E-MAGAZINE

VOLUME 2

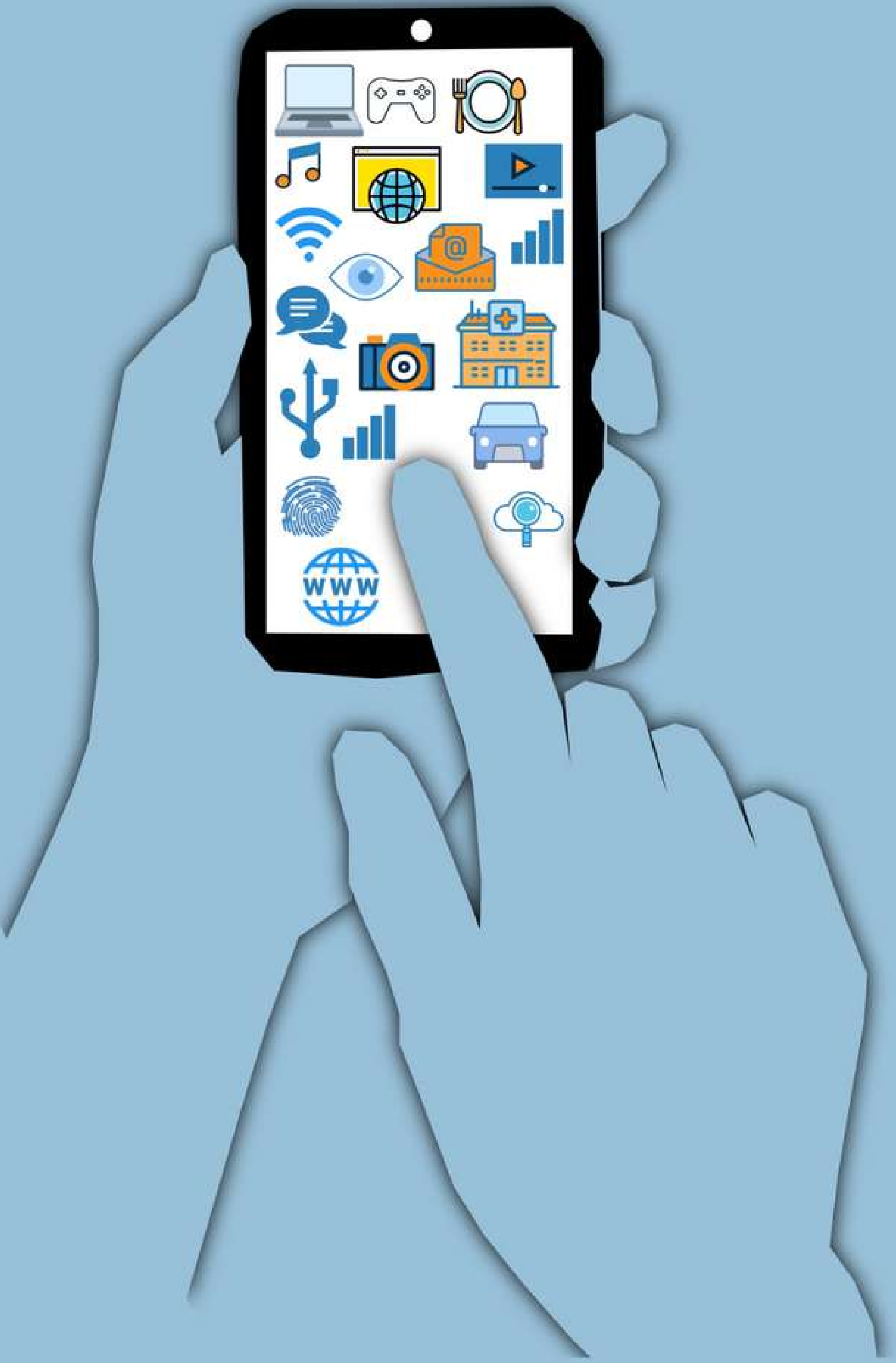
HERITAGE LAW COLLEGE

DIA-LA(W)-GUE

DIGITISATION AND BREACH OF PRIVACY

Campus: Chowbaga Road,Anandapur,P.O.
East Kolkata Township,Kolkata- 700107
Ph: 8420193533/03366270575,
Fax:+913324430455
Email: admin@hlc.edu.in
Website: www.hlc.edu.in

DIA-LA(W)-GUE



FROM THE FACULTY AND STUDENTS OF HERITAGE LAW COLLEGE

EDITORIAL BOARD

DESIGN TEAM

- **TRIDIBESH DASGUPTA**
  8th Semester
- **SUBHANJANA ROY**
  6th Semester
- **UPAYAN CHAKRABORTY**
  6th Semester
- **ARGHAJYOTI BAGCHI**
  6th Semester
- **SOUPAMA SEN**
  4th Semester
- **SUVAM DASGUPTA**
  4th Semester

FROM THE EDITORS' DESK

Hello Everyone!

This is indeed a special moment for all of us at the Heritage Law College. We are honored to announce the launch of the second edition of our vibrant E Magazine Dia-law-gue on the theme DIGITIZATION AND BREACH OF PRIVACY.

