RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date: 11-04-2018

Analyzing the case for a new data protection law

Source: https://www.bing.com/images/search

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date : 11-04-2018

In This Issue

COVER STORY:

Analyzing the case for a new data protection law

HEADLINE OF THE WEEK:

- Deepening Crisis in MGNREGA Wage Payments

SECTION 1: ECONOMY

- India Had Job Losses in 2014-15 & 2015-16–Years of High GDP Growth

SECTION 2: GOVERNANCE AND DEVELOPMENT

- **Politics and Governance:** RTI reveals contradictory numbers of EVMs from Election Commission, suppliers; raise question mark on polls**,** Eight journalist groups question Press Council chairperson's revamp decisions, ask Centre to step in
- Health: From Best State to the Worst, Where Does India Stand on Health**?** AYUSH dispensaries in Delhi don't have half the essential medicines: CAG
- Law and Justice: Legal justice still difficult for sexually assaulted disabled women: Report

SECTION 3: INDIA AND THE WORLD

- Tariff hike issue: India wants amicable settlement with US

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date: 11-04-2018

Lead Essay

Analyzing the case for a new data protection law

Introduction:

India is witnessing rapid digitalization and expanding horizons of social media resulting in wide scale permeation of internet into the everyday activities of an average India. According to National Association of Software and Services Companies (NASSCOM), India's internet base today is the second largest after China and is projected to have more than 200 million people accessing the internet by 2022. Amidst all this data protection regime in India is in a state of flux. This influx of information resulting from several online activities has left sensitive data unprotected in the absence of a data protection law to protect information. News involving data harvesting, psychographic profiling and the alleged unethical influencing of votes in the US elections by British firm Cambridge Analytica and social network Facebook have raised legitimate concerns in India regarding the safety of data privacy. Events over the past year have exposed a threat of data leakage, invasion of privacy and identity theft by both state and non state actors. Data leaks and thefts are no longer limited to stealing of passwords and bank details. It entails several other threats such as theft of identity, unwanted access to personal records of mental and physical health, sexual orientation, biometrics as well as use of any other information provided to corporate or apps for a particular purpose with the intention of manipulating and influencing decisions of that individual. While Aadhaar has been a part of the privacy and data protection discourse for some time now, the revelations and exposés about leaks, invasions and the illegal usage of such data by apps have further increased apprehensions regarding the safety of an individual's information either with the state or any other party.

In the absence of a clear framework to deal with data protection and privacy issues and with increasing digitalization, the magnitude of vulnerability has increased over the years. This can be witnessed by the fact that the number of Indians experiencing cyber-attacks, as per the Internet Security Threat Report 2017, increased to 84 per cent in 2017 as compared to 73 per cent in 2016. The first 6 months of 2017 saw 918 data breach incidents reported globally compared to 815 in the last six months of 2016, a 13% increase. India has also been ranked fourth in online security breaches by the Internet Security Threat Report 2017. These numbers are clearly indicative of the threats that hover around data privacy and underline the urgent need for intervention. In the wake of serious concerns arising out of allegations of mass state surveillance along with possible data security breach, the inadequacy of India's data protection and privacy regime and the immediate need for a robust law to govern the same has been underscored repeatedly in the last few years.

Contours of data protection and privacy:

The debate on data privacy and the need for a credible data security framework reached India in the early years of the 21st century with the technological revolution and the rise of the software industry and telecoms. Today, data processing and collection is done through apps and other consensual sources with the help of automated systems. With the rise of automated processing and collection of data by the state or private individuals, conflicting interests of data collection vis a vis data protection and privacy presented itself as a grey area in the field of IT law. Publicly available personal information pose a greater risk for Indians because majority of the population is illiterate or possess limited digital literacy and individuals are repeatedly transmitting their personal information for various activities. While individuals often consensually opt to share personal details online, they may be largely unaware of the implications of providing personal details to

Lead Essay

sources online or might do so because it is required for availing others services. Thus, preparing a framework for data protection rules and guidelines require an understanding of the broad contours of data protection and privacy in the context of Indian society and the consequences its absence have on citizens. The reconciliation of competing interests is particularly pertinent incase of data collection by state actors which might possibly be coercive yet justified under the pretext of welfare and development.

