To,
Justice Srikrishna Committee of Experts on Data Protection,
℅ Shri Rakesh Maheshwari,
Scientist 'G' and Group Coordinator, Cyber Laws
Ministry of Electronics and Information Technology,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi 11003

Submission by Electronic Frontier Foundation (EFF) to the Justice Srikrishna Committee of Experts on Data Protection

Dear Sir,

We welcome the opportunity to provide our views to the Committee of Experts on Data Protection. Since its founding in 1990, Electronic Frontier Foundation (EFF) has been committed to fighting for user rights and online privacy. Our work on protection of expression and speech on the Internet includes research on censorship technologies and policies, investigating corporate overreach and documenting government abuses of power. We also develop technologies that can help individuals protect their privacy and security online, which our technologists build and release freely to the public for anyone to use. In the United States, EFF is engaged in major legislative challenges, beating back digital censorship bills, opposing private censorship, and championing reform bills that rein in government surveillance. Globally, we work with advocates and partners to create a global digital environment that upholds human rights.

Last year a nine-judge bench of the Supreme Court of India, in the case of Justice Puttaswamy v. Union of India1 declared that citizens were entitled to a fundamental right to privacy. The lead judgment called upon the government to create a robust data protection regime balancing individual interests and legitimate concerns of the state.2 In the wake of the judgment, this Committee of Experts headed by Justice Srikrishna has released a white paper soliciting comments on more than 200 questions covering a wide-range of critical issues related to governing and protecting citizens personal data.3

Please find enclosed our submission to the white paper. We have limited our response to the Committee's provisional view for incorporating a so-called “Right to Be Forgotten” within the data protection framework for India. Our submission builds on existing bodies of knowledge on the “right to be forgotten”, both in and outside of Europe. In particular we have referenced the work of Article 19, Centre for International Media Assistance (CIMA), Stanford Law School Center for Internet and Society, Berkman Klein Centre for Internet and Society, Reuters Digital News, and Oxford Internet Institute.

Our submission is divided in three parts. In the first part, we outline some of the unintended consequences of establishing the “right to be forgotten”, including a content removal obligation for intermediaries in relation to personal information. In outlining our concerns on the so-called right to be forgotten, we touch upon issues analysed in other sections of the white paper such as the balancing freedom of expression and privacy, entities involved in the processing of data, scope and exemptions for obligations related to the processing of personal data. In the second

part, we summarise our concerns and recommendations on introducing a right to be forgotten within data protection regime in India. The third part of our submission addresses the questions posed by the Srikrishna Committee on the right to be forgotten.

Part I: Substantive Concerns and Procedural Issues

Protecting privacy online is a vital part of preserving in a digital environment the rights and liberties that individuals deserve and expect in the offline world. However, in updating laws and jurisprudence for a new era, we should tread cautiously when seeking to protect one right and ensure that we do not excessively interfere with other, equal rights. While acknowledging and strongly supporting robust and flexible privacy oversight on the Internet and in other digital arenas, our focus here is on the unintended consequences of adopting a provision that seeks to create an entirely novel additional right, exclusive to the digital world: the so-called “right to be forgotten”.

This so-called right has not been expressly recognized in international human rights instruments, nor in national constitutions. Its scope remains murky, meaning different things in different contexts and jurisdictions. While most commonly seen as a part of data protection, its spirit draws more on laws regarding defamation and honor.

In an attempt to address concerns regarding the spread of untruthful or outdated information online, lawmakers and judges have attempted to graft their idea of remediating these problems onto privacy legislation, with very mixed results, and unclear goals.

The so-called right to be forgotten has been interpreted, most notably by the European Court of Justice, to allow individuals to request search engines to remove links from the search results.4 This has been seen as an extension of the data protection principle of the right of erasure (also known as cancellation or opposition),5 a component of data protection legislation that allows individuals to request to delete their personal data stored by companies when the user decides to stop using that service, or when they believe it to be inaccurate or outdated.

The right of erasure was not developed to be applied over online content, but rather was intended to grant user control over their own personal information collected and stored in proprietary databases.

