LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +919310053923 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

# LINKING SOCIAL MEDIA PROFILE WITH AADHAAR – A WAY OF INKING THE CYBER EXISTENCE *

## ABSTRACT

*"I just miss – I miss being anonymous"*

- *Barack Obama*

*Cyber-crimes are well served in an anonymous world, so does the present scenario goes hand in hand with this assertion. Perpetrators hide behind the screen, and with technologically advanced knowledge, the law enforcement agencies find it hard to keep up with them. Not to mention country mediated cyber warfares, which are on the rise. It is this notion that could've spurred the Tamil Nadu State government to garner the linking of social media Profile with the Aadhaar Id.*

*In 2018, the social media platforms like facebook and facebook owned whatsapp were directed by the state of Tamil Nadu, albeit being opposed by them, not serious repercussions surfaced from the public. Prima facie, question arises as to the authority of the government to take such measure. Other Pertinent questions here would be why the government would want to take this drastic measure amidst the privacy arguments. If so necessary, why was aadhar ID the 'chosen one' from all other types of IDs. This paper would delve on the above raised questioned having regard to the necessity of cyber security.*

## INTRODUCTION

**I**nternet is considered to be the world wide electronic computer operated network that connects people and information. It has brought people closer, and its contribution to collective is growth of the community is undeniable. But this communication like any other communication requiring a media, requires the aid of the 'social media'. Social media is the latest form of media available to all classes of people. It is pertinent to note here that this popularity finds its roots to the reason that the users are given free service to create a virtual social world where they exchange information *inter alia*. Most importantly the anonymity of the users are safe kept. This is one of the main reasons for social media being the safe house for the cyber criminals. Therefore, this anonymity and jurisdictional issues have marked the rise of cyber-crime in India.

**'Inking' the Cyber Existence**

As the title of the paper itself suggests that linking of social media Profile with aadhar is pre-mediated for 'inking the cyber existence' i.e. determining distinctly the data flow in the cyber world. This is very important for the law enforcement agencies to curb various forms of cyber-crimes.

**The Problem**

The SC itself has said that there is a need to find a balance between the right to online privacy and the right of the state to trace the cyber wrong doer.[1] Fundamentally, it boils down to the issue of cyber security and data privacy of the Indian citizens. Further, the social media platforms have felt that linking would violate the users' privacy policy. It is also pertinent to note here the feasibility of the cyber security afforded against accounts from outside India. It is also pertinent to note why that aadhar has to be linked to social media account. A global perspective on this issue would be imperative for the present discussion. Linking aadhar ID will have to be analysed keeping the vires of the Aadhar Act

**Social Media and its Vibrant Users**

Facebook and whatsapp are two of the most popular social media which provides its users a platform to express themselves without any restrictions. This unfettered usage entails a major challenge as it involves infringement of various fundamental rights of individuals or groups, or other rights of interested individuals or groups. So, it would not be wrong to say that the anonymity in social media is not attractive as it may seem to be considering the rise of cyber-crimes in social media.

**Questions to Ponder Over**

Whilst it is necessary to determine the cyber-crimes perpetrated through social media, it would be vain if it is not determined whether or not linking aadhar ID is the only way to trace the wrong doer. Before that it would be to understand the authority of the state to impose such rule given the lack of any express enabling provision under the Aadhar Act, or under any other in law in force. As to the defences raised by the social media platforms, it would be pertinent to determine whether they have locus standi to defend or rather speak for its users, when the welfare of its users to be given primacy by the state. Consequently, with emphasis from the Hon'ble SC, it would be pertinent to bring a balance between cyber security and data privacy, and which would have precedence over the other in case of conflict.

The instigation behind the present research paper roots to the PILs being filed at various HCs and SC seeking direction to the government to ascertain the feasibility of linking Aadhar with social



* Ashwin Bala Someshwerar, Student, Tamil Nadu National Law University, Tiruchirappalli.

[1] Sankat Vijayasrathy, "Aadhaar-Social media Linking: 10 things to know about the ongoing issue" *India Today,* Aug. 23 2019.

media accounts, including facebook, twitter and web news portals, in order to curb fake news. The reasons for such an extreme measure are due to the rise of hate content, fake news and cyberbullying. The researcher would be delving into the procedural back ground of the issue and would try to answer the question put before the Hon'ble Supreme Court of India.