The rapid growth in the popularity of the digital media which definitely had made life endurable for most of us especially during the pandemic, has, however, many a flip side to it and needs to be handled in a judicious and prudent manner. This edition of our E Magazine contains an array of exhaustive articles and evocative artwork from the young intellectuals analyzes the enormous responsibility of all technological empowerment and the informative section reminds us to be always watchful of the fundamentals of technological computing.

We are thankful to our brilliant design team, who has labored hard to compose the resplendent and elegant layout for this edition. As always, we are indebted to all such spirited minds whose creative sparks help us to ward off the ennui of continuous curricular instruction and at the same time quadrate with the demands of intensive academic objectives.

Let them soar higher and higher with blessings from all!!!

Cheers!!!

TABLE OF CONTENTS

ENSURING PRIVACY IN A DIGITAL AGE

TRIPARNA CHAKRABORTY

Digitalization is the conversion of analog information into texts, photographs, voices, and among others, through electronic devices such as scanners or specialized computer chips. Information is organized into bits which can be separately categorized into bytes. This serves as the binary data that computers can process. Digitalization is done to process, store, and transmit the information through digital circuits, equipment, and networks. Now due to digitization, it is easier to access, preserve, and share information. It is a process of converting everything into digital format, which ultimately aims to ease lives. But nowadays digital privacy has increasingly become a topic of interest. It is often used in contexts that promote advocacy on behalf of individual and consumer privacy rights in e-services and is typically used in opposition to the business practices of many e marketers, businesses, and companies to collect and use such information and data. Digitalization is, not surprisingly, driving up user data privacy concerns. Business need to take protective actions or regulators will step in. Increasingly, users are taking steps to control their own data. Information and data shared over the social web have continued to become more and more commoditized; the users of socialmedia are now considered unpaid 'digital labors', as one pays for 'free' e-services through the loss of their privacy. All of the

information and data one shares is connected to clusters of similar information. As the user continues to share their productive expression, it gets matched with the respective cluster and their speech and expression are no longer only in the possession of them or of their social circle. This can be seen as a consequence of bridging social capital. As people create new and diverse ties on social networks, data becomes linked, and thus this decrease of privacy continues. For example, between 2005 and 2011, the change in levels of disclosure for different profile items on Facebook show those, over the years, people want to keep more information private. Again; as per a report from the Federal Trade Commission, less than 10,000 households could generate 150 million data points every day. With the onset of contemporary technologies, we are unknowingly storing our private data in hundreds of devices.

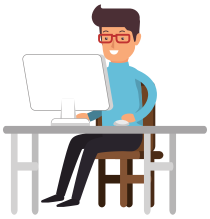
It is the responsibility of companies to use consumer's data responsibly, but it is also their accountability to use the services wisely. Besides changing own passwords for all devices, one should follow a lean publishing practice, switching off all devices when not in use, adopting VNP services, avoiding malicious browser e tensions and transitioning from just user to smart user. Some Laws allow filing a case against breach of digital privacy. In 2007, for instance, a class-action lawsuit was lodged on behalf of all Facebook users that led Facebook to close its advertising system "Beacon." In a similar case in 2010, the users sued Facebook once again for sharing personal user information to advertisers through their gaming application. Laws are based on consumers' consent and assume that the consumers are already empowered to know their own best interest. Therefore, for the past few years, people have been focusing on self-management of digital privacy through rational and educated decision-making.

A STUDY OF PRIVACY IN THE INDIAN CONTEXT

SOUPAMA SEN

We live in a digitalized society, where we can access any kind of information related to persons, things or places within a click. However, this rapid digitization has proved to be a major hurdle for privacy issues. Privacy means the protection of sensitive personal information of an individual which the individual feels not to be disclosed in the public domain. The pandemic has proved to be a booster for the digitalized world where online operations have increased significantly. With the increased number of online users, it also increased the high risk for online scams involving stealing of data.

Digitization brings huge value to any business exposure. We all are using various banking apps, pharmaceutical apps education apps on the basis of our requirements. To use them, there is certain mandatory information which needs to be provided like user name, address, contact number, medical details, KYC details, bank details etc. Now the only question is whether these details are secure from any kind of cyberattack. However, recent cyber attacks on Indian start-ups like Big Basket, Just Dial, Unacademy has raised serious question regarding the state of data protection not only in our country but also in the global context. Not only start-ups but also global IT giants like Facebook and LinkedIn had faced a massive cyber-attack. Recently in April 2021, the data of Facebook was leaked which put the users' data in a



compromising position. More than 532 Million users' data out of which 6 Million were Indians were made available on a low level hacking forum. One of the vulnerabilities is identity theft for which an individual can suffer financial loss, can have reputation damaged or suffer emotional distress. From a password breach to email or social media to stolen credit card number, banking details, misuse of passports these vulnerabilities can become catastrophic.

