Cyber Security and Data Protection: Challenges in the Indian Context

Subhasis Das

Traditionally, the terms cyber security and information security have been used interchangeably. However, there is a subtle difference between the two. Information can be stored in both physical and computerised forms. Hence, information security is a broader term, which includes all the means taken to protect information and information systems. Cyber security is a narrower term, denoting the means to protect or defend the cyber space so as to ensure its unhindered use. Large enterprises, companies, governments and organisations have historically guarded their data and information systems zealously. Increasingly, the focus shifted from the physical to the cyber domain, since most information and data systems shifted to the digital form. In the cyber domain, it led to the development of an entirely new cyber security industry, which came out with revolutionary new technical solutions, on a regular basis. However, this cyber security industry was focussed more on institutional and organisational data. Personal user data protection was addressed as an adjunct to organisational information security. Individual user data security was debated, and treated, under the umbrella of privacy laws, being left

Colonel **Subhasis Das** is Senior Fellow, Centre for Land Warfare Studies, New Delhi.

N.B. The views expressed in this article are those of the author in his personal capacity and do not carry any official endorsement.

to individual expertise and discretion. However, the emerging global discourse on personal data and its misuse, following the March 2018 Facebook and Cambridge Analytica revelations, has arguably shifted the focus of information security from the organisational to the personal space. What has also emerged is the fallacy of the term "personal cyber space". Personal data is being collected while users travel on holidays, while buying groceries, while having a meal at the neighbourhood restaurant or even while carrying out the most mundane of daily chores. This is being done while most users are unaware of the intricacies and implications of the process. The data volumes being generated are very large, the storage mechanisms are different, and the intended use is ambiguous. Traditional cyber security measures are incapable of handling this huge shift in sensibilities. This article will analyse the implications of individual user data, social media-driven manipulation of data and the overarching need for data privacy. Is it time that governments and institutional security mechanisms shift focus on this aspect, especially in view of the growing debate and clamour over the failure of existing mechanisms to protect personal user data?

Personal user data protection was addressed as an adjunct to organisational information security. Individual user data security was debated, and treated, under the umbrella of privacy laws, being left to individual expertise and discretion.

The Digital Ecosystem

An ecosystem can be defined as the complex of living organisms, their physical environment, and all their inter-relationships in a particular unit of space[1]. It consists of biotic and abiotic constituents, connected to each other as an integrated whole, where each component is dependent on the other. It would not be imprudent to extend this definition to the

At the foundational level, the ecosystem is driven by sheer economics and even the most insignificant occurrence in this vast maze has an economic underpinning.

context of the ubiquitous digital world of today. This is, indeed, an ecosystem where numerous discrete components are feeding on each other and have evolved complex and non-retractable dependencies. Within this mega digital ecosystem, certain smaller but connected sub-systems may be identified. The cyber sub-system has been well documented over the years wherein different types of software companies, anti-malware companies, zero-day bounty hunters, cyber criminals, hackers, legitimate and illegitimate users, etc., feed on each other and coexist, albeit with some inevitable conflicts. At the foundational level, the ecosystem is driven by sheer economics and even the most insignificant occurrence in this vast maze has an economic underpinning. An anti-virus solution was never intended to be permanent, nor was the recently discovered bug in software, the last in the line. Users, who used illegitimate software, were prepared to gloss over the associated problems which affected the ecosystem from time to time, for purely economic and parochial reasons. Software companies issued bug fixes and updates from time to time, but the issues never really got resolved permanently. Large corporations and financial companies that were adversely affected by the activities of cyber criminals have been known to keep the news under wraps, fearing the adverse publicity it would involve. Hefty payouts and ransoms have reportedly been paid by legitimate businesses to protect data and information. It has been a "win some, lose some situation", for the stakeholders of the ecosystem. The ecosystem has thrived over the years because the economic gains have consistently outweighed the losses.

