SCC Online Web Edition, Copyright © 2020
Page 1 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

6 CMET (2019) 1

Simple Amendments, Clipped Democracies and No Privacy - Need for Informed Participation

SIMPLE AMENDMENTS, CLIPPED DEMOCRACIES AND NO PRIVACY — NEED FOR INFORMED PARTICIPATION

by

Smriti Kanwar[*]

Abstract

In a technologically interconnected world, participation via electronic means is the norm. Successive Indian governments have praised the Information and Communications Technology (hereinafter 'ICT') revolution and attempted to create a 'Digital India' with e-governance, e-commerce and, a digital existence complementing the real lives of all citizens. While technology adoption is no longer optional and many benefits are attributable to ICT and the Internet, these technologies have also ushered in their own specific challenges. As relatively new adopters of ICT, the government and the users of these technologies in India face a steep learning curve in light of constantly evolving technologies with progressive capabilities and utilities. In particular, there is a real danger of marginalization of citizens' rights and freedoms if they cannot comprehend the nature of the technologies they use and how these technologies interact and have real-life consequences. In December of 2018, the government invited comments on its draft amendments to the 'Intermediaries Guidelines Rules' under the Information Technology Act, 2000. Implementation of these rules does not require Parliamentary passage, but they deal with matters of immense importance to all technology users, citizens, corporate entities, the government itself and India as a democracy.

While Part I of this research paper introduces the proposed amendments and the role of intermediaries in everyday internet and technology use, Part II lays out the impact of all proposed amendments when read together. Part III explores related provisions under International law and what has been the impact of rules and laws of similar nature, historically and in other nations. It also includes partial analysis of local empirical research on how different groups view government tracking and how it will impact their exercise of freedom of speech and expression. Part IV presents some suggestions for a revised as well as, a wider and informed public engagement in light of the involvement of essential and inalienable rights and freedoms.

INTRODUCTION

Make no mistake: The digital age will change the meaning of freedom of expression. The only question is how it will change. If we do not reconsider the basis of liberty in this age, if we do not possess the vigilance of the guide as well as the guard, we shall end up like every person who travels through the wilderness without a compass, or through the forest without the forester. We shall end up lost.[1]

Proposed 2018 Amendments and Invitation of Public Comments

SCC Online Web Edition, Copyright © 2020
Page 2 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

On 24th December, 2018, the Central Government released the draft of the proposed amendments to the Intermediaries Guidelines Rules, 2011 under the Information Technology Act, 2000 (hereinafter 'the Act').[2] Relevant stakeholders were invited to send their comments and suggestions on the proposed amendments aimed primarily at fighting fake news by midnight of 31st January, 2019.

Intermediaries and 'Due Diligence'

Before discussing the proposed amendments, their practical implications and effectiveness in meeting their objectives, it is important to lay down who are 'Intermediaries' under the Act to understand the scope and extent of data and information (personal, commercial, legal and otherwise) which could be impacted by such amendments.

In simple terms, intermediaries are 'entities that provide services enabling the delivery of online content to the end user'.[3] They include Internet Service Providers (hereinafter 'ISPs') who enable internet connections, search engines, web hosts, interactive websites (social media sites, e-commerce or auction sites, payment gateways and blogging platforms among others), Domain Name System (hereinafter 'DNS') providers and even cyber cafes.

Page: 3

Safe Harbour Protection

Section 79 of the Act provides protection to intermediaries from potential liabilities stemming from any legal action initiated based on user-generated content as long as 'due diligence' is exercised while discharging their duties and governmental guidelines on the matter are observed.[4]

Section 79 must be read with Rule 3 of the Intermediaries Guidelines Rules, 2011 that deals with 'due diligence' and is also the subject of the majority of the 2018 proposed amendments. The rule incorporates publication of usage policies, list of potential 'red-flags' and circumstances of sharing information with the government along with other sub-rules.

Overview of Proposed Amendments and Their Impact

The amendments place a burden of extensive 'pro-active' technological use on data and information transmitted via intermediaries. The reaction periods for intermediaries to deal with certain kinds of 'content' has been reduced to 24 hours from 36 hours. Data retention periods have been increased from 90 days to 180 days. The amendments continue to embrace the power of intermediaries to unilaterally and immediately terminate access and use of facilities. They do prescribe a minimum 'once-a-month' notice to the users about such termination upon non-compliance but do not lessen the burden on the users to fight for services that might have been unfairly terminated. The amendments also encourage surveillance capitalism at the cost of freedom and rights of citizens.