## THE DISPUTE BEFORE THE COURTS

*"I was like how can something like this happen, and people can get away with it?"*

- *Antony Clement Rubin*[2]

### Prologue

There are several PILs filed at various High Courts across India seeking direction to make it mandatory to link aadhaar or any other government ID for authenticating social media user profiles. The first of its kind was by an animal activist Antony Clement Rubin. He was also subject to cyber bullying during the jallikattu protests. His efforts to nab the perpetrator was all in vain when the police, even after a direction from the Hon'ble High Court of Judicature at Madras, said it could not catch the cyber bully citing reasons of inadequate details with facebook. Subsequently, the case was closed.

Rubin's primary concern was there are victims in cyber space subject to cyber-crimes. When the perpetrator's content is removed, it's just water under the bridge, nobody ever cares about the injustice being done to the victim. Therefore, he filed a PIL[3] in 2018 along with another petition[4] seeking direction to give effect to the prayer in the PIL.

### Madras HC's Take on the Issue

Albeit, the Hon'ble HC made a passing reference, reiterating the Supreme Court[5] that aadhaar card being a government accord used only for social welfare schemes. But it didn't stop here; the scope of the PIL was widened to include curbing cyber-crimes and intermediary liability protection. It was also emphasised that the government should notify the amendments to the IT Rules which enforce traceability on intermediaries.



### The Stand of the Government

The main objectives of the government's argument that Social media profiles should be linked to are, as follows;

(i) identify terrorist messages,

(ii) Preventing proliferation pornography or obscene contents, and

---

[2] An animal activist since 2000; He was part of the Jallikattu Monitoring Committee in January 2017.
[3] *Antony Clement Rubin v. Union of India,* vide WP No. 20774/2018.
[4] *Janani Krishnamurthy v. State of Tamil Nadu,* vide WP No. 20214/2018.
[5] *Justice K.S.Puttaswamy v. Union of India,* (2016) SCC 1.

(iii) To prevent spreading of fake news.

The state also enlightened the court on various steps being taken to curb this menace, for instance it is finding a solution to trace down whatsapp messages with the aid of Professors from Indian Institute of Technology.

The government seem to be in bliss with regard to its authority to link aadhaar ID with social media. It has been time and again reiterated by UIDAI that the Aadhaar Act only provides for welfare schemes. And is use has been extended for income tax purposes after an amendment to the Act. It cannot be whimsically accorded the access to such details which will be against the view of the Highest court of the country.[6]

**The Stand of Social Media**

*Prima facie,* facebook, the primary social media involved herein, sought for transfer of cases to the Supreme Court stating that the petitions pendent lite before various high courts involve common question of law that is whether private entities can have access to aadhaar numbers of individual users. It stated that such transfer would prevent conflicting opinions on same question of law, given the pan India operation of social media.

Facebook contended that if it had verify with aadhar, it would violate its user privacy policy. It also stated that the government cannot share such sensitive information to a private entity. The pertinent question here is, when larger public interest is involved, does the facebook's argument hold water? This stand seems to quivering given the consequence of linking government ID, which will increase the surveillance, which in turn will reduce the number of social media users. This view cannot be totally disregarded as it could be the motive, even after so much governmental pressure.

**The Promulgation of Ordinance**

Before the promulgation, the Aadhaar Act authorized to access for establishing the identity of an individual, by the State or a body corporate under any law. But this provision removed to give effect to any entity may be allowed to perform authentication through Aadhaar, if the UIDAI is satisfied that it is: (i) compliant with certain standards of privacy and security, or (ii) permitted by law, or (iii) seeking authentication for a purpose specified by the central government in the interest of the State.[7]

---

[6] Surabhi Agarval "New law needed for Aadhaar-Social Media Linkage" *The Economic Times* September 25, 2019 *available at* https://economictimes.indiatimes.com/news/politics-and-nation/new-law-needed-for-aadhaar-social-media-linkage-uidai/articleshow/71285787.cms

[7] The Aadhaar and other Laws (Amendment) Ordinance, 2019 *available at* https://www.prsindia.org/billtrack/aadhaar-and-other-laws-amendment-ordinance-2019

## THE CASE OF AADHAAR CARD BEING USED AS THE 'TRUMP CARD'

Before even going into the substantive arguments in favor and against, it is pertinent to note the prayers of before the Madras High Court. Linking may done with the help of not only aadhaar card but also any other government related ID card. Further, it was also prayed that a committee maybe formed to handle these cyber-crimes with specialized task force. Therefore, the central issue here is some form of authentication to trace down erring user profile. The veracity with which the said concern should be taken into consideration with regard to aadhaar card has to reduced, otherwise it will render the substance of the issue to nullity.