The recent Cambridge Analytica episode has brought into the public discourse another matter that was known to most experts, but was kept under the carpet for years. This pertains to the commodification of user data in all forms. Combined with the explosive growth of the social media and the reach of the ubiquitous mobile phone, a new, more organised ecosystem driven by user data is emerging. This ecosystem appears to be benign and harmless to the casual user, but, in reality, is effectively organised, planned, is eminently intrusive and feeds on the user's social needs and insecurities. It is estimated that this user data-driven ecosystem will push digital advertisement spending worldwide to US$ 335.48 billion by the year 2020[2]. In his widely popular book published in 2015, *Future Crimes – Everything is Connected, Everyone is Vulnerable and What We Can Do About It*, author Marc Goodman has talked about this user data, which is being continuously collected by numerous agencies, both legally and illegally. There is no disclosure on the storage, intended use, collection methods or deletion of such data by such agencies, a majority of which are foreign multinational corporations. The user needs to contend with the fact that "isolation" is no longer a safety net. Every connected user is continuously generating data and, shockingly, the user has no lien on this data and its further manipulation. This new reality of the user data-driven ecosystem needs to be accepted, as this is likely to be the future, the debates over privacy and security notwithstanding.

The user needs to contend with the fact that "isolation" is no longer a safety net. Every connected user is continuously generating data and, shockingly, the user has no lien on this data and its further manipulation.

Whistleblowers' Revelations

Julian Paul Assange in 2010, Edward Snowden in 2013, and Christopher Wylie in 2018, have arguably altered the course of history of digital space. These whistleblower disclosures have shown that in the ubiquitous, all pervasive internet, there is, indeed, a thin line between the hunter and the hunted. It would not be far-fetched to predict that such revelations from insiders could be the new normal for the future. After all, who would not like to attain "cult status" in the new digital world order? What comes across alarmingly in all the previous episodes of whistleblower revelations is that the agencies or people, who are now in the dock, were never on the wrong side of the law in the very first place. The agencies that are now being questioned are perfectly legitimate entities, funded by government or public monies, with large scale transparent operations. These agencies were not operating from dark, dingy, underground quarters with computer screens eerily glowing in the dark, but from swanky offices located in central business districts of major cities.

In July 2017, the world had witnessed twin ransomware attacks of unprecedented proportions. The "Wanna Cry" ransomware attacks affected almost 150 out of 196 countries presently recognised in the world. Both "Wanna Cry" and "Petya" exposed the alarming interconnect among government agencies, software companies, hackers, anonymous groups like the "shadow brokers", digital currency and the internet community. Interestingly the tools used in the attack were initially intended for use by the National Security Agency (NSA) of the United States of America, but were lost to anonymous hackers. Hence, the lapse can be attributed to legitimate government agencies whose activities are fully supported by legislation and regulations. In spite of the scale of the attack, there has been no clear attribution or accountability till date, and there is likely to be none in the future.

The modern-day whistleblowers have indeed contributed to transparency and widespread understanding of the problem at hand, proving to be a boon to the common world citizen. It has also emerged during the revelations that even large multinational corporations like Facebook and security organisations like the NSA have failed to ensure the security of data under their control, in spite of holding the foremost cutting age technologies, qualified personnel and modern systems. Large organisations are plagued with a propensity to lose intimate control over the various processes, and this tendency is likely to continue in the future, assurances and testimonies by Marc Zuckerberg notwithstanding. The subsequent use and manipulation of the collected data signals the emergence of an entirely new dimension of warfare, where actors can allegedly influence the minds of the electorate of another nation – being termed an undeclared war of supremacy in cyber space. In this race, the tools, techniques, targets and effects of warfare are completely different, with analysts calling this Cold War 2.0, a fascinating study of conflicting national interests being played out in a digital domain, where the base data is being generated by normal, unsuspecting citizens.

The subsequent use and manipulation of the collected data signals the emergence of an entirely new dimension of warfare, where actors can allegedly influence the minds of the electorate of another nation.

Personal User Data and Social Media

What Facebook gave away to a respected University of Cambridge researcher and to other legitimate App creators, was information, which was handed over voluntarily by the users of the ecosystem, people like you and me. Individually, the pieces of information could be seen as innocuous and minor, however, when seen in the larger context of 87 million users and their suspected effect on elections, the result is entirely different. It is also alarming that the initial indicators about the suspected data leak were available to Facebook as early as 2014, however, only limited corrective action was taken. There was no attempt to analyse the quantum of data lost, its deletion and further proliferation. Incidentally, the black hat hackers and cyber criminals are also actively seeking similar user information. It is evident that the dividing line between the good and the bad is vanishing rapidly in this quest to collect user data. This concern about data security in the age of social media is likely to dominate the public discourse in the years to come.