In times of increased cyber-security and privacy issues, the amendments require denial of or cracking of 'encrypted' services availed of by users across different platforms and areas of lives, leading to an aggregation of data and information that the users may not have consented to the first place. Additionally, a prescription of 'denial of encryption' services undermines cyber-security as well as notions of embracing and adopting technological neutrality and innovation.

PROPOSED AMENDMENTS: READ TOGETHER

SCC Online Web Edition, Copyright © 2020
Page 3 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

Given the widespread ICT adoption, it is no surprise that any change in the Act or its accompanying rules has an impact on the use and utility for users of technology, in the present and the future. The proposed amendments also impact the industrial paradigm. There are questions about the burden of

operation, impact on innovation and respect for ancillary obligations among others. But the primary focus of this paper is on the socio-economic and even, the politico-cultural consequences for individuals and citizenry of a nation.

The proposed amendments have increased data-retention periods, granted unfettered discretion to public servants,[5] and opened-up encrypted communications and confidential communications (commercial and personal) to multiple players in the ICT industry as well as multiple governmental departments.[6] The consequences of such changes are discussed below.

Arbitrary Mass-Surveillance

The proposed amendments cover all forms of information and data, suppressing the freedoms to speech and expression, right to privacy including the right to be forgotten, among others. Further, the requirement of some access or information does not *ipso facto* translate into all available information becoming liable to be accessed or processed.

The amendments enable the creation of a database and inter-linking of data/information within governmental agencies or private entities in the light of increased horizontal integration.

Collision of Digital and Physical Identities

The proposed amendments link a citizen's data with his or her physical identity in light of the government IDs or bio-metric IDs (linked to other databases) required for telecom (internet) connections. Thus, the amendments make available to all concerned intermediaries, such information that an individual may not wish or may not have consented to share with anyone.

Also, ‘big-data analytics’ may place financial, health and, geographical information and data together in a manner not consented to by the users. The amendments compromise privacy (including informational privacy) assured under the Indian constitution without first putting in place appropriate safeguards to ensure enjoyment of the said right in a meaningful manner.

Pro-Active Surveillance on Vague Criteria Resulting in Pre-Censorship & Suppression of Freedom of Speech

The proposed amendments impact Freedom of Speech and Expression along with other freedoms and rights such expression allows. In particular, Rule 3(2)(b) which has been retained from the 2011 Intermediaries Guidelines places a burden on users to not host, display, upload, modify, publish, transmit, update or share that is ‘is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or

SCC Online Web Edition, Copyright © 2020
Page 4 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

otherwise unlawful in any manner whatever'.[7] Non-compliance leads to unilateral termination of services by the intermediaries.[8]

It is clear that many of the qualities listed under Rule 3(2)(b) are highly subjective. The danger of personal communications or even jokes falling within the same is exceptionally high, earning disproportionate penalties for those who use ICT for communications.

Misuse of such provisions is a reality in India, as evidenced by events leading up to *Shreya Singhal* v. *Union of India*[9]. Other nations do not lag behind as evidenced by elaborations in Part III and includes the concept of 'Cyber Scouts', 'Cyber Witch Hunts', '50 cent bloggers' or even 'Human Skinning'.[10]

Pro-Active Scanning

The intermediaries are also obligated to utilitize 'pro-active' technological methods to constantly scan for such information and take action upon the same.

Burden On Intermediaries — Economic Protection of Freedoms

The proposed amendments put an unreasonable burden on the intermediaries themselves to determine the legality of content on their platforms with vague terminology like 'obscenity', 'hateful', 'disparaging' that tend to have subjective connotations and standards of the breach. With the rise of social media and large-scale adoption of electronic communication as the default

Page: 6

mode of communication, the inevitable intersection of freedom and sanctity of private conversations and law(s) pertaining to defamation is a fine line to be walked that cannot be left to the determination of intermediaries.