In a scenario such as creation of the Aadhar database, the state is directly responsible for collection of information. Aadhar was promoted as a social security scheme which would ensure effectiveness in the functioning of government schemes by reducing loopholes in its implementation. However, in the past few years, attempts have been made by the ruling government to make Aadhar mandatory to open and maintain bank accounts and also linking it to phone numbers. Aadhar was initially regarded as an efficient means to plug gaps in the welfare system by linking it to ration cards and other welfare schemes of the government but by making it compulsory for services like gas connections, bank and phone services, it has made it possible for the government to track every activity of an individual. A sting operation carried out by The Tribune earlier this year revealed that a service being offered by anonymous sellers over WhatsApp provided unrestricted access to details for any of the more than one billion Aadhaar numbers created in India thus far, severely compromising the data security of millions of users. This leakage of confidential information and biometrics was referred to as a national security threat and called for an urgent appraisal of the data protection system in the country. In the light of such surveillance arguably without the consent of the citizens, the Supreme Court clarified the position of privacy by recognizing it as a fundamental right, enforceable against the state. Hence this judgment largely curtailed the power of the state over a citizen's personal information and established the position that data protection and right to privacy are intrinsically linked. However since this can only be applied against the State, it could not be treated as blanket right, leaving a void in the field of data protection. Moreover, there has been no corresponding law enacted to implement the right.

Prior to the Aadhar data leak, there were other data and identity thefts of equally large magnitude and impact in the recent past which forced the government to take note of the growing challenge posed by technology and the inadequacy of the system to regulate it. One such serious lapse was the Debit Card Breach in 2016 where about 3.2 million users lost their debit card PINs as well personal banking details due to ineffective implementation of payment security standards. The breach took place across ATM networks of a number of popular banks. The Food Tech Database scam in 2017 also shocked the Indian market when personal details of over 17 million users were found at risk. The privacy of the registered users was invaded and all the important details such as email addresses and passwords were also hacked. Another 120 million users reportedly suffered an invasion of personal data. In 2017 alone, almost 2 data billion records were reportedly breached.

The significance of this discourse on privacy protection increased exponentially after the revelation by a whistleblower from political marketing firm Cambridge Analytica who alleged that confidential information of 87 million Facebook users have been used without their consent to enable targeted advertising and manipulate elections in USA . This was facilitated by Facebook which, between 2007 and 2014, allowed third party apps to access a large number of personal data of Facebook users, with the consent of the user. The allegations have left Indians concerned as well since the reports suggested attempts by Indian political parties to divert citizens' information to third parties for electioneering. The NaMo app which is the Prime Minister's app has been accused of setting up a default privacy setting which allows it to access full data stored on a user's phone while sending the information to a third party analytics company without the consent of the user. While the latest data theft has now turned into a political war between parties across the Indian political

Lead Essay

landscape, the important issue that emerges out of this is the right of a citizen to safeguard his privacy and identity from data thefts and if there is any recourse available to him/her against both state and non state actors.