We all remember the incident of the AAdhar Card which occurred in our country in 2018 and affected more than 1.1 Billion users. Now Right to Privacy is a Fundamental Right and an integral part of Article 21 that protects Life and Liberty of the citizens. However, India has not yet enacted any specific legislation on Data Protection. The Information Technology Act, 2000, deals with cyber crimes and safety and involves several Sections that deals with online frauds, data breaches and outlines the guidelines to be followed by corporate bodies while handling the customers'/clients' sensitive data. This Act had undergone certain changes and resulted in the Information Technology (Amendment) Act, 2008, and added Section 43A which deals with implementation of reasonable security practices for sensitive personal data and provides for the compensation of the person affected by wrongful loss and wrongful gain and Section 72A which provides for imprisonment for a period up to three years and a fine up to Rs. 5,00,000 for a person who causes wrongful loss or wrongful gain by disclosing personal data of another person. We are now in the year 2022 and there is a need to have a comprehensive Data Protection Act which will protect the users from cyber crimes and data stealing. Apart from that a user should be made aware of various forms of cyber crime so that he does not fall prey to the vicious dark web and suffer from unnecessary harassment and mental anguish without any fault on his part.

CYBER SECURITY IN A NUTSHELL

AYUSH TALUKDER

Corporations who use data mining techniques in order to more accurately target their products and services sometimes compromise the privacy of the consumers they wish to court. Entire enterprises have been created and sustained by the private sector's desire to market goods and services to the specific demographic that most closely matches their "ideal consumer." While in most cases the pursuit and use of this information is legal, there can be no denying that it compromises the privacy of the consumer, whether they know their privacy is being compromised or not.

Currently, there are specific laws governing the protection of digital privacy. In the age of the digital economy, data is the new currency of the 21st century. Lots of applications have no revenue generation, but their only benefit is data. This business model of the Internet is called Surveillance Capitalism, where all social media apps and other such platforms make their money collecting data on users and monetizing on that. Companies such as Google, Facebook, and Amazon have all built empires atop the data economy. Apart from Surveillance Capitalism, the majority of the world's consumer data is with few digital companies like Google, Facebook, and Amazon that dominate online search, social media and online retail, respectively. Thus, their market power creates an imbalance for new market players. In the process, both

producers and consumers of data are hurt, resulting in twin problems of data privacy and net neutrality.

We are in an information age and information of all kinds is just a few clicks away. The information explosion has manifold advantages but also some disadvantages. Over the last decade there has been a substantial increase in the amount of data that is generated through the usage of various electronic devices and applications. In nearly everything we do; data surrounds us and is produced. States are utilizing technology in the most imaginative ways particularly in view of increasing global terrorist attacks and heightened public safety concerns. One such technique being adopted by States is profiling, which involves automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences interests, reliability, behaviour, location or movements Data is generated not just by active sharing of information, but also passively, with every click on the internet. Social network providers, search engines, email service providers, messaging applications are all further examples of non-state actors that have extensive knowledge of our movements, financial transactions, conversations both personal and professional, health, mental state, interest, travel locations, fares and shopping habits.Thus, there is a need for protection of such information which the users are not willing to share. It requires

appropriate action by the state and legislative intervention so that the privacy of the users is maintained.

Now Right to Privacy is a fundamental right and an intrinsic part of Article 21of the Indian Constitution that protects the life and liberty of the citizens and as a part of the freedom guaranteed by Part III of the Indian Constitution. This landmark decision was held in Justice K.S. Puttaswamy v. Union of India led by a nine-judge bench on 24th August 2017, by giving a unanimous verdict, affirming that the Constitution of India guarantees to each individual a fundamental right to privacy. However, India has not yet enacted any specific legislation on data protection. The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha on December 11, 2019.

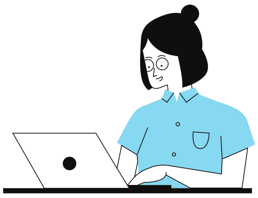
The right to privacy is a fundamental right. It protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices. It is rightly expressed that the technology has made it possible to enter a citizen’s house without knocking at his/her door and this is equally possible both by the State and non-State actors. It is an individual’s choice as to who enters his house, how he live,s and in what relationship.

IMPACT OF DIGITIZATION ON PRIVACY

SUPARNA CHAKRABORTY

Digitalization is the key to success. Data is power in a fast moving world, which is not restricted and can be easily broken through. It answers several questions and makes our life simpler but it has several cons as well. Everything becomes "publicly visible "and the social media, which is a platform for us to express our views, now discusses controversial issues and personal issues. Today, almost everything has become digitalized. Now, in order to withdraw money from the bank, one does not need to physically go to the bank rather, they can do so by pushing some buttons on their smart phones. However, this has created several problems and leads to an enhancement in the rate of cyber crime and fraudulent activity.

If a person visits a beautiful place, instead of enjoying the grandeur of the place, she becomes busy in makings videos and reels to post on the social media. Nevertheless, he does not realize that, at the end of the day, they lose their privacy. The world witnessed one such incident in the case of Sandhya Organic Chemicals Private verses United Phosphorus Limited Anr and Others. Similarly, most of the cyber crime cases arise out of it. During the pandemic, most of the schools and colleges had online classes across the globe but this definitely affects privacy. Most of the children who belong to middle-class families live in a two BHK apartment and thereby, carry on their online classes in a limited space as a result, cannot possibly maintain absolute privacy.