Absence of Safeguards and Remedies

The proposed amendments cater for excessively broad paradigms of potential requirements of government or its agencies on the basis of ill-defined criteria that are highly subjective,[11] while mandating quick essential compliance without providing for:

- similar quick processes of resolution for the users;
- public disclosure of such requests, use and results of the same;
- legislative oversight;
- accountability on part of the government or its agencies;
- any protection for the civil liberties of the users.

Additionally, even pre-publication censorship must meet judicially and constitutionally limited benchmarks for narrow well defined and legitimate objectives met in the least intrusive manner possible. The amendments do not provide a proportionate and stable aka predictable parameter to be enforced.

Absence of Precautions and Penalties Concerning Pro-Active Scanning

The proposed amendments do not clarify the safeguard proposals pertaining to 'for-profit' and private organizations carrying out technology-assisted proactive surveillance on private communications, including—

- Restriction of present and future data mining in any form on such data access and storage across a field famous for horizontal integration.
- Processes, Procedures and Infrastructure to ensure compliance with point (a)
- Potential technological solutions with reference to point (a)
- Accountability and Transparency Measures from the 'Intermediaries' including involvement of external experts and other forms of oversight

SCC Online Web Edition, Copyright © 2020
Page 5 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

- Penalties to be imposed in case of violation, Guidelines for compensation to the victim(s), Suggested time-periods for remedial action.

Surveillance Capitalism

Corporate Surveillance is already a danger that governments across the globe (including ours) are finding tough to tackle. The increased periods of data-retention, without making clear the rationale for the same, make such a database even more attractive for abuse in a global data economy by entities interested in the commoditization of not just data but citizens.

Security Concerns — Decrypt or Don't Offer Encryption

The proposed amendments undermine encryption and cyber-security in times of increased cyber-attacks. The said amendments contradict the principles of data minimization, endorsed by the same Ministry in the Draft Data Protection Bill. No replacement proposal has been unveiled to ensure similar, if not greater, cyber-security for common information technology (hereinafter 'IT') users in the absence of the limited built-in security that encryption offers.

Absence of Breach/Exposure Intimation & Compensation Provisions

There is a lack of clarity about the burden of intimation upon accidental exposure of personal information (sensitive or otherwise) or commercial information due to such surveillance to the world at large, unauthorised personnel or third parties. There is also lack of clarity about the parameters to quantify the impact of such exposure on a particular individual and others (individuals, groups and corporate entities) who may be indirectly impacted by the same along with processes and procedures to ensure that due compensation is awarded.

Trade and Commerce

Trade and Commerce require free communication. Surveillance, as well as acquisition of information, sit has potentially harmful effects on economic growth and acceptance of the technology. Mass surveillance not only renders user data open to abuse, but it also undermines the premise of secure and stable payment gateways. Similarly, legal or commercial activities transacted online require some semblance of confidentiality to ensure the protection of proprietary rights and effective functioning.

HUMAN RIGHTS — PROTECTED ONLINE

Without repeating information about national and international laws protecting human rights such as freedom of speech and expression, or the right to privacy that is well documented and well known, I submit that these 'physical world' human rights subsist with the same force in the online world.

In 2013, the United Nations (hereinafter 'UN') General Assembly adopted Resolution 68/167, which highlighted growing global concerns about the potential adverse impact of surveillance and interception of communications on human rights.[12]

UN members got together to observe that "*State efforts to address the security ICTs must go hand-in-hand with respect for human rights and fundamental set forth in the*

SCC Online Web Edition, Copyright © 2020
Page 6 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

Universal Declaration Human Rights and other international instruments". Privacy was reaffirmed as a mechanism for 'realization of the right to freedom of expression'.[13]

Similarly, the UN General Assembly also affirmed that the rights held by people offline must also be protected online. States were called upon to respect as well as protect the right to privacy in digital communication(s). States were also called upon to conduct a review of their procedures, practices and legislation(s) dealing with communications surveillance, interception and collection of personal data. The General Assembly underscored the need to ensure effective compliance and implementation of States' obligations under international human rights law(s).[14]

Resolution 69/166 — 'The Right to Privacy in the Digital Age', follows the Report of the High Commissioner for Human Rights requested in Resolution 68/167 of the General Assembly.[15] The Office of the United Nations High Commissioner for Human Rights (hereinafter 'OHCHR') Report in question noted that technology can facilitate violations of human rights via mass surveillance, interception of communications and data collection and expressed concern that mass surveillance 'technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls'.[16]

In a potential networked-database, abuse can come from both, public and private entities. It is also important to understand that between 'privacy transgressors' - public or private, there exists a level of inherent 'mutual complicity', even though the pressurizing tactics may be employed by only one, if not both. However, the eventual victim is always individual freedoms and thus, societal well-being. The above-mentioned OHCHR Report further notes that,[17]

The resultant sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating Article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.