The de-indexing provided for under the ECJ's "right to be forgotten" has been slowly broadened to cover issues unrelated to personal data. For example, in 2015, the Mexican Data Protection authority initiated a sanctioning process against Google Mexico because a Mexican citizen was not able to exercise his “right of cancellation and opposition to the processing of his personal data."6 The case was initiated by a businessman who had asked Google Mexico to remove various search results related to his name. A Mexican Appellate court annulled an order from the Mexican Data Protection Authority (INAI) requesting Google Mexico to remove a link to a journalistic note about acts of corruption.

Elsewhere,the concept of the "right to be forgotten" has been expanded to include orders aimed at

newspapers, blogs and journalists, requiring them to remove content instead of simply de-indexing it from search engines.7 For example, a Peruvian, Miguel Arévalo Ramírez filed complaints against journalists and media for reporting on the investigations on charges of drug trafficking carried out by law enforcement. The court has ordered an online newspaper, Ojo Publico to "remove, delete and exclude personal data related to 'Miguel Arévalo Ramírez' or 'Miguel Arévalo' to de-index sites, links and pages captured by www.ojo-publico.com, which was considered a database; and implement necessary procedures that make future access to his personal data impossible... ".8 The court limited the availability of "his image" from the Internet, in other words, it has ordered publication to remove the news that reported investigations carried out against him by the Peruvian Police Department's Anti-Drug Directorate (Dirandro), the Peruvian Anti-Drug Prosecutor's Office and the U.S. Drug Enforcement Administration (DEA).9

This Committee has called for an approach to right to be forgotten that balances the right to freedom of speech and expression with the right to privacy. The white paper has correctly recognized that the issue at hand is to what extent can any right to be forgotten be compatible with the right to freedom of speech and expression. Consequently, it recommends that sectoral guidelines for implementing and enforcing the right should be developed in accordance with the data controller's capability to undertake this balancing exercise.

While all parts of the data protection framework should be considered in the light of their effect on other rights, the proposal to include the amorphous right to be forgotten within a data protection framework is troubling. It places strong privacy protections and free expression in direct, and unnecessary, conflict. It also challenges several other basic principles of an open society, including due process, the role of private actors in public policy, press freedom, transparency, the duty of society to preserve debate for its citizens, protection of the integrity of archives and history for its descendants.

Adjudication of Fundamental Rights by Private Intermediaries

Although the Internet is viewed as a global public resource, its functioning and access to information remains predominantly controlled by private actors.

The so-called right to be forgotten, as created by the European Court of Justice's interpretation seeks to create obligations for intermediaries to remove links to content that is lawful and available in the public domain. This right expands the power of private intermediaries, making them the arbitrator of relevance and legitimacy of online information including, if information being available has public interest.

As experts have noted, the risk that lawful speech will be suppressed through cautious overcompliance is increased when an intermediary rather than the speaker herself decides how to interpret unclear regulation.10 In the absence of rules and criteria under which intermediaries may deny requests, there are clear incentives for them to remove or erase information in order to avoid penalties or litigation. The right to be forgotten creates an opaque, unaccountable censorship regime that curbs journalism and free speech. It introduces obligations for a specific class of intermediary/ies whose decision to delink results or erase content will become the de-facto rules for defining the contours of online speech and expression. Neither the Puttaswamy judgment nor the white paper have addressed these concerns of censorship and private ordering of

information that the a broad “right to be forgotten” raises.

Effects on Press Freedom and Historic Integrity

In its report released earlier this year, the Centre for International Media Assistance has pointed out that, "new rationales for censorship are being developed in the digital age, and the RTBF (right to be forgotten) is one of the principal legal tools being adopted by those who seek to control information, which is why it poses a significant challenge to press freedom."11 Journalism is built on a network of links, references, and sources and therefore, introducing the so-called right to be forgotten has major implications for journalists and media freedom. In the UK, following the implementation of a procedure for processing right to be forgotten requests, the Guardian and BBC noticed 'wrongful' deletion of links to news article on their sites.12

A public outcry led Google to restore some of the news items. It is unclear if the search engine will take similar action for wrongful removal of articles for smaller media, bloggers or national and regional dailies like Dainik Bhaskar and Amar Ujala. The BBC has created a continually updated list of articles delisted by Google.13 The framework of a prospective right to be forgotten will need to account for such transparency efforts.