The existing framework and its drawbacks:

The Constitution of India does not patently grant the fundamental right to privacy. However, the courts have read the right to privacy into the other existing fundamental rights, ie, freedom of speech and expression under Art 19(1)(a) and right to life and personal liberty under Art 21 of the Constitution of India. Recently, in the landmark case of Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors., the constitution bench of the Hon'ble Supreme Court has held Right to Privacy as a fundamental right, subject to certain reasonable restrictions. However no corresponding law has been enacted to implement the judgment and it is still uncertain whether an individual has the right to withdraw his consent and refuse to participate in the data collection by government. The current data protection regime in India revolves around provisions of the IT Act which was enacted in 2000. By virtue of the tremendous strides made by technology in the last decade, these provisions have been gradually rendered redundant. The Information Technology Act, 2000 provides specific protection of sensitive personal data or information such as health records, sexual orientation, biometric information and financial information, compensation claim by aggrieved individuals. Further, it also provides for general protection of privacy and confidentiality by imposing imprisonment and granting compensation for disclosure of information without the consent of the individual involved. While the Indian data protection law has extra-territorial application and would apply to entities outside India like Google and Facebook that collect data of Indian users, practical enforcement of the same may be a challenge under the current framework where no specific powers of enforcement are codified against foreign entities.

In 2008, The Information Technology Amendment Act, 2008 (ITAA) enacted two loosely framed provisions under Sections 43-A and 72A of the Act. Compensation for failure to protect data (Section 43-A) was introduced which states the liability of a body corporate to compensate in case of negligence in maintaining and securing the “sensitive data.” However, the Act fails to define “sensitive data” and states the same as “personal information as may be prescribed by the Central government.” Three years later, IT Rules 2011 were issued by WIPO defining in detail the term “sensitive data” and what it entails but the vague drafting of the provision has left the applicability of the same uncertain. Section 72-A provided for penalty for breach of data privacy and makes the offender liable to be jailed for 5 years or fined.

The effort to bring in a second legislation — The Personal Data Protection Bill — governing data protection and privacy has been in the pipeline since 2006. Several amendments have been made to the Bill and the latest draft was introduced in Rajya Sabha in 2014. This bill provides a definition of “personal information” and vaguely explains the role of a “Data Controller but does not substantially elaborate on other issues like its application to all the sectors, time period for retainment of sensitive data and regulation of data collected by government. In 2017, the Srikrishna Committee, set up in the aftermath of the privacy judgment by the Supreme Court, presented a white paper on data protection in India. However, a fundamental issue that was not addressed, which forms the core of any debate on data protection is whether India needs one data protection law to cover both the public and private sector and whether we really want to bestow on a coercive State the authority to create a data protection regulator that will have the powers to punish both public and private sectors across the country for any violation of privacy or data protection laws. While it is necessary to have a law that holds private players accountable for the abuse of data obtained by them, the new Act must ensure that unlike the existing rules and guidelines, it does not provide all encompassing powers to the

Lead Essay

government and prescribes adequate provisions for determining the liability of state actors in case of a breach of data collected specifically by the government.

Need for a new framework:

Today there is an unprecedented amount of personal data available with Government and private sector players. Digital India, Aadhaar and demonetization drives have added to the already growing pool of personal data with various public and private players. With the country moving towards further digitalisation, infrastructure and devices are increasingly getting vulnerable without a robust framework that substantially address the current needs of data privacy. There are several loopholes that can be manipulated by cyber criminals, especially if a large database is stored in a single space, as has been proven by the Aadhar data leak as well data theft through apps. As data security is becoming a matter of great concern, it is important that it incorporates and offers meaningful consent online and strictly oppose inappropriate data practices. Other measures should include having policies and processes in place to ensure strict safeguarding of personal information. Regulatory bodies have routinely stressed the need for a framework to protect information of the app users, server location and third-party services. Moreover, a mechanism to monitor and prevent unauthorised state surveillance should also be addressed.

Since data is not limited by physical or geographical boundaries, it is often difficult for the current laws to define the jurisdiction of courts. Any data protection law targeted at foreign data companies, be it social media giants or cloud service providers, should provide Indian consumers with a bill of consumer rights guaranteeing certain baseline rights protecting their data, which they can enforce in India through either litigation or arbitration panels provided that both take place in India and are accessible to Indian citizens. Globally, governments and other stakeholders, including the industry and civil society, are looking at newer norms of data privacy. However, although much of India's draft data protection laws are influenced by the European model, it is important to remember that the Indian bureaucracy and political system function very differently from that in Europe and creating a centralised data protection authority along the lines of EU will contribute to centralisation of power that might not effectively be able to tackle government excesses. Ultimately, the need of the hour is to formulate a comprehensive new law which can balance the privacy concerns of citizens, protect business systems and at the same time regulate state control over data.