It may be further noted that compliance with Article 17 of International Covenant on Civil and Political Rights, 1966 (hereinafter 'ICCPR') concerned with integrity and confidentiality of correspondence-requires that correspondence is delivered to the addressee without an interception and without being opened or otherwise read. It envisages a prohibition on surveillance (electronic or otherwise) interceptions of communications (telephonic, telegraphic or otherwise in nature), wire-tapping and recording of conversations.[18] The term 'correspondence' implicitly incorporates digital correspondence and electronic communication and expression such as emails, text messages, etc.

FREEDOM OF SPEECH AND EXPRESSION, RIGHT TO PRIVACY AND SURVEILLANCE

Cyber communication is the dominant mode of expression of this century— 'More and more people express their views not by speaking on a soapbox at a Speakers' Corner, but by blogging, tweeting, commenting, or posting videos and commentaries.'[19]

Freedom of Speech and Expression — A Cornerstone

Freedom of speech and expression is not a stand-alone right.[20] It is the key to other fundamental rights and human rights. The protection awarded to every

SCC Online Web Edition, Copyright © 2020
Page 7 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

citizen's speech, expression, thought and beliefs or even his privacy is essential to ensure that the public need not fear that its conversations and activities are being recorded, monitored, analysed and in the present age, monetized.

The Indian jurisprudence on 'right to privacy' reached a definitive milestone with the 9-Judges Bench of the Hon'ble Supreme Court overruling *MP Sharma* v. *Satish Chandra*,[21] and the 6-judge bench decision in *Kharak Singh* v. *State of UP*,[22] and holding that the right to privacy is protected 'as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution'.[23] This right to privacy also includes the right to have one's data protected. Digital privacy is a subset of the right to privacy. The rights-based approach creates a safety net wherein citizens can exercise control over their data — mandating consent for any kind of usage, processing, sharing with third parties, entitlement to seek removal of data as well as the 'right to be forgotten'. The right to privacy includes the right to respect for digital communications.[24]

Consequences of Tinkering with Communications and Privacy

The collection, as well as retention of the communication/content along with the meta-data or other 'physical' links, is an infringement of the right to privacy, regardless of whether it is utilized for any purpose or not. If the Government (or any other entity) infringes the right of privacy, the injury spreads far beyond the particular citizens targeted, it intimidates many more.

Additionally, the right to a conducive environment for development is also infringed, because people may alter their behaviour if they are under surveillance. For example, the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, asserted that the practice of 'surveillance and intelligence databases undeniably has a chilling effect on protestors who fear to hold further protests',[25] thus, undermining their freedom of expression as well as effective participation in a democracy.

Similarly, the factum of collection of data can cause an individual to self-censor and affect an individual's right to freely seek and impart information.[26] (Elaborated in the next section)

European Vigilance for Freedom of Expression and Right to Privacy

In *Handyside* v. *The United Kingdom*,[27] the European Court of Justice (hereinafter 'ECJ') observed that the freedom of expression:[28]

> *It is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'.*

In another case, the ECJ observed that the mere existence of legislation permitting secret monitoring of communications will amount to an interference with the right to privacy, irrespective of any measures actually taken against individuals.[29]

ABSENCE OF PROPORTIONALITY ENCOURAGES ABUSE: OVERREACH IS

SCC Online Web Edition, Copyright © 2020
Page 8 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

LIKELY?