Internet behemoths like Google, Facebook and Amazon that have taken data collection to an entirely new level, are likely to be joined by a host of other players, including government departments. Latest news reports indicate that the social media outlet Twitter also sold data to Camridge Analytica[3]. WhatsApp founder Jan Koum has reportedly quit the parent company Facebook over differences over data privacy. This is significant since WhatsApp has created a mobile payments system for India over its hugely popular social media platform and also reportedly shared customer payment data with its parent, Facebook[4]. The purpose and methods of data collection may differ, however, the underlying theme will be economics and opinion building of the target population. The emergence of the Internet of Things (IOT) will push this data collection process to even greater levels. The underlying economics-driven ecosystem is unlikely to see any drastic transformation, since the common user of digital space is too intricately involved in the process. In spite of the adverse publicity of platforms such as Facebook and Google, a minuscule number of netizens would have actually exited from the same. Today, convenience and social needs far outweigh privacy and security concerns for a common net user. In this complex environment, it would also be utterly naïve and illusionary to expect a solution to the problem from the same players who are making billions of dollars from the system. Hence, it would be prudent to explore alternate solution frameworks.

User Data Protection

The proposed framework, in which a reasonably acceptable degree of user data protection can be expected, is based on two major facets. Firstly, the primacy of the nation-state vis-à-vis the multinational internet giant(s) has to be reestablished unequivocally. Secondly, the common netizen has to be offered far greater choices on aspects which affect privacy. There is a need to bring increased transparency, awareness and genuine disclosure methodologies.

- **Nation-State and the Multinational Internet Company:** While multinational giants exist in multiple areas like energy, Fast Moving Consumer Goods (FMCG), pharmaceuticals, media, etc., none wields as much power and attention as the internet giants. Most nations are unsure about regulations over the internet, and technological superiority offers these companies enormous leverage. Many governments depend on these platforms for easy roll out of programmes and to reach their citizens swiftly. In certain cases, these companies operate in the grey zone of laws, taxation and regulations. As awareness increases, instances of conflict in taxation, privacy, net neutrality and monopoly are emerging across the globe. Paradoxically, in this same environment, countries like China have created stringent checks and also created home grown alternatives, thereby, reducing their dependence on multinational companies. Since most nations cannot follow the Chinese model, there is a need for a more workable middle of the path approach. There is a need for all nation-states to proactively exert the right to privacy and data security of their own citizens. For internet companies to operate legally in a country, they should be made to enter into well analysed disclosure agreements and contracts with the necessary penal provisions. It would be a challenge to evolve such legally binding provisions in the amorphous digital world; however, government departments should pursue this serious requirement with alacrity. After the Christopher Wylie revelations, Facebook Chief Executive Zuckerberg was quick to testify in front of the United States

Countries like China have created stringent checks and also created home grown alternatives, thereby, reducing their dependence on multinational companies.

There is a need for all nation-states to proactively exert the right to privacy and data security of their own citizens. For internet companies to operate legally in a country, they should be made to enter into well analysed disclosure agreements and contracts with the necessary penal provisions.

Congress. Simultaneously, he refused to personally testify in front of the United Kingdom Parliament or the European Parliament, in spite of receiving multiple summons[5]. This contrast is significant as it denotes what binding and strong legal provisions can achieve.

- **Primacy of the Common Netizen:** "#DeleteFacebook", the Twitter hashtag created by concerned social media users and supported by Brian Acton, the co-founder of WhatsApp, has possibly caused greater consternation to Marc Zuckerberg, than all the summons to testify, received from various governments. During the fallout of the fake news and privacy scandals, Facebook stocks saw a sharp downturn, wiping out $ 100 billion of investors' money[6]. There are also reports in the United Kingdom that users could claim for compensation for the distress caused by the data breach. This could potentially cost Facebook more than its present worth[7]. While the internet has the potential to expose personal user data to legal and illegal manipulation, it has also given immense power of generating public opinion to the common netizen, primarily through the platform of social media. The internet-based behemoths, unlike the brick and mortar multinationals, depend to a great extent on acceptability and trust. Any report pertaining to a breach in trust spreads rapidly and it takes little effort on the part of the user to switch loyalties to a different service provider. In order to have a balanced partnership in the digital ecosystem, the common net user needs to recognise this immense power he holds. There is also a trend, which suggests the diminishing boundary between a cyber security professional, and the common man. As users of the global common digital space, every user has a stake in the security of data. It would be naïve to shift the complete onus of cyber security of an organisation to the handful of professionals handling the networks. Every netizen is a target and, hence, has a role to play in the fight. The day of the "internet dummy" is over.