Digitalization also creates fear in the minds of an individual as they are in constant fear of being watched by CCTV cameras. CCTV cameras are for our own safety but when they are installed within one's house, one need to think twice before making any action. Not just the common people but even celebrities are prone to this. For instance, the media shows every single incident of a renowned public figure and some people enjoy this but they fail to realize that it leads to their breach of privacy. Unfortunately, women are prone to this issue as some people portray women in a terrible manner and most of the poor people fail to take a stand against this. Some people misuse this power of data for the fulfillment of their selfish desires. For instance, while a communication happens between two people and one shares his or her live – location then it does not remain restricted to two people only.

Rather, hackers tap such information by their IP Address and take out relevant information like saved card details and make fake calls in the name of banks. Some people are so gullible and ignorant that they land up sharing such information with hackers as they do not read the relevant messages of the banks. The only solution to this problem is to use the digital platform judiciously and in a controlled manner. We simply cannot afford to be irresponsible enough to allow machines and digitalization to overpower us. The sites should be made more secure. The only reason for which the company "Apple "enjoys monopoly in the digitalized market is because its privacy policies are the best and very tough to crack. If such features are used by other companies as well and social media apps use such policies then breach of privacy can be avoided.

INDULGENCE OF DIGITIZATION IN THE CONTEMPORARY ERA

PALAK KARWA

In the present times, we are all living in a digital world where everyone is interconnected. Digitisation means converting data or information into digital format which is essential for e-communication and e-governance escalating user data privacy concerns. Businesses need to take protective actions or regulators will step in. Increasingly, users are taking steps to control their own data.

In today's technological world generally, privacy means data privacy or information secrecy. Every individual's data should be protected and should not be used without the consent of the individual. Main purpose of data privacy is to protect any technology driven app or platform or portal user from unwanted cyber risks or threats. Now our society is very much dependent on various online portals or platforms, such as banking apps, insurance apps, pharmaceutical apps, food delivery apps etc. While using the services of these platforms or apps users must share some very critical personal data, which includes contact details, banking details, credit card no and many more. But the concern is whether these critical or sensitive data are actually stored in a safe or secured server or not. If any kind of casualties takes place who will be responsible and just to protect the interest of individuals or entities from any data breach the concept of data privacy is introduced

Digitization brings a huge value to any business exposure. With the help of digitization various business worlds merged and brought the new knowledge into the board room, which added additional value to the business. There is a very common online security question, whether these online portals such as banking, insurance, pharmaceuticals are actually safe or not? If any of these accounts are hacked, hackers can find out a lot more personal data which are generally sensitive in nature. With the help of this data any hacker can easily create an artificial or fake identity of the actual user and later on these could create havoc in the society or in the corporate world. Hackers can try to use this information to get more sensitive information from that user and then that will lead to targeting the user in a more destructive manner, which includes financial damage as well. One of the latest practices is any stolen digital information can be sold to the dark web and hackers can get a handsome amount but selling personal data in the dark is more fatal in nature from the users' point of view.It's a technological advancement which has raised concern about internet privacy. One of the latest examples is the advent of the Web 2.0, which has caused social media profiling. Web 2.0 is the system that facilitates sharing and collaboration of participatory information through the Internet from social media websites like Facebook, Myspace etc. If data is collaborating, sharing and interconnecting with various platforms at that time data leakage or cyber-attack can be more dangerous. During the pandemic in 2020, every corner of the globe all industries had severely impacted. After that everyone was running behind digitization and this transition phase opened the gateway for cybercriminals who were able to target vulnerable victims in the healthcare industry, banking & insurance industry, education industry or many other industries. According to IBM Remote work during COVID-19 increased data breach costs in the United States by $1,37,000.

DIGITIZATION: THE ROOTS TO BREACH OF PRIVACY

SANANDA CHATTERJEE

We all are living in a digital shell nowadays, where everyone is interconnected. Living in a time when digitization is everywhere is an experience in itself. Digitization is the process of converting data or information into a digital format which is essential for e-communication & e-governance. In modern times using of digital technologies or running towards digitization has transformed global business models. While we like to focus on the positive impacts of new technology implementation on business operations, the challenges of such an initiative cannot be overruled.

One of the major challenges is undoubtedly trying to navigate complex data privacy regulations as operations are moved online.

Among the many concerns and risks that have arisen from digitization – the biggest one is related to the one matter that is the most scary to all of us, our privacy. We live in a digitalized world, a world where we can access the information of any person, thing, or place within a click. This rapid digitalization proves to be a major hurdle for privacy issues. In today's technological world generally, privacy means data privacy or information secrecy. Every individual's data should be protected and should not be used without the consent of the individual. The invasion of our privacy, especially in the digital age, is becoming a bigger risk by the minute, even though there are plenty of security options and programs that have been created to protect us. Unfortunately, the rise of the popularity of social networks created a platform where a lot of personal information and data is shared, and therefore left to be exposed to various threats ranging from a password breach on our emails, to stolen credit cards, misuse of passports and IDs. The vulnerabilities that we face are endless. Our very known, WhatsApp was introduced in 2010 and was acquired by the global tech giant-Facebook in 2014, arguing that its privacy policy will remain unchanged. On January 2021 WhatsApp announced its new privacy policy which has led to a lot of controversy. According to the new policy WhatsApp users would not have the option to opt out of their data being shared with Facebook.In this digital and interconnected era, businesses are increasingly transacting directly with consumers through digitizing operations. This gives businesses access to data analytics that can help them discover new insights with regard to its clientele. As result, data breaches are becoming very common.