The Prism Scandal and 2014 National Security Agency Report

It is admittedly difficult to reconcile seemingly contradictory priorities like security and freedom of expression or right to privacy. However, history shows that overreaction and overreach to the detriment of freedom of speech and expression, right to information, right to privacy and the process of public opinion formation are more likely.[30] Reference may be made to the National Security Agency (hereinafter 'NSA') Report 2014 (result of the United States PRISM program) wherein the leading global cyber experts noted that whenever they are charged with keeping nation or national ideals safe, programs and policies often go beyond what is necessary and appropriate to protect the nation,

and instead take steps that are unnecessary and at times, dangerously endanger individual freedom.

The Report presents a well-known fact that US Presidents Johnson and Nixon encouraged government intelligence agencies to investigate 'subversives' for which extensive surveillance and information collection was undertaken. It covered over 3 million people in an attempt to investigate critics as well as expose, disrupt and neutralize their efforts to affect public opinion.[31] When the matter was investigated by the Legislature subsequently, a committee member noted that:[32]

> "*The government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts (…) The Government, operating primarily through secret informants, (…) has swept in vast amounts of information about the personal lives, views, and associations of American citizens.*"

The NSA Report of 2014 also refers to the Church Committee which noted years back that, too often intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression. This danger is inherent in the very essence of government intelligence programs because the natural tendency of the Government is towards abuse of power and because men 'entrusted with power, even those aware of its dangers, tend, particularly when pressured, to slight liberty.'[33] The Committee also noted that it encourages the natural 'tendency of intelligence agencies to expand beyond their scope' and to generate ever-increasing demands for new data. Apprehensions were also expressed about the fact that once the intelligence (information and data within the present context) is collected; there is strong pressure to use it.[34] The Committee called for caution for 'in an era where the technological capability of Government relentlessly increases, we must be wary about the drift towards 'big brother government' and instead put special emphasis on restraints for even future abuse'.[35]

Global Overview of Abuse and Overreach

The rationale behind such repetition of abuse of power is not to cast aspersions but to state a well-documented fact that massive collections of data are often used to the detriment of citizens and their fundamental rights. Examples

can be found across the globe. For instance, Thai citizens have found their freedoms

SCC Online Web Edition, Copyright © 2020
Page 9 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

and rights impacted by three interconnected elements-mass surveillance, surveillance by the masses, and normalization of surveillance.[36]

The use of Cyber-Scouts (a form of government-backed cyber vigilantism) and Cyber Witch Hunts (that punish even non-conformity with the majoritarian views) is not unique to Thailand.[37] It also finds a parallel in the Chinese government-backed '50 -cent bloggers' used to promote pro-regime information as well as to detect and file a complaint(s) for action against expressions deemed unfit.[38] Jacobs also quotes a Chinese student as observing that 'If we restrict our internet and we Chinese cannot protect our voices, then the whole world will only hear those other voices'. Though made within a specific context distinct from the present discussion, the essence of the statement is still important — freedom of expression must be protected, and non-proportionate measures that have been documented to adversely impact the same are constitutionally invalid.

Similarly, a writer argues that in Ethiopia, the extent of surveillance abuse — perceived and real, has impacted the range of communication and self-expression along economic growth.[39] He contends that 'state incursions also obstruct the flows of domestic and global information exchange, accelerate social divisions among citizens, and ultimately restrict the full capacity of sustainable development.

Dangers of Mass Surveillance

Double Threat - State Surveillance and Surveillance Capitalism

To quote US Supreme Court Justice Robert H. Jackson - without clear limitation(s), "*a federal investigative agency would 'have enough on enough people' so that 'even if it does not elect to prosecute them, the government would (…) still 'find no opposition to its policies' 'even those who are supposed to supervise are likely to fear them*."[40]

In a 2013 meeting of the UN Human Rights Council, the High Commissioner noted that the threat posed by mass surveillance to human

rights ranks very high on the list of pressing global human rights situations.[41] The combination of state surveillance and surveillance capitalism has divided 'citizens in all societies into two groups: the watchers (invisible, unknown and unaccountable) and the watched' which has far-reaching consequences for democracies 'because asymmetry of knowledge translates into asymmetries of power'.[42]

Private entities sharing data with the government or vice-versa (depending on the nation and corporate interest involved) is a reality that no one can deny. For instance, in China, a facial-recognition system for quick access by residents at a residential complex has added to the local police's collection of photos of local residents.[43]

Altering Behaviours in Functional Democracies

A 2015 survey (though small in scale) found that 'levels of concern about government surveillance in democratic countries are now nearly as high as in non-democratic states with long legacies of pervasive state surveillance', resulting in erosion of faith that the government will respect their freedom of expression or rights to privacy.[44] Almost one-third of the respondents admitted to avoiding particular topics and some expressed apprehensions about even researching certain topics or expressing certain views publically due to fear of negative consequences.