While the internet has the potential to expose personal user data to legal and illegal manipulation, it has also given immense power of generating public opinion to the common netizen, primarily through the platform of social media.

The Indian Context

The number of internet users in India stood at 481 million in December 2017, and is expected to reach 500 million by June 2018[8]. There is, however, a huge urban-rural digital divide wherein 64.84 percent of the urban and 20.26 percent of the rural population is covered, as per data of December 2017. Interestingly, data pertaining to Facebook users shows that India claimed first place in the world with 270 million users, ahead of the United States with 240 million Facebook users. The Facebook-owned WhatsApp has 1.5 billion active users worldwide, of whom 200 million are in India[9]. The Facebook-owned Instagram has 59 million users in India, which puts it at number three worldwide[10], in terms of numbers. In spite of these large numbers, the social media-driven digital marketing industry in India is still in its infancy. According to a report on digital advertising by Dentsu Aegis Network, the Indian digital advertising industry, currently pegged at around Rs 8,202 crore, is slated to reach Rs 18,986 crore by 2010[11]. India is undoubtedly a massive market opportunity for the global internet giants. With 4G penetration set to explode, especially to the rural areas, the Indian opportunity cannot be ignored. It is time

It is time that India flexes its might and demands a better and equanimous deal for its citizens, which will address all privacy and security concerns.

that India flexes its might and demands a better and equanimous deal for its citizens, which will address all privacy and security concerns. It is also encouraging that in a few recent instances, an emerging assertion and determination at the national level is visible. The government came out strongly in favour of the net neutrality debate. In 2016, the Telecom Regulatory Authority of India (TRAI) barred differential pricing for data services, effectively prohibiting the rollout of Facebook's Free Basics platform[12]. The Indian government also came out strongly against Camridge Analytica and Facebook after the recent data breach reports, and has sought responses from the companies. The government has termed the initial response from Cambridge Analytica as "cryptic and evasive" and has served further notice[13].

Data Protection Laws in India

The Constitution of India does not patently grant the fundamental right to privacy. India also does not have any exclusive legislation on digital data protection and privacy. The Information Technology (IT) Act, 2000, and its amendments in the year 2009, were followed by the IT Rules, 2011. The IT Act has, over time, included provisions pertaining to "sensitive personal data or information of a person". However, the existing provisions are by no means exhaustive and do not address the ever emerging concerns of privacy in digital space. A burning need has been felt in India to have separate data protection and privacy, which matches up with world standards. Towards this, a White Paper drafted by a committee of experts headed by Justice BN Srikrishna, which was set up by the Ministry of Electronics and Information Technology, was published on November 27, 2017[14]. In 2012, a separate expert body under Justice

AP Shah, constituted by the erstwhile Planning Commission, came out with a comprehensive report and identified nine critical areas of citizens' privacy and data protection. The group was set up after concerns were raised about the impact on the privacy of individuals with the emergence of several national programmes such as the Unique Identification number, NATGRID, DNA profiling, Reproductive Rights of Women, privileged communications and brain mapping, most of which would be implemented through Information and Communication Technology (ICT) platforms[15]. Amidst the vibrant national debate on Aadhar and the rolling out of Aadhar-related government schemes, the Supreme Court of India, in a landmark judgement on August 24, 2017, ruled that Indians enjoy a fundamental right to privacy subject to certain reasonable restrictions and that it is intrinsic to life and liberty under Article 21 of the Indian Constitution. It is evident that the stage has been set for the promulgation of a new national data protection and privacy law in India. The challenge for the legislature is to draft provisions which can stand the test of obsolescence, in an area where technological advancements establish fresh rules of the game at a very fast pace.

The Supreme Court of India, in a landmark judgement on August 24, 2017, ruled that Indians enjoy a fundamental right to privacy subject to certain reasonable restrictions and that it is intrinsic to life and liberty under Article 21 of the Indian Constitution.