By creating a right to alter lawful information that is in the public domain, the right has created tension between between the “the right to know” on the one hand, and personal privacy and what should be considered public record or “the right to inform”.14

The so-called right to be forgotten also impacts historical integrity of published works as information about a private individual could have public interest or become relevant in the future.

The public domain requires transparency, accountability, and the ability to reevaluate information as its relevance potentially changes due to evolving circumstances or new ways to interpret data —for example, if an investigation about misuse of taxpayer funds by an elected official is reopened due to the revelation of new evidence.15 Indeed, determining what information is relevant and who has the power to determine its relevance over time is central to press freedom and democracy.16

In creating a right to be forgotten in Google Spain, the Court drew a clear distinction between truthfulness and relevance. Relevance is used to express news worthiness with respect to passage of time. However, relevance is not just a temporal value. For example, as the Amsterdam Court of Appeal noted in its ruling, negative publicity caused by criminal offense may be relevant information even if time elapses.17 The second important distinction that the judgment makes is in distinguishing ease of search and setting the standard that the original news article does not need to be unpublished from the newspapers website.

The Centre for International Media Assistance documented that not only archives under threat, but the right to be forgotten also has the insidious effect of empowering governments with the ability to de-index information from public scrutiny and censor content.18 Since the ruling was

upheld, examples of the right impeding media freedom have emerged as courts in Italy19 and Belgium20 have ordered news media archives to be altered.

In Colombia, the highest Constitutional Court refused to recognize a European-style "*right to be forgotten*." In a legal action against El Tiempo, the main newspaper in the country, a Colombian citizen argued that her right to a good name and privacy were violated in the publication and subsequent indexing by Google of a newspaper article in which El Tiempo said that she participated in an alleged crime for which she was never convicted. Seeking to balance the right to clarify the record and the right to freedom of expression, the court held that the newspaper was not required to remove the article. Regrettably, the court did require the newspaper to update the published information and use "robots.txt" and "metatags" to prevent the indexing of the content by Google.21

The right to be forgotten legislation can become censorship tool in the hands of powerful individuals and groups who will use the right to takedown content, public images, and news reports. The possibility of misuse of the right is high given the propensity of politicians, public officials, public figures and celebrities to exert autonomy rights to control information by limiting what is publicly accessible to both citizens and journalists. Last year, Rajya Sabha member Rajeev Chandrasekhar obtained an ad interim ex parte injunction against the Wire22 for pointing out his conflicts of interest in his ownership of national media.23

The conflict between the right to be forgotten and press freedom has also played out in Mexico. 24Mexico's right to be forgotten is largely dictated by the Federal Personal Data Protection Processed by Private Entities Act,25 which came into force in 2011. Section IV creates the right to cancel and erase the processing of personal data and Section V establishes the right to oppose data processing and storage. In 2014, a Mexican transportation mogul, Carlos Sánchez de la Peña, wanted links to an article published by by Fortuna Magazine in 2007 with negative comments about his family's business dealings and the government's bailout of bad loans removed from Google Mexico.

In response, National Institute for the Access to Information (INAI) ruled, "The request met the privacy law requirements that allow for the removal of information when 'persistence causes injury' even if the original articles were lawfully published. While privacy law in Mexico contains exceptions if the information is in the public interest, these exceptions were not applied in the judgment. The decision required that Google remove the results on its national site for Mexico."26

The Mexican human rights organization R3D appealed and the case came up before Appellate Court. Two years after INAI had passed its resolution , the circuit court repealed the decision.27

Even though the repeal set an important precedent for press freedom in general, the decision will likely be appealed to a higher court. It seems inevitable that the right to be forgotten will continue to be used as a tool by powerful Mexicans to control information—further eroding press freedom and access to objective, high-quality information.

"Unpublishing" news has impact on media freedom, historical integrity and the accountability in

journalism. Online technologies have not only expanded the range of information we have access to, but have also made it easy to access and store information for long durations.