Wary Local ICT Users — A Survey

In a non-probability random sampling survey of two groups (Public Servants and Law Students) in the Union Territory of Chandigarh undertaken by this writer, the

SCC Online Web Edition, Copyright © 2020
Page 10 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

following data emerges from a partial preliminary analysis:

Group I - Public Servants.

Trusting Government with Data, Government Surveillance & Impact on Expression

40% of respondents agreed (or strongly agreed) with the statement— 'I trust the government (any government in power) with my data'.

Interestingly, of the 40% expressing trust, only 50% believe that concerns over government data collection and surveillance are overrated. Further, 62.3% of the same group believed that government tracking will affect how they express themselves while 12.5% believed that they will not be affected by government tracking. (25% were neutral)

30% of respondents disagreed (or strongly disagreed) with the statement while 30% were neutral about the same.

Of the respondents aware of the proposed 2018 amendments, 15.38% believe that complete surveillance is likely in India while 46.15% consider it to be a possibility, and 38.46% believe it to be unlikely.

Group II - Law Students

Trusting Government with Data, Government Surveillance & Impact on Expression

Only 10% of respondents agreed with the statement— 'I trust the government (any government in power) with my data'.

Of this 10%, half believed that concerns over government data collection and surveillance are not overrated while the other 50% was neutral. Additionally, 100% of this group agreed that government tracking will affect how they express themselves.

Overall, 55% of Group II respondents disagreed (or strongly disagreed) with the statement, while 35% were neutral about the same.

Of the respondents aware of the proposed 2018 amendments, 62.5% believe that complete surveillance is likely in India while 25% consider it to be a possibility. 12.5% of the respondents opted for 'Do Not Know' as an answer.

European Pro-Activism Against Retention of Data/Information

ECJ, in 2014, held that a requirement mandating retention of data, relating to a person's private life and to his communications for a particular period of time by providers of publicly available electronic communications services or of public communications networks for the purpose of possible access to such data by the competent national authorities, directly and specifically impacts private life and accordingly is in violation of the EU Charter of Fundamental Rights.[45]

CONCLUSION AND SUGGESTIONS

It does not appear to be pragmatic or backed by historical evidence (global, within the sub-continent and the Country— discussed above) that 'trust' is enough to assure

SCC Online Web Edition, Copyright © 2020
Page 11 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

that the constitutionally protected rights of the citizens will be protected. Or that massive database of extraordinarily sensitive private information will not be utilized, now or in the future, by any unauthorized personnel, government or corporate body despite the absence of any substantial safeguards, independent oversight mechanism and economic and criminal penalties for such violators.

The rules place an undue burden on both intermediaries and users. No information has been put forth what potential technologies are to be utilized to offset these burdens or ensure due processes for artificial intelligence technologies are still very 'context-dependent' and require human oversight.

The severe and long-lasting implications of these amendments do not encourage retrospective cures. The government should first put in place functional protections and guarantees, safeguarding Indian constitutional and social sensibilities before responding in a piece-metal and often, contradictory fashion in light of international trends. ICT and Internet consist of varied stakeholders with different utilities and levels of dependence— a 'one size fits all' solution is very likely to fail in the attainment of its objectives and adversely affect more stakeholders than anticipated.

Even as netizens and citizens fight for their freedoms and rights in a space increasingly oriented towards surveillance capitalism and no solutions are in sight, the government could abstain from creating fears of a 'big brother' structure that will hamper the values India and Indians hold dear.

Page: 17

There are obvious solutions for some of the problems posed by the proposed amendments. Fast-response 'due process' procedures online and offline with dedicated judicial oversight as well as prior judicial approval of orders dealing with 'objectionable' content is a starting point. Legislators must pay equal attention to present day capacities and future challenges. IT-related legislations and the rules thereunder ought not to be contradictory to one another, rendering them infructuous.

