventional platforms. If a journalist is tech-savvy and holds adequate resources, they should opt to build their own cloud server or a personal one<sup>47</sup>; otherwise, get a pod<sup>48</sup>.

**YubiKey:** A pen drive is handier than a hard disk, and though it may seem like mobile storage and cloud storage are making these obsolete, they are still relevant and beneficial to journalists. Besides, journalists can password protect pen drives. For instance, journalists can use multi-protocol tools like YubiKey<sup>49</sup> as a physical password or literally as a key that protects access to computers, networks, and online services. They can also be plugged in with most Operating Systems. However, this will likely be found and seized if journalists are searched, so hiding them well and encrypting them would be ideal.

**Operating System Encryption:** Journalists can securely store their data on the PC using files encryption features provided by two of the most prominent operating systems, i.e., Windows OS and Apple's iOS. In Windows OS, there is an opt-in feature called Encrypting File System (EFS)<sup>50</sup>, which aids the user to encrypt the information stored in the hard disk. In the case of Apple, most versions of iOS have encryption of files as a default setting. But to step up the security, iOS also provides an opt-in feature called FileVault<sup>51</sup>, which protects the encrypted files (password-based).

**Pen and paper mode:** This is the most vintage but the best note-taking and transcription method for sensitive data. Still, it is also most likely to land up in the wrong hands, so journalists must destroy (by fire - paper shredders aren't foolproof) any paper with sensitive information as soon as finishing the piece.

---

45 <https://keepass.info/>

46 <https://bitwarden.com/>

47 <https://www.cloudwards.net/diy-cloud-storage-tools/>

48 <https://solidproject.org/>

49 <https://www.yubico.com/>

50 <https://www.ccnv.cuny.edu/it/windows-os-encryption>

51 <https://support.apple.com/en-in/guide/mac-help/mh11785/mac>

## 4.4. SECURING DATA SHARING

**Anonymous file-sharing tool:** To share sensitive data, every journalist needs a secure and anonymous file-sharing tool like OnionShare<sup>52</sup> or SecureDrop.<sup>53</sup>

## 5. WHAT CAN YOUR ORGANISATION OFFER?

If you are a freelancer, that is all, folks for now. However, if you work for an organisation, make sure you ask them what privacy protections they afford you, from protected servers, freedom of unafraid speech, and breach checks to encrypted devices, software, and even anonymity and a lawyer.

To protect personal information, your organisation should invest in non-attributable tools and processes. Do you need a safe Dropbox folder to transfer files? Instead of your personal name, use your company's name and a non-attributable number for each user. If your organisation is not investing in these things or does not have a security manager who can assist you, ask your bosses to hire and/or conduct workshops with a trustworthy digital security expert to do it for you and teach you to do it successfully in the future.

Write to us and let us know some of the privacy protections afforded to you by your organisation.

## NEXT UP: THE PRIVACY JOURNALISTS GIVE

Quiz for the next issue:

1. Do you take permission before you click a picture for a story
  - a. When you're in a public place (y/n)
  - b. When the subject is a child (y/n)
  - c. When the subject of the photo is the subject of the story (y/n)
  - d. When there are no humans in the photo, but it is a private space (y/n)
  - e. When the subject is a celebrity (y/n)
  - f. When the subject is a victim (y/n)
2. Is information off the record if a person says off the record after disclosing the information? (Y/n)
  - a. Can you still publish it anonymously? (y/n)
  - b. Can you still store it? (y/n)
  - c. Can you report the grapevine or an eavesdropped conversation? (y/n)
3. How do you protect anonymous sources? (Short answer)
4. Are there any circumstances under which you could break anonymity? (What are they?)

---

<sup>52</sup> <https://onionshare.org/>

<sup>53</sup> <https://securedrop.org/>



The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

The Dialogue was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

Email: [info@thedialogue.co](mailto:info@thedialogue.co)  
Website: [www.thedialogue.co](http://www.thedialogue.co)



**The Dialogue**<sup>™</sup>

INFORM ENGAGE IDEATE