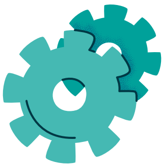
The pandemic had adversely affected the industry houses all across the globe. Due to obvious reasons, everyone was after digitization during this period and this transition phase opened the gateway for cybercriminals who were able to target vulnerable victims in healthcare, banking & insurance, education industry and many other sectors. Though some level of protection is provided by The Information Technology Act (2000) and the Personal Data Protection Bill, (2019) which primarily focuses protection of the privacy of an Individual, it is imperative that a user should be made aware of the immense value of data in these days so that they do not fall prey to cyber crime without any fault on his part.

THINK BEFORE YOU CLICK

SAMIMA JASMINE

We live in a word which is a digital shell connecting almost everything. Digitization means converting data or information into a digital format which is indispensable for e-communication & e-governance. Also, digitization is essential for any data processing, data storage and data transmission around the world. In these times, digitization has led to the rise of global business models like Zoom, Amazon, Facebook, WhatsApp, Swiggy, etc which have generated tremendous revenue and business opportunities. But do we really know how WhatsApp makes money? After a decade full of technological revolution, it is now known that they do so by selling our data to the advertisers. But what is alarming is the degree of our privacy at risk.

Our society has become dependent on various online portals or platforms for banking, insurance, pharmaceuticals, food delivery, etc. While using the services of these platforms or apps, users end up sharing some very vital personal data, which consists of contact details, banking details, credit card number etc. But the issue lies whether this critical data is secure in their server or not.Most of the internet services and information is free because the user is the product in this case. Our personal and professional data, every decision we take on the web is tradable with other service providers. The primary source of revenue for internet service providers is selling our activity information to advertisers. Your full name, phone number, pictures, emails, or any data that