Recognising these conflicts with privacy rights, the white paper argues for creating an exception in any data protection law for journalistic purposes. However the chapter outlining exemptions does not offer much clarity on the definition of "news", "journalistic purpose" or a "journalist". Legal scholars have objected to terming journalistic activities as an exemption on the grounds that it gives the impression that fundamental rights to freedom are going to be an exception to the fundamental right to privacy.

These are serious steps in media control to take, and should not be considered exclusively within the space of data protection and privacy. The chilling effect of the right to be forgotten on the right to report and media freedom needs a wider debate beyond the data protection consultation.

Protections for Expression Beyond Defined Categories

The white paper refers to the exemptions to the right to privacy crafted under the EU's General Data Protection Regulations (GDPR), which comes into effect later this year brings and brings an enhanced right to be forgotten to Europe.28 The GDPR lists "the processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression."29 Daphne Keller from Stanford Law School has pointed out that while European Union Member States are specifically required to create exemptions for these categories of speech, legal protections are less clear for expression that does not fall in one of these categories.30

In the absence of clearly defined basis for denying requests private intermediaries may struggle to interpret the law. However defining categories of legal speech is problematic. Neither Puttaswamy nor the white paper address the need to provide protection for diverse forms of speech and information create exemptions for processing of certain categories of data.

Privacy and Knowledge

Human rights organizations have always maintained a legitimate claim for greater access to information about serious violations of human rights committed by previous governments and military regimes. The population wants the truth and reconciliation: they want to remember and not forget.31 In this regard, it is important to recognize how a legal mechanism such as the so-called "right to forget" and its incentive for “de-indexing” can affect the right to truth, memory and reconciliation.

The act of seeking search engines to de-index links also affects the "forgetting" of other individuals—those who are involved in the same event and yet do not want to be forgotten. It also impacts those who may be involved in the future or interested in similar events.32 The idea that, it is the individual who should retain ultimate control over information, ignores the broader right of the public to share and receive material that is legitimately in the public domain.33

Transparency Under Censorship

The takedown procedure that is developing in the application of right to be forgotten has serious implications for transparency under censorship.34 Since 2002, Google's established a policy of informing users when content is missing from search engine results and has posted a message at the bottom of each search page. Google has also passed on original legal order to Chilling Effects. 35

Under Google's implementation of the right to be forgotten, the company places generic warnings at the bottom of searches that have no connection to deleted content. Moreover, Google is now placing a generic warning at the bottom of *any* European search based on what its algorithms think "real names" look like.36As EFF has pointed out during Google Plus's Real Names fiasco, Google's determinations of individual names are notoriously inaccurate.37

In 2014, Google's Advisory Council in its recommendations on right to be forgotten raised the importance of transparency. The final report recognized four related but distinguished aspects on the issue of transparency concerns:

- transparency toward the public about the completeness of a name search;
- transparency toward the public about individual decisions;
- transparency toward the public about anonymised statistics and general policy of the search engine; and
- transparency toward a data subject about reasons for denying his or her request.

In 2015, 80 academics from around the world wrote to Google demanding more transparency about its processes.38 The academics sought the release of anonymised and aggregated statistics as well as the process and criteria used in delisting decisions.

Under the GDPR's requirements for responding to right to erasure requests, an online service provider must inform other processors of the request, and must inform the data subject when it erases information or takes action based on request. As Daphne Keller has pointed out these requirements can lead to perverse outcomes.39 Sharing more precise or granular information about delisting standards in difficult cases might risk disclosing personal information about the data subject, bringing both legal penalties and public opprobrium to the company.40

Data protection authorities have also clashed with Google on transparency of right to be forgotten requests. The Spanish DPA has fined Google for notifying publisher about the delisting holding that notifying the publisher of the removal of content violates the duty of secrecy set forth in the Data Protection Act.41 Google has appealed the decision.

Transparency and censorship online are at odds, especially when censorship is intended to make more obscure publicly available data. It is difficult, and may be impossible, to maintain appropriate levels of public oversight and political control, when intermediaries are required to hide from sight the content of information that they de-link or “forget”.