Meaningful Public Engagement

Given that the topic at hand has significant consequences for the freedoms of Indian citizens, possibly fulfilment of their responsibilities under the Constitution and their participation in the democracy as well as the government's ability to effectively safeguard the citizens, it would be appropriate to undertake wider-publicized public engagement before rushing to use executive powers to create a contradictory regime of rules which may or may not attain the desired objectives. In addition, users of technology tend not to be mere consumers— they are also co-creators. To enable IT users to understand both their roles and the socio-economic consequences of the same, it is essential that any outreach effort recognizes the need for exposure-level based differentiated programs.

Such public discourse and engagement could be made more meaningful by providing concrete information on:

- The causal links of the problems that the government wishes to solve, and the anticipated results when such problems are dealt only via digital intervention(s);
- Reports (final or preliminary) of studies or analysis, if any, that have been undertaken for the cost-benefit analysis in economic, social, political and cultural terms;
- Reports (final or preliminary) of studies or analysis, if any undertaken, supporting the implementation of these digital amendments first instead of alternative

SCC Online Web Edition, Copyright © 2020
Page 12 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

resolutions to the problems sought to be resolved;

- Results of a Privacy and Civil Liberties Impact Assessment, if any conducted;
- Opinions of legal and technical experts, if any sought, upon the reliability, cost-effectiveness and non-infringement of the Indian Constitution by these amendments in achieving their said objectives;
- Measures and penalties being considered to ensure Privacy and Civil Liberties Elements have a forceful and effective voice in the process with the government and private entities if any; and

- Specifications of the standard of special legal and technical training and operations intended to be imposed upon and adhered to by the public and private actors to ensure compliance with the Constitution and international law.

Transparency and Accountability

The rules ought to, regardless of the fate of the proposed amendments, incorporate specific and binding provisions for transparency and accountability mechanism—provisions that ensure that any agency or department requesting information or data declare the same to the Legislature and provide data on the same to the public with the limited and well-defined but essential exemptions, capable of effective demarcated enforcement, in favor of national security. Excessive delegation ought to be avoided. Where delegation cannot be avoided, specific parameters of operation have to be provided, and there must be effective oversight over such implementation.

The Path Ahead

Intermediaries form a large and significant link in the ICT dependent present-day world. And the proposed amendments have got the businesses mulling over the viability of operations, the potential for compliance, pros and cons of data localization and what definition of user ought to be utilized for the purpose of mandatory national office and incorporation under Companies Act, 1956 or Companies Act, 2013.[46] Some foreseeable impacts on individual rights and a democratic setup have been enumerated earlier.

Different nations have responded to the same challenges that the proposed amendments seek to combat in different manners. The varied responses can be grouped on the basis of present socio-political tendencies as well as historical leanings of different nations. However, the key takeaway is that different mechanisms can be utilized to deal with the problem at hand. The question remains whether the government and the people would want to and are able to utilize this opportunity to show respect for constitutional and historically respected values and further the same.

---

* LLM Candidate, University Institute of Legal Studies (UILS), Punjab University.

[1] Jack M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 (1) NYU Law Rev 57.

[2] Comments/Suggestions Invited on Draft of the Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 (Ministry of Electronics and Information Technology) <http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9C-information-technology-intermediary-guidelines> accessed 31 January 2019.

[3] FAQ on Draft Amendment of Intermediary Guidelines Rules in India (SFLC, 8 January 2019) <https://sflc.in/faq-draft-amendment-intermediary-guidelines-rules-india> accessed 31 January 2019.

SCC Online Web Edition, Copyright © 2020
Page 13 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

[4] FAQ on Draft Amendment (n 3).

[5] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, rule 3(8).

[6] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, rule 3(9).

[7] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, rule 3(2)(b).

[8] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, rule 3(4).

[9] (2013) 12 SCC 73.

[10] Katrien Jacobs, *People's Pornography: Sex and Surveillance on the Chinese Internet* (Intellect Books Ltd 2012) 50; Pinkaew Laungaramsri, 'Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand' (2016) 9 (2) Austrian Journal of South-East Asian Studies 195.

[11] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, rule 3(5).