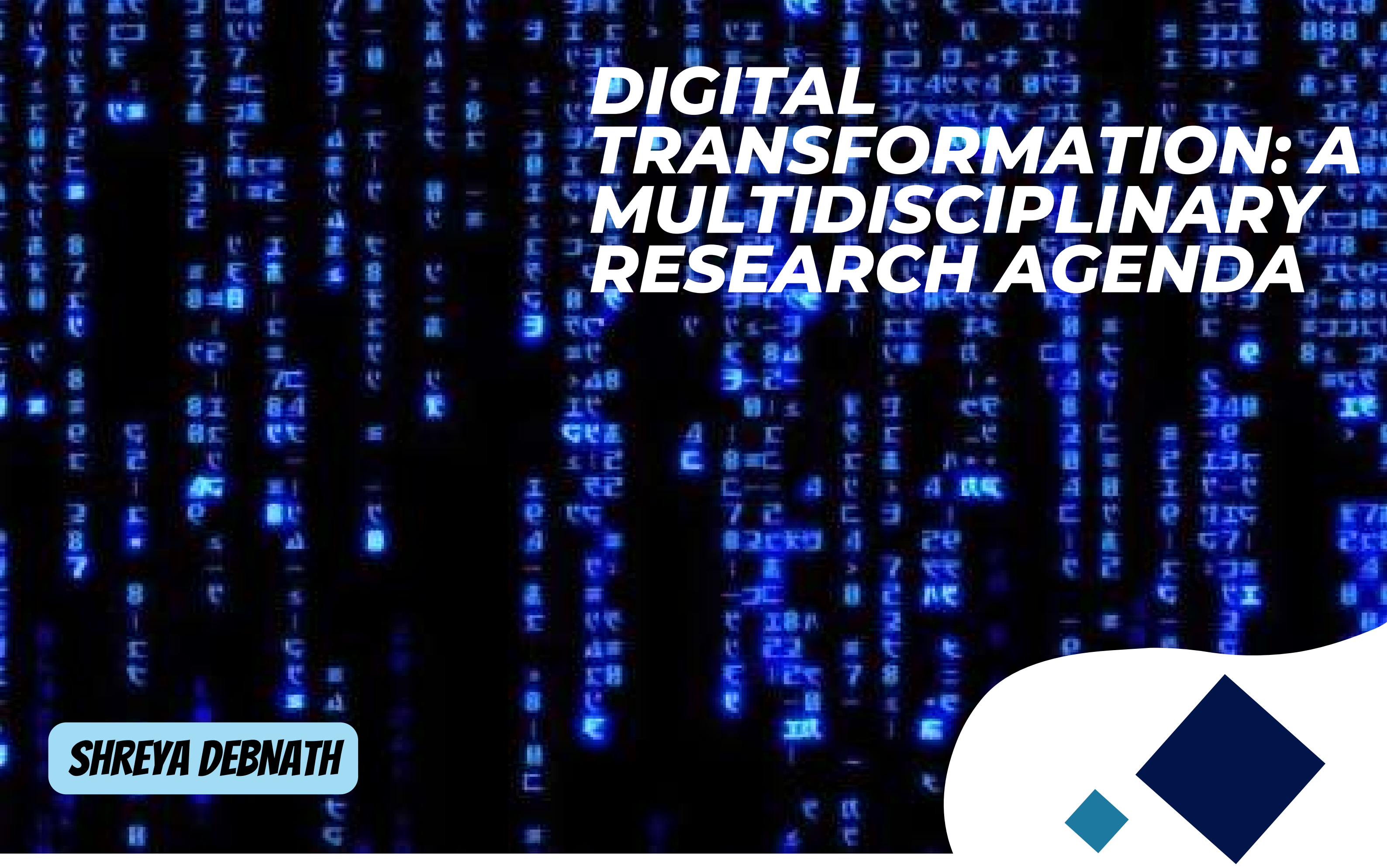


you digitize is of great value to advertisers. Even if you take vital steps to safeguard your data, it still gets exposed some way or the other. From the product page on any public forum like Facebook, Amazon, etc. that you looked into for some time or your consumer behaviour, all of it is up for sale to the advertisers. It is dreadful to realize how much Google or Facebook know about us. Moreover, e-commerce platforms such as eBay and Amazon are latent threats since they have our banking information. Imagine the number of times you surpassed the Terms & Conditions page. There are two sets of users – one those who had no idea about the risks and others who can't resist the attraction of trying the latest app despite privacy breach risks.

Depending on the type of data involved, the consequences can include destruction or corruption of databases, the leaking of confidential information, the theft of intellectual property and regulatory requirements to notify and possibly compensate those affected. These types of information attract the attention of third parties for whom the data has value. Personal, financial and health information can be sold and used for marketing, fraud and identity theft. Intellectual property can be sold and used to develop products and services similar to those of your business. Competitive information can be sold and used by your competitors to block your plans and leaked legal information may damage your legal position. Data on IT security is a valuable target in itself because it lets the unauthorized parties gain access to all the other types of information on your system.

We are all digitized and it's hard to escape the web. The idea is to control the amount of data we produce and follow all privacy protocols. Besides changing passwords for all devices and platforms frequently, we should adopt the following measures for achievement of better data protection. First, we should follow a lean publishing practice. There is really no need to publish without any purpose. Secondly, we should switch off all devices when not in use. We should ensure that all the devices connected to the web are completely switched off when not in use. Thirdly, we should use VPN as much as possible as VPN provides a gateway to access data prohibited in your region, they come with undeniable security and privacy risks. Fourthly, we should avoid using malicious browser extensions. Users should be more cautious while enabling extensions on Google Chrome or Microsoft Edge as these modern browsers give developers the right to ask users' permissions.

The biggest threat to digitization is not only the cyber threat in itself but an inability to build a sufficient technological deployment and failure to develop safe communication or data sharing internally within the organization. Those organisations that will have effective technology will be in better position for their continued growth. But organisations who are in vulnerable position for digital or cyber security will expose their organization to risks with potential calamitous implications. Organizations or entities should take a comprehensive inventory of potential cyber risks, quantify their potential impact, and prioritize them effectively.



DIGITAL TRANSFORMATION: A MULTIDISCIPLINARY RESEARCH AGENDA

SHREYA DEBNATH

Digitization essentially means to convert the data or information into any digital format which is essential for e-communication & e-governance. Digitization is required for any data processing, data storage, and data transmission in a borderless world. In modern times usage of digital technologies has transformed global business models (Cloud tech-driven platforms i.e., Airbnb, Swiggy, Zoom & Amazon) and has become really helpful for producing new business opportunities.

With every passing day, people are getting more inclined and more reliant on digitization. Digitization, however, results in creating a huge risk of a cyber breach. Many applications require in-app payments to access its features. Those apps generally require details such as name, address, contact details, and bank details.

We do not know where this information is stored and whether or not it is secure. Many people also fall into traps because of fraudulent messages. WhatsApp forwarded messages, or messages generally saying 'You have won Rs 1crore' are too common, and any person who is not properly aware of the fraudulent nature of such messages becomes vulnerable only by a single click.

The primary enactments which deal with the protection of data are Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and

Procedures and Sensitive Personal Information) Rules, 2011.The IT Rules imposed additional requirements on commercial and business entities in India relating to the collection and disclosure of sensitive personal data or information. It included various new rules that required companies and organizations which process personal information to obtain data owners' written consent before undertaking certain activities. Previously the IT Act, 2000 had undergone certain changes which were introduced by the Information Technology (Amendment) Act, 2008 and added section 43A and 72A to the Act. Section 43A deals with implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain. Section 72A provides for imprisonment for a period up to 3 years and or a fine up to Rs. 5, 00,000 for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract.

Technology has progressed in leaps and bounds we need to change laws according to that.

In February 2021 an application was filed in the case of Karmanya Sareen v. Union of India which challenged this new privacy policy based on the contention that privacy protection standards being followed in India are much lower than those being observed in European countries which amounts to a sheer discrimination for its Indian users. The Supreme Court has issued notice to the parties and asked them to file their replies.