It is pertinent to understand the argument that the intention behind linking is just to prevent the spreading of fake news in social media, and he opines that linking Indian people's Aadhaar with social media is not a panacea for the fake news plague. It was also pointed that how linking would curb this menace from offshore social media accounts. Fake news can be curbed on social media by taking other suitable measures. Most importantly, the concept of linking goes against the fundamentals of Indian cyber law i.e. all Indian data must be kept within the country, there could severe ramifications on national security in case of data breach.[8]

## CYBER SECURITY VERSUS PRIVACY

### The Flaw with Cyber Security

The threat to privacy is has many intervening aspects. One of the crucial and most mooted aspect is placing an individual under surveillance. The assertion whilst no harm can be envisaged on the individuals concerned, it should be understood that such information being put to use furthers the ubiquitous nature of such information i.e., the information put use for one purpose can be used for another purpose. This is very crucial in determining the balace between cyber security and privacy. Further, any attempt to strike a balance between compeing interests in a dynamic environment would only open the flood gates of previously settled positions. As it may be attractive to agree that data can constitute an extremely valuable investigative tool but the whole premise of data protection legislation over the decades has been that the potential for misuse is considerable.[9]



Though the context in which the above argument made is not social media, it is undeniable that the premise on which assertion is put forth is that balancing the interest of the state to surveillance its citizens whereas the citizens are sceptical about the necessity of such surveillance, which would open flood gates of violation of online privacy.

[8] Editorial, "View: Aadhaar Linkage with Social Media is troublesome" *Economic Times,* Aug. 27 2019.
[9] Ian J. Lloyd, *Information Technology Law* (Oxford University Press, UK, 7th edn., 2014).

It is obvious that whilst law enforcement agencies requires sharing of data, it raises concerns for civil liberties. It is pertinent to note that over the years scholars have deliberated on the risks associated with privacy and freedom arising from such data sharing. However the literature in this regard is only to the extent of its implications.

The interplay between private and public uses of the same data has important implications for social welfare. It is a matter of significance – the growing role of private firms play in facilitating governmental access to data, analyzed the incentives of private companies to collaborate with governmental surveillance, and explored the implications of such data sharing for civil liberties.[10]

**Privacy – Primacy?**

The privacy question involved in the constitutionality of the internet surveillance in India finds its place in those situation where the policy preference chooses between the collective security interest and liberties of the individual. It is susceptible the argument that the collective interest is mere abstraction when view in comparison with the real, tangible harms that accompany a restriction, however, minor and reasonable, of an individual's right.[11]

It would be useful to get cue from this argument on privacy, making any surveillance policy of the government subservient to individual's privacy. It should be understood here that a non-fail safe system would be imperative i.e. it should not be easy for the perpetrator who has knowledge of network security to blend in or spoof his identity to match another person's.

**Resolving the Conflict in a Conventional Way**

The discussion about balancing public interest and security with privacy is not something new, and had been mooted extensively in the past. First of all the public interest justification must rationalised and then can we move on to resolve the conflict. It is pertinent to that even in the case of privacy the proportionality test would succeed in giving the best results especially in cases concerning freedom of expression.[12] It was further emphasised that protection of privacy is in itself a substantial component of public interest in most circumstances.

But there are plethora of judgments which says public interest overrides the interest of specific individual whose confidentiality has been breached. Therefore, right to privacy cannot be invoked when the national security or public safety is at stake.

## CYBER SECURITY AND ITS IMPLICATION IN OTHER JURISDICTIONS

### Cyber Security in United States

[10] Niva Elkin-Koren and Michal S. Gal, "The Chilling Effect of Governance-by-Data on Data Markets" 86 *University of Chicago Law Review* 403 (2019).

[11] Anirugh Rastogi, *Cyber Law – Law of Information Technology and Internet* (Lexis Nexis, 1st edn., 2014).

[12] Rishika Taneja and Sidhant Kumar, *Privacy Law – Principles, Injunctions and Compensation* (Eastern Book Company, Lucknow, 1st edn., 2014)

In the US context, where the privacy laws are stringent and most proactively enforced, the question of governmental surveillance is susceptible blatant violation of Fourth Amendment, which provides for prohibition on unreasonable searches. But it is pertinent to note it does not afford protection to data already exposed to public or voluntary dissemination.
There are proposals for affording fourth-party developers for creating surveillance software for the government. These parties will be given access similar to that of other commercial developers (social media), so that their interests are aligned with the law enforcement agencies and at the same time it would be easy to impose liability, and thus protect people from harm.[13]

Therefore, it would be imperative to analyze whether there is any positive duty imposed on the state to restrain itself from interfering with anonymity of the user when the data is exposed to third party, or in public.