[12] UNGA Res 68/167 (21 January 2014) UN Doc A/RES/68/167.

[13] Daniel Joyce, 'Privacy in the Digital Era: Human Rights Online?' (2015) 16 (1) Melbourne Journal of International Law 270, para 5.

[14] The Right to Privacy in the Digital Age (United Nations Human Rights Office of the High Commissioner) <http://ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx> accessed 31 January 2019.

[15] UNGA Res 69/166 (10 February 2015) UN Doc A/RES/69/166.

[16] Human Rights Council, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014); Daniel Joyce (n 13).

[17] UNHCR, Human Rights Council 27th Session 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37; Daniel Joyce (n 13).

[18] UN International Human Rights Instruments 'Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies' (27 May 2008) UN Doc HRI/GEN/1/Rev9; Daniel Joyce (n 13).

[19] Harold Hongju Koh, 'International Law in Cyberspace' (*US Department of State*, 18 September 2012) <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm> accessed 31 January 2018.

[20] 'The Right to Freedom of Expression and Religion' (*Icelandic Human Rights Centre*) <http://humanrights.is/en/human-rights-education-project/human-rights-concepts-ideas-and-fora/substantive-human-rights/the-right-to-freedom-of-expression-and-religion> accessed 31 January 2018.

[21] AIR 1954 SC 300.

[22] AIR 1963 SC 1295.

[23] *KS Puttaswamy* v. *Union of India*, (2017) 10 SCC 1.

[24] UNGA Res 68/167 (21 January 2014) UN Doc A/RES/68/167; UNGA 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (23 September 2014) 69th Session UN Doc A/69/397; *Copland* v. *United Kingdom*, [2007] ECHR 253; *Weber and Saravia* v. *Germany*, [2006] ECHR 1173.

[25] Gabor Rona and Lauren Aarons, '*State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace*' (2016) 8 (3) Journal of National Security Law and Policy 1.

[26] Manon Oostveen and Kristina Irion, '*The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?*' (2016) Amsterdam Law School Legal Studies Research Paper 68/2016, 11.

[27] *Handyside* v. *United Kingdom*, [1976] ECHR 5.

[28] The Right to Freedom of Expression and Religion (n 20).

[29] *Weber and Saravia* v. *Germany* [2006] ECHR 1173; Gabor Rona (n 25).

[30] Richard A Clarke and others, *The NSA Report: Liberty and Security in a Changing World* (Princeton UP 2014).

[31] Richard A Clarke (n 30).

SCC Online Web Edition, Copyright © 2020
Page 14 Tuesday, September 01, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

[32] ibid 40.

[33] ibid 42.

[34] ibid.

[35] ibid 43.

[36] Pinkaew Laungaramsri, 'Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand' (2016) 9 (2) Austrian Journal of South-East Asian Studies 195.

[37] ibid.

[38] Katrien Jacobs, *People's Pornography: Sex and Surveillance on the Chinese Internet* (Intellect Books Ltd 2012) 50.

[39] Daniel Grinberg, '*Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia*' (2017) 15 (3) Surveillance and the Global Turn to Authoritarianism 432.

[40] Richard A Clarke (n 30).

[41] Elspeth Guild, 'What does Mass Surveillance do to Human Rights?' (*OpenDemocracy*, 12 May 2014) <https://search-proquest-com.library.britishcouncil.org.in:4443/docview/1523700045?> accessed 31 January 2019.

[42] John Naughton, 'The Goal is to Automate Us: Welcome to the Age of Surveillance Capitalism' (*The Guardian*, 20 January 2019) <https://theguardian.com/technology/2019/jan/20shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> accessed 1 February 2019.

[43] Paul Mozur, 'Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras' *The New York Times* (Zhengzhou, 8 July 2018) <https://nytimes.com/2018/07/08/business/china-surveillance-technology.html> accessed 7 September 2018.

[44] 'US Mass Surveillance Curtails International Freedom of Expression: Watchdog' (*Sputnik*, 06 Jan 2015) <https://sputniknews.com/us/201501061016547856/> accessed 31 January 2019.

[45] *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources*, [2014] WLR III-1607.

[46] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, rule 3(7).

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.

© EBC Publishing Pvt.Ltd., Lucknow.