References

Rachna Khaira, Data Breach: Aadhaar Details up for Grabs for Just Rs 500, The Wire available at https://thewire.in/government/data-breach-aadhaar-details-grabs-just-rs-500

Vijay Pal Dalmia, Data Protection Laws In India - Everything You Must Know, Vaish Associates and Advocates, available at http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Laws+in+India

Sunneth Katarki, Ashi Bhat, Privacy Policy & Policy Of Privacy – Data Protection Conundrums, Indus Law Associates available at http://www.mondaq.com/india/x/671084/Data+Protection+Privacy/Privacy+Policy+Policy+Of+Privacy+Data+Protection+Conundrums

Prashant Reddy,Does India Need Only One Data Protection Law and Regulator to Rule Them All? The Wire, https://thewire.in/tech/data-protection-law-regulator-india

Amber Sinha, India's Data Protection Regime Must Be Built Through an Inclusive and Truly Co-Regulatory Approach, The Wire available at https://thewire.in/business/inclusive-co-regulatory-approach-possible-building-indias-data-protection-regime

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date: 11-04-2018

Lead Essay

Sonakshi Awasthi, Data privacy: Where is India when it comes to legislation?, The Indian Express available at http://indianexpress.com/article/india/what-is-india-data-privacy-laws-4811291/

Madhavan Narayanan, Apps, whether NaMo or Facebook, are meant to harvest data; what India needs is a Lokpal for data protection, The Firstpost available at https://www.firstpost.com/business/apps-whether-namo-or-facebook-are-meant-to-harvest-data-what-india-needs-is-a-lokpal-for-data-protection-4405639.html

Namitha Viswanath, Facebook-Cambridge Analytica scandal: Need for a robust data protection regime, The Business Times, available at https://www.businesstoday.in/opinion/columns/facebook-cambridge-analytica-scandal-need-for-robust-data-protection-regime/story/273736.html

Dipankar Sarkar, Emerging fault lines in data protection, LiveMint, available at https://www.livemint.com/Opinion/9mtp71AGFjWv1sKhzkr8EP/Emerging-fault-lines-in-data-protection.html

Surbhi Kapila, Increasing Digitisation in India, available at https://mediaindia.eu/digital/increasing-digitisation-in-india/

Internet Security Threat Report, April 2017: India Highlights, available at https://www.symantec.com/content/dam/symantec/docs/infographics/istr-5-1-en-in.pdf

Prepared by: Aadrita Das

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date: 11-04-2018

Headlines

The Deepening Crisis in MGNREGA Wage Payments

(Ankita Aggarwal, The Wire, April 8, 2018)

For 2018-19, due to no increase in the MGNREGA wage rates from last year of at least ten states out of which some of them are amongst the poorest in the country, millions of rural workers fall back on MGNREGA when there is no other employment available in their area. Increasingly un remunerative wage rates, together with long delays in payments and denial of compensation in case of the delays has turned many workers away from the employment guarantee programme. Much of the crisis in MGNREGA wage payments stems from the government's unwillingness to allot an adequate budget for the employment guarantee programme. This year's MGNREGA budget is only Rs 55,000 crore which is the same as last year's total budget in nominal terms.