Procedural Issues

In the above section we have laid down the issues arising from interpretation of the scope and enforcement of the right. Procedural rules related to content removal are separate from the issues arising from interpretation of the rights in the legislation. The notice and takedown procedures for intermediary liability and copyright infringements include legal procedures for appealing removal of content and a right to be heard. On the other hand, the takedown procedures for right to be forgotten favors right to removal over the right to be heard, or juridical review.

The procedure for removing information under right to be forgotten, relies on data controllers to review the legitimacy of claims, and offers no criteria for granting or rejecting requests. The takedown procedure being developed in Europe does not include a right to appeal to the decisions taken by the intermediary. There is also no procedure or mechanism outlined for the public or the publisher to seek reinstatement of content, and it is the sole right of the data controller to restore content.

When making requests for removal, the GDPR does not specify what information should be included in requests made by the data subject. As the Manila Principles, a set of global principles outlining best practices for content removal recommends, notices for content restriction must be clear, unambiguous and follow due process to prevent abuse of removal mechanisms.42

Under the GDPR, the online service provider can also temporarily suspend or restrict content as soon as it has received the request. The obligation to restrict comes into play before the controller has had a chance to judge the legality of the claim or determine its legitimacy based on balancing other right to privacy and freedom of expression. Immediate, unsubstantiated restrictions on content deprives users of lawful content. The implications of such broad censorship are particularly significant during national, local or regional events such as public emergencies, elections or court hearings.

In Indonesia, the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions took effect on 25 November 2016 created a right to be forgotten.43 The regulations are broad and apply to electronic service providers (ESP) which includes "any person, state administrator, business entity, and society that provides, manages, and/or operates an electronic system."44 The Amendment creates the right for a relevant person to request that an ESP delete any 'irrelevant' electronic information or documents under the ESP's control. However, the law does not specify how or under which circumstances electronic information or documents will be deemed as 'irrelevant', nor who will be considered a 'relevant person' entitled to request deletion of such information or documents. While the requests have to be based on a court order, ESPs are required to have a deletion mechanism in place to deal with such requests.

In July 2014, members of the Israeli Parliament introduced a new bill seeking to amend the Protection of Privacy Law to enact the "Right to be Forgotten"45The Bill establishes a right for "any individual who believes he or she has been harmed by the publication of personal information on the Internet." Under the takedown procedure an applicant may submit a request to the operator of the search engine. If the search engine declines the request or does not respond the Bill establishes a right to appeal, whereby the applicant can approach the court and seek an order for removal.

In considering requests for removal of personal information, courts need to balance the degree of harm an individual has suffered or may suffer against the public harm from the removal of information. In addition the court must also take into account the identity of the individual, his or her character, and the sensitivity of the information are also criterias for the court's consideration. While Google has the right to reject requests, the Bill does not include a right to be heard or mandatory notice for the publisher of the content.

Most recently, Canada has proposed a system for processing right to be forgotten requests where rather than de-indexing a link, search engines might instead be asked to lower the rank of a search result or flag the result as inaccurate or incomplete. While algorithmic decision-making is far from neutral and deserves greater scrutiny, using privacy law to justify intentionally obscuring results by lowering ranks transforms information intermediaries into knowledgeable publishers.46 As Micheal Geist has pointed out, the approach features a remarkable level of micro-managing of search engine activity and would vest vast editorial power in search engines.47 The takedown procedure in Canada has also include recommendations on limiting access including calling on search engines to use geo-identifying technologies once revised search results have been developed.

Any framework for de-listing or de-indexing of personal information should include substantive and procedural safeguards. The implementation of the right within EU and in other parts of the world has been varied and in most cases have included broad, ambiguous criteria.

Well-crafted processes are important to prevent censorship of content that falls outside of the scope of the legislated right. Including procedures for appeal and reinstating content that has been removed are essential to prevent lawful content from being unfairly targeted and removed from the Internet.

Any legislation that places obligations on intermediaries needs to take into account the broad and evolving Internet ecosystem: not just the large and well-resourced companies but also smaller intermediaries. The law should not incorporate any assumptions that all intermediaries will put effort into avoiding over-removal, or even that the ones doing it now will be able to play that role forever.48

Part II: Recommendations on the Right To Be Forgotten

EFF does not support nor recommend the recognition of a "right to be forgotten", in which online media must de-link or remove references to existing public resources, in the Data Protection framework in India. We are of the view that legislating such a right is not the correct way to secure individual control over personal information. Drawing on the conclusions of Article 19, and the Manila Principles, we instead suggest that:

1. Existing remedies should be pursued such as those offered by privacy and defamation laws, and remedies under the terms and conditions of intermediaries, instead of recognising the right to be forgotten.