The Way Forward

While the new data protection and privacy law will be a welcome step, there is a pertinent need for the government to upgrade its own enforcement apparatus, educate its citizens, develop technical capabilities and create alternatives, if India and its citizens are to

The data protection and privacy model has to be India-specific, and not just a reproduction of the American or European models.

be treated as equal partners in the ecosystem. Market forces will drive global internet companies and the sheer magnitude of the Indian market, coupled with strong regulations, would ensure a better deal for its citizens. In order to leverage the advantages, there is a need for the nation to embrace digital inclusion and ensure that connectivity is provided to the furthermost citizen. In this age of social media, data protection cannot be achieved by isolation, technical security or cyber hygiene alone. Strong laws, enforcement and the implied risk of losing out on the India marketplace, would be the primary motivation for global internet multinationals to act as per national interests. The data protection and privacy model has to be India-specific, and not just a reproduction of the American or European models. Levels of education and awareness amongst citizens in India will take considerable time to reach advanced global standards; therefore, citizens cannot be expected to fight for their rights on all occasions. Cyber and data security lawyers and industry experts have indicated that millions of active Facebook and other social media users in India, could be at a far greater risk of user data breach and of giving away more information about themselves on social media platforms as compared to other markets like Europe or Singapore due to weak rules and a lax approach. Fragile rules and regulations for app developers, which do not explicitly require them to seek user permission and the rampant proliferation of the Andriod platform, coupled with unique social media habits, are factors, which place Indians at far greater risk[16]. In India, the government agencies have to be far more proactive, aware and alive to the infringement of the rights of the citizens and take up the fight against defaulting players.

Conclusion

The future India story appears positive, more by default than by design. Facebook has admitted that potentially 5.62 lakh people in India have been affected by the data breach incident. Compared to the 87 million who have been affected by the same incident in the United States and one million affected in the United Kingdom, the effect in India may seem comparatively less. There have been some reports of electoral manipulation even in India, but the evidence is not conclusive. Digital marketing through social media platforms has still not become the focus of the internet giants in India and, hence, the cumulative adverse effect is comparatively muted. The positive fallout of the Christopher Wylie revelations is that as a nation, India has been warned of the negative implications of individual data breaches, before getting adversely affected on a major scale. This warning which has ominously arrived at the cusp of the expected internet and data boom in India, will undoubtedly bring in greater awareness amongst the policy-makers, professionals dealing with privacy and security issues, and the common netizen. Looking forward optimistically, this should lead to a safer and secure digital ecosystem for India and its citizens in the years to come.

Digital marketing through social media platforms has still not become the focus of the internet giants in India and, hence, the cumulative adverse effect is comparatively muted.

Notes

1. https://www.britannica.com/science/ecosystem
2. https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/
3. https://m.timesofindia.com, Twitter also sold data to Cambridge Analytica researcher:Report, PTI, April 30, 2018.
4. https://economictimes.indiatimes.com, "WhatsApp CEO Jan Koum Quits Facebook Over 'Data Privacy' Concerns," IANS, May 01, 2018.

5. https://www.theguardian.com, Alex Hern and Dan Sabbah, “The Cambridge Analytica Files, Zuckerberg’s Refusal to Testify Before UK MPs ‘Absolutely Astonishing’,” EDT, March 27, 2018.
6. https://globalnews.ca, Jessica Vomiero, “Facebook Has Lost $100 B in Value - And Its Money Problems May Just Be Beginning,” March 27, 2018.
7. http://metro.co.uk, Jimmy Nsubuga, “UK Facebook Users Could Get £12500 Each After Data Breach, March 28, 2018.
8. https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june
9. https://financialexpress.com.FE Online, February 01, 2018.
10. https://www.statista.com/statistics/578364/countries-with-most-instagram-users/
11. https://economic times.indiatimes.com, Gaurav Laghate, ET Bureau, January 16, 2018.
12. https://thehindu.com, Yuthika Bhargava, “TRAI Rules in Favour of Net Neutrality,” February 06, 2016.
13. https://timesofindia.com, “Data Breach: Government Again Sends Notices to Cambridge Analytical, Facebook,” April 25, 2018.
14. https://www.livemint.com, Parag Mathur, “What the Upcoming Data Protection Law Means,” January 17, 2018.
15. https://www.gktoday.in/gk/nine-point-code-by-the-justice-a-p-shah-panel/
16. https://economictime.indiatimes.com, Anumeha Chaturvedi and Gulveen Aulakh, “Indian Social Media Users More Prone to Data Breach,” ET Bureau, March 29, 2018.