Read More: https://thewire.in/the-arts/when-artists-collectively-archive-labour

Date Accessed: 08.04.2018

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date: 11-04-2018

Economy

India Had Job Losses in 2014-15 & 2015-16–Years of High GDP Growth

(Tish Sanghera, *Indiaspend*, March 30, 2018)

According to data released by the India KLEMS database, a research project supported by the Reserve Bank of India, India's employment growth rate fell by 0.1% in 2015-16 and 0.2% in 2016-17, despite the country's real gross domestic product (GDP) growing by 7.4% and 8.2%, respectively. The data reveals that several sectors –including mining and quarrying, and textiles and manufacturing – saw falling employment growth rates between 2014-15 and 2015-16. In 2015-16, as the Skill India Mission spent Rs 1,176 crore on training people with the right skills to find alternative employment, the employment growth rate fell 0.2%, indicating a loss of jobs to the economy at a time when the government was attempting to make 400 million people employable under the scheme.

Read More: http://www.indiaspend.com/special-reports/india-had-job-losses-in-2014-15-2015-16-years-of-high-gdp-growth-85686
Date Accessed: 01.04.2018

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
Rajiv Gandhi Institute for Contemporary Studies
Volume: 6, Issue-28 Date: 11-04-2018

Governance and Development

POLITICS AND GOVERNANCE

RTI reveals contradictory numbers of EVMs from Election Commission, suppliers; raise question mark on polls

(Firstpost, April 8, 2018)

As per a recent RTI reply filed by Manoranjan S Roy, there is an indiscriminate acquisition of Electronic Voting Machines (EVMs) by the Election Commission, inexplicable mismatch in numbers of machines from producers and buyers, and insecure transportation. While Roy's RTI queries reveal that from 1989-90 till May 15, 2017, the Election Commission procured a total of 1,005,662 BUs and 928,049 CUs from BEL, plus another 1,014,644 BUs and 934,031 CUs from ECIL, a RTI query to the Union Ministry of Law and Justice showed that the government received intimation of purchase of 1,395,306 BUs and 930,716 CUs in 2016-17. According to Roy, against the figures provided by the EC on the number of EVMs received, BEL and ECIL have submitted data with huge differences in the numbers they have supplied, at times ranging from several thousands to lakhs of EVMs, raising questions on "where the excess number of EVMs are going, what is being done with them".

Read More: https://www.firstpost.com/india/rti-reveals-contradictory-numbers-of-evms-from-election-commission-suppliers-raise-question-mark-on-polls-4422967.html

Date Accessed: 08.04.2018

Eight journalist groups question Press Council chairperson's revamp decisions, ask Centre to step in

(Scroll, April 8, 2018)

Journalists from eight media bodies-the All India Newspaper Editors Conference, Indian Journalists Union, Indian Newspaper Society, Working News Cameramen Association, Hindi Samachar Patra Sammelan, National Union of Journalists (India), All India Small and Medium Newspapers Federation and Press Association have issued a statement on Saturday, expressing "grave concern" about the decisions the chairperson of the Press Council of India, Justice CK Prasad, made to form the 13th Press Council. They said the "procedures" Prasad followed while reconstituting the council cast doubts over the council's autonomy. They pointed out that Prasad had called a meeting of the reconstituted Press Council, but only of eight members – five MPs and three official nominees and left out 20 other representatives of print media organisations. "The remaining 20 names have yet to be notified and reconstitution is still under way," –the statement said. They also appeal to the government to intervene and restore the credibility and sanctity of the Press Council of India.

Read More: https://scroll.in/latest/874895/eight-journalist-groups-question-press-council-chairpersons-revamp-decisions-ask-centre-to-step-in

Date Accessed: 08.04.2018

HEALTH

From Best State to the Worst, Where Does India Stand on Health?

(The Quint, April 8, 2018)

According to a NITI Aayog, while India has managed make notable gains in improving life expectancy, reducing fertility rate, addressing maternal and child mortality, and other health issues, the performance has fallen short of meeting targets both on the national as well as the global scale. Going by the NITI Aayog health index, under the larger states category, Kerala ranked as the healthiest state, Uttar Pradesh was ranked the worst. Under the smaller states category, the index ranks Mizoram the best state, and Nagaland the worst. Among the Union Territories, Lakshadweep ranks best while Dadar and Nagar Haveli ranks worst. On the

Governance and Development

global health index, India ranks 154 of the 195 countries on the index. On the global front, as per the Global Burden of Disease Study, India's dismal ranking comes owing to its poor performance in tackling cases of tuberculosis, diabetes, chronic kidney diseases and rheumatic heart diseases.