In conclusion we can say that laws should be changed as and when necessary keeping in mind that technology is an ever growing field and all technological advancements carry the responsibility of cyber security and data protection.

DIGITIZATION MEANS DEATH OF PRIVACY?

BISWADIP GHOSH

Digitization means converting data or information into a digital format which is essential for e-communication & egovernance. Also, digitization is required for any data processing, data storage and data transmission in a borderless world. Digitization brings a huge value to any business exposure. Let's come to a very common day to day digitization impact, e.g. we all are using various banking, pharmaceutical or educational applications basis our requirements. Whenever we try to use any of the above-mentioned apps, there are some mandatory information which must be provided, such as name of the user, address, email id, contact no, medical details, KYC details, bank details etc. Now the matter of concern is whether these users'digital information is kept secure or not.

Hackers can try to use this information to get more sensitive information from that user and then that will lead to target the user in more destructive manner, which includes financial damage as well. One of the latest practices is any stolen digital information can be sold to the dark web and hackers can get handsome amount. During the pandemic on 2020, everyone was after digitization and this transition phase opened the gateway for cybercriminals who were able to target vulnerable victims in the healthcare, banking & insurance, education and other industries.The biggest threat to digitization is not only the cyber threat in itself but an inability to build a sufficient technological deployment and also failure to develop safe communication or data sharing both within and outside the organization . Evolution of digital and cyber technology is an ongoing process and thus the process ofidentification of cyber or digital threat along with the rectification of the same should be a constant process.

MENACE CAUSED DUE TO PRIVACY IN DIGITIZATION

ANKITA DUTTA

The use of digitization has been tremendously accelerated especially in the last two years. Thus it is essential to maintain digital privacy so that the users' security can be preserved and their information is not disclosed to any strangers. The word digitization refers to converting non–digital structures into digital representations.

Where there is a breach of privacy, the individual will be hesitant in using the internet in a free and unimpeded manner. As more and more information gets online placement, there is an increased danger of hackers and other malicious agents mishandling the data and thereby leading to the compromise of personal privacy. In some cases, data is outright stolen.

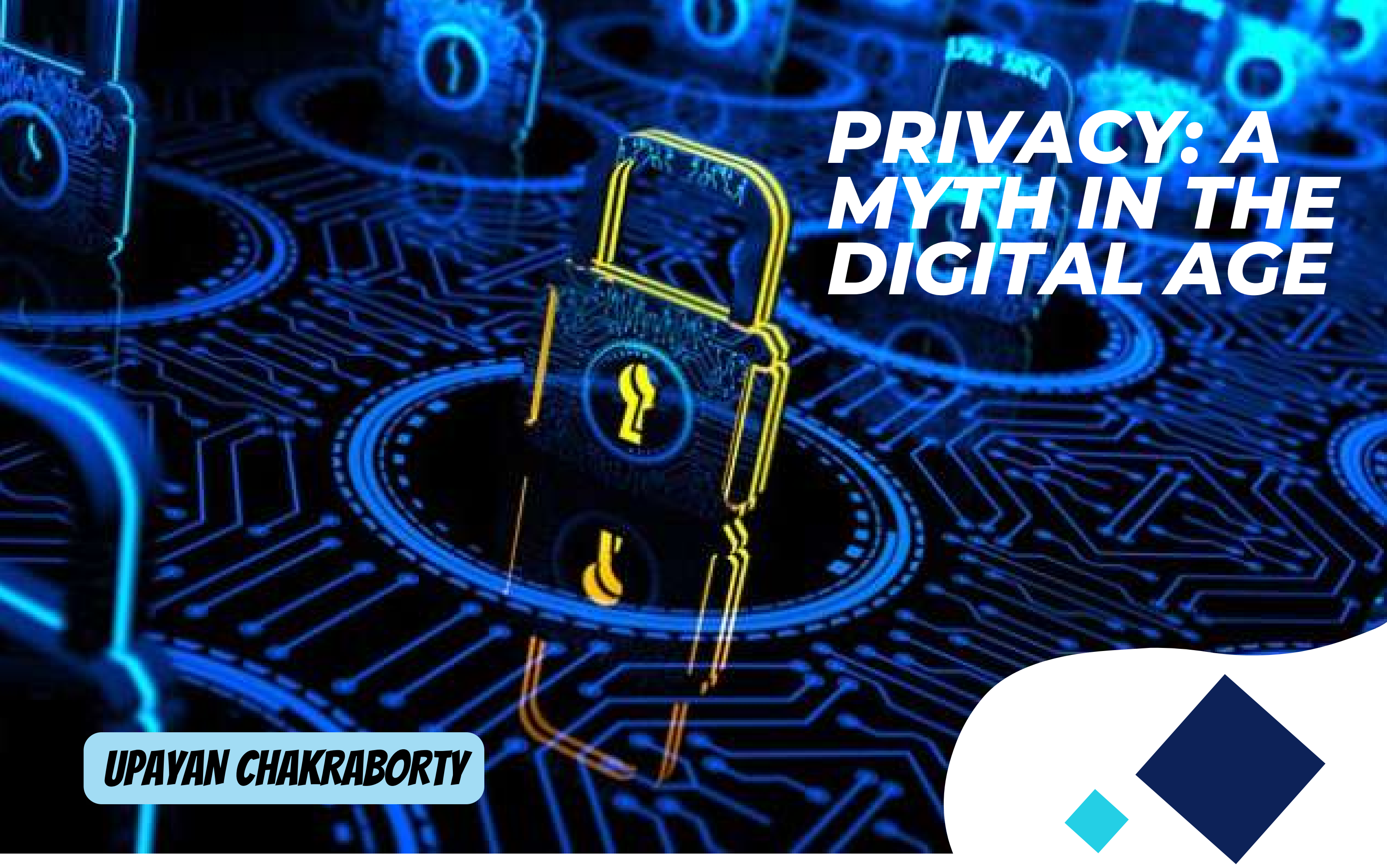
Sometimes, online criminals target social networking sites because these sites are a mine of personal information. Digitization is helpful because we are dependent on various online platforms for a number of services that online applications render but the situation may turn adverse when privacy is breached while using these apps.