**Singapore's Fake News Act vis-à-vis IT Act**

By executing POFMA, Singapore has exhibited a determination to battle the developing spread of false news and deception crusades. There are various significant takeaways for India from this analysis. Right off the bat, there is a need to recognize the job of Social media and other ICT corporations as significant stakeholders in guaranteeing national security, and their aptitude and range of abilities should be ideally used for the equivalent. Furthermore, sufficient arrangements exist in the IT (Amendment) Act 2008 for observing and blocking web services. A proactive methodology with the assistance of ICT corporations can help in distinguishing messages and posts which are becoming a web sensation and further examination of these can help with isolating messages that are probably going to bring about the responsibility of unlawful acts. Limiting the number of forwards has been a significant advance toward this path as it helps in hindering message proliferation. Thirdly, cyber knowledge of our populace in recognizing and settling on considered choices as for false proclamations will lessen the intrigue and spread of such messages. Fourthly, all messages which are being initiated and proliferated on the web should be particularly recognized and followed with the goal that the anonymity of the message originator, beneficiary and propagator can be evacuated and this would thus prompt an increasingly dependable user behavior. Fifthly, prompt and exemplary actions should be made against people and associations falling back on the spread of false messages both inside and outside the nation. Ultimately, community oriented and cooperative association should be fashioned with likeminded nations to recognize the origin of falsehood and starting counter measures against the perpetrators.

[13] Christopher L. Izant, "Equal access to public communications data for social media surveillance software" 31 *Harvard Journal of Law & Technology* 238 (2017).

**Myanmar and its Digital Divide**

The government led by Suu Kyi's NLD walks a fine line, grappling with this new digital world, pondering how to fight online hate speech against Muslims without antagonizing the Buddhist majority, organize electronic services, and police the cyberspace democratically. In this new, more open era for Myanmar, regression is just as possible as progress while old laws remain and the military retains significant control of the legislature, the executive, and key economic sectors.

With the new digital media deeply embedded in Myanmar's culture and society, there will never be a way to completely return to an older system, but media suppression in various forms remains deeply entrenched after a history of censorship, surveillance, and suspicion. Progress on these fronts will take longer, but will undoubtedly depend on the Internet, strong independent media, and an interconnected, educated online society to truly move beyond this authoritarian historical legacy.[14]

**Data Retention Policy in UK vis-à-vis Aadhaar Linking**

The data protection Act, a legislation spear headed to protect the privacy of individual's vis-à-vis processing their data. Albeit the progressive privacy laws for the Europeans, there is dire need of data retention policy to enhance the law enforcement agency in curbing cyber-crimes and threats to national security.[15]

This would be relevant as the author discusses various human rights aspect to the current discussion. He also brings in the term 'data retention' to indicate the power of law enforcement agencies to avail data for investigation is in nexus with the intention behind the linking of social media accounts with aadhaar.

## INFERENCES & CONCLUSION

It pertinent to note that given the technologically advanced era, the need of cyber savvy judges in this era to fasten the cyber-crime investigation via social media for the ends of justice.[16] The jurisdictional lacunae needs no special mention in this regard. Further, it important to note that loss of evidence being crucial problem in every cyber-crime as all the data are routinely destroyed. And given the non-traceability of perpetrators adds oil to the fire. It would be imperative to determine whether there is any positive duty imposed on the state to restrain itself from interfering with anonymity of the user when the data is exposed to third party, or in public.

---

[14] Tej Parikh, "Social Media Exhibits its Disruptive Power in Myanmar" *The Diplomat* November 9, 2017 *available at* https://thediplomat.com/2017/11/social-media-exhibits-its-disruptive-power-in-myanmar/

[15] Paul Lambart, *The Laws of the Internet* Chapter IV, 441-488 (Bloomsbury, 4th edn., 2015)

[16] *See* Rekha Pahuja, "Impact of Social Networking on Cyber Crimes" 4 *Epitome-International Journal of Multidisciplinary Research* 9 (2018).

Governments around the world are keen on imposing liability on the technology companies to curb cyber wrongs. Nowhere, the idea of linking social media profiles being linked with government issued IDs had been discussed or atleast not in a magnum level. But given the state affairs of law enforcement agencies in India, it is not advisable to shy away from the idea of linking social media profiles with some government IDs. The objective here is to trace down the perpetrator in the social media. And the conception of this idea is only possible only if users understand that social media is not a place to be taken for granted; cyber space is not a place where one does those acts that are not done in the physical space. If at all the India is keen on aadhaar, it is necessary they do it by legislating appropriate laws because the current legal system.