2. Any process that seeks to remove or limit information already in the public sphere should be strictly limited, as certain minimum requirements must be met for such a right to be compatible with the right to freedom of expression, both in terms of substance and procedure.

3. Such regulations should also make explicit reference to the right to freedom of expression as a fundamental right with which such protections must be balanced. They should also specify criteria and test for making these determinations based on existing jurisprudence.

4. Platforms that decline to remove content because they honestly believe in its public interest value should face minimal or no financial penalties, in order to prevent perverse incentives to over delete.

5. Historical integrity and accountability require that public information should be kept public. The law should err on the side of maintaining a permanent, open record of the past, including errors.

6. Procedural safeguards such as specifying details to be included in requests, seeking identity for data subject to prove their identity, creating mechanisms for appealing requests should be included.

7. Transparency criteria for data controllers including their obligation to inform the original publisher of information should be clarified.

8. If publicly available content is removed, a mechanism to reinstate content that has been wrongfully removed, is contested, under judicial review should also be considered to balance the takedown procedure which favors deletion in its current form.

Part III: Response to Questions

What are your views on the right to be forgotten having a place in India's data protection law?

EFF does not support nor recommend the recognition of a “right to be forgotten” in the Data Protection framework in India. We are of the view that legislating such a right is not the correct way to secure individual control over personal information placed into the public sphere. The so-called “right to be forgotten” should not be considered to be an unspoken or natural part of data protection principles. Regulation on the right to be forgotten cannot simply be read into data protection regime, but rather should require careful review and legislative reforms by Parliament.

Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

Data Protection has historically applied to back-end processing such as stored hospital records or Internet user logs. It has rarely needed to consider issues about speech and expression. Rather than attempt to separate these two spheres by considering the method by which the data was divulged, we recommend concentrating privacy legislation on more targeted and narrow “right of erasure”, which delineates user rights over data not used for purposes of expression.

Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

We believe that the protections potentially provided by laws, and judicial interpretations that create a separate “right to be forgotten” are better considered in defamation and comparable law, not privacy law.

Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller‘s possession?

The “right to be forgotten”, as attached to data protection law, emerged as a limited right that applied to search engines removing data from "list of results displayed following a search made on the basis of the person's name"49 The right evolved in the very narrow context of creating obscurity for information rather than making it unavailable from the Internet. As we have shown, it has been since adapted in multiple contexts, with very different interpretations elsewhere. Given the nascent stage that development of the right to be forgotten is at globally, we recommend that India not include such a right in its data protection framework.

Whether a case-to-case balancing of the data subject‘s rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise?

Decisions involving complex factual and legal balancing exercises, involving both the right to freedom of expression and the right to privacy, should only be made by a court or independent adjudicatory, not a private service provider. Only courts or independent adjudicatory bodies should decide whether “right to be forgotten” requests should be upheld.

If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority

or courts?

We do not recommend imposing heavy penalties for denial or failure to respond to right to be forgotten requests. As evident in the copyright and intermediary liability regime in India, heavy-handed penalties coupled with ambiguity in law create the incentive for intermediaries to process all requests and take down content in order to avoid fines. It is more appropriate to encourage a system of self-regulation for intermediaries.

Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

The relationship between the right to freedom of expression and the right to privacy is complex. Both fundamental rights are mutually reinforcing but occasionally conflict. Right to privacy is essential in order to exercise freedom of expression: however the publication of private information can represent an infringement of the right to privacy. These conflicts can be especially difficult to manage when the information at issue is both personal and public.

Such conflicts are better addressed by separate regulation that equally considers both free expression and privacy. Merging the multiple concerns embodied in a "right to be forgotten" into data protection or privacy law risks unbalanced enforcement.

Therefore, we recommend that India should not legislate a right to be forgotten.