Read More: https://www.thequint.com/news/india/india-ranking-global-health-index-world-health-day

Date Accessed: 08.04.2018

AYUSH dispensaries in Delhi don't have half the essential medicines: CAG

(DTE Staff, Down to Earth, April 4, 2018)

Highlighting shortcomings of the Directorate of Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homeopathy (AYUSH), a recent report by the Comptroller and Auditor General (CAG) has revealed that Ayurvedic and Unani dispensaries in Delhi were provided with only 40 per cent of essential medicines during 2012-17. Forty three per cent of essential medicines were not available in Homeopathic Dispensaries at any given time during the period 2012-17. The report further notes that the three hospitals under the Directorate of AYUSH —Tibbia College, Dr. B. R. Sur Homeopathic Medical College Hospital and Research Centre and Chaudhary Brahm Prakash Ayurvedic Charak Sansthan—are functioning with around half the manpower they need. "Shortages in the cadres of doctor, pharmacist and nurse in the three medical colleges with attached hospitals were between 37 per cent and 52 per cent," says the report.

Read More: http://www.downtoearth.org.in/news/ayush-dispensaries-in-delhi-don-t-have-half-the-essential-medicines-cag-60097
DateAccessed:07.04.2018

LAW AND JUSTICE

Legal justice still difficult for sexually assaulted disabled women: Report

(IANS, Business Standard, April 5, 2018)

A new report by Human Rights Watch notes that despite important legal reforms on sexual violence, women and girls with disabilities lack equal access to justice. The challenges include reporting abuse to the police, obtaining appropriate medical care, having complaints investigated, navigating the court system and getting adequate compensation. The report, titled "Invisible Victims of Sexual Violence: Access to Justice for Women and Girls with Disabilities in India," interviewed around 111 people, including victims of sexual violence, family members, lawyers, officials from mental health institutions and shelter facilities, police, disability rights activists, etc., and covered 17 cases of rape and gang-rape from eight states: Chhattisgarh, Delhi, Karnataka, Maharashtra, Odisha, Tamil Nadu, Uttarakhand and West Bengal.

Read More: http://www.business-standard.com/article/news-ians/legal-justice-still-difficult-for-sexually-assaulted-disabled-women-report-118040500634_1.html
Date Accessed: 07.04.2018

RGICS POLICY WATCH
Policy Highlights | Quick Analysis | Insights
RAJIV GANDHI INSTITUTE FOR CONTEMPORARY STUDIES
Volume: 6, Issue-28 Date: 11-04-2018

India and the World

Tariff hike issue: India wants amicable settlement with US

(Amiti Sen, *The Hindu Business Line*, April 09, 2018)

Government officials say that India is in favour of an "amicable settlement" to the issue of increased import tariffs on Indian steel and aluminium by the US. Clarifying that India does not want to indulge in a trade war with the US, an important trade partner, one official said: "If one examines the items in the steel and aluminium category that have been penalised with raised import tariffs, they are largely the ones that China exports. India, on the other hand, exports a small percentage of the penalised aluminium and steel items." India, however, wants the US to revoke the duty hike against the country, as it has already done in the case of the EU, Argentina, Australia, Brazil, South Korea, Canada and Mexico.

Read More: https://www.thehindubusinessline.com/economy/macro-economy/tariff-hike-issue-india-wants-amicable-settlement-with-us/article23484194.ece
Date Accessed: 09.04.2018

Issue Coordinator: Aadrita Das **Connect with RGICS at:** info@rgics.org; www.rgics.org