India has not yet enacted any specific legislation on data protection. There is an urgent need for the protection of information that users are not willing to share. It requires appropriate action by the state and legislative intervention so that the privacy of users is maintained. Facebook one of the commonly used apps tracks its users across the web by using tracking cookies. If a user is logged

in to Facebook and also browses other websites, Facebook can track the sites they are visiting. Facebook tries to control data security issues security by offering privacy controls by limiting the parties from using the posts of its users.

In order to boost our online privacy, the usage of the volume of personal data may be restricted. This can protect our financial and personal information while we visit social media, news, and entertainment sites. Providing a huge quantity of information makes it easier for cybercriminals to obtain identifying information which would allow them to steal our identity or access our financial information. Sometimes, we fall into a trap by clicking on a phishing link that takes us to a spoofed webpage that looks like a homepage of a bank or financial institution. Once we put our account information it becomes easier for the scammers to infringe our privacy. So, we should be very careful before clicking on any kind of unknown and strange link.

All the software that we use is regularly updated as updates contain advanced protection systems and safeguards against the latest malware. Antivirus software should be installed on all devices and especially on those systems from which financial transactions are carried out. This software keeps hackers from accessing our personal or financial information or tracking our location. Thus we are dependent on digitization in different ways but it may turn out to be a veritable nightmare if our privacy is infringed. We should remain conscious of the processes through which individual privacy may be infringed upon and adopt proper measures so that we can safely enjoy the benefits of digitization in an uninterrupted manner.



PRIVACY: A MYTH IN THE DIGITAL AGE

UPAYAN CHAKRABORTY

As our technology is updating, we are getting more dependent on the digital world. Now a day it is really easy to pay our bills, make payment, transfer funds etc. just sitting at home and by just one tap. The way technology is making our life easier, in the same way we are putting our privacy on risk. Now as we are speaking about digitization it is really important for us to know what actually this term means? Digitization is the method involved with changing over data into a computerized design. The outcome is the portrayal of an item, picture, sound, report or sign (generally a simple sign) acquired by creating a progression of numbers that depict a discrete arrangement of points or samples. How does WhatsApp bring in cash? The greater part of us have clashed with the income model behind most internet providers cheerfully permitting us to involve their space for driving borderless correspondences. Following 10 years brimming with innovation developments, it is at long last uncovered that tech programming and even equipment producers offer our information to sponsors. What the vast majority of us actually don't know is how much our security is under danger. So if you thought that only the website browsing activity was public, then you know less,your complete name, telephone number, pictures, messages, or any data that you digitize is of worth to any publicist out there. Regardless of whether you have set the entrance settings to 'private', your specific contacts may not see it yet the stage can. No matter what your assent, individual data is supposedly presented to numerous offices.It is shocking to acknowledge the amount Google and Facebook have any familiarity with us. You might have failed to remember your most loved bistro you checked in yet they haven't. Simply check your Google and Facebook Ad settings where your own data is populated of course. Additionally, web based business stages, for example, eBay and Amazon are possible dangers since they own our financial data. Notwithstanding 'end-to-end encryption' guarantees, our credit card distributed on auto-fill structures ought to caution.Hence, there is a requirement for insurance of such data which the clients are not ready to share. It requires fitting activity by the state and official intercession with the goal that the security of the clients is kept up with and furthermore to decide the degree to which it very well may be essentially attacked. Hence, it would not be inappropriate to say that in the current situation right to privacy of the residents happen as a restriction on the powers of government as well as other non-state actors. Presently Right to Privacy is an essential right and an inherent piece of Article 21 that safeguards life and freedom of the residents and as a piece of the opportunities ensured by Part III of the Constitution. This landmark decision was held in Justice K.S. Puttaswamy v. Union of India led by a nine judge bench on 24th August 2017, by giving a consistent decision, insisting that the Constitution of India assurances to every individual a major right to privacy. However, India has not yet enacted any specific legislation on data protection.The essential authorizations which manage assurance of information will be Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal

Information) Rules, 2011 (otherwise called "IT Rules"). The IT Rules forced extra necessities on commercial and business elements in India connecting with the assortment and revelation of sensitive individual information or data.It included different new standards that necessary organizations and associations which process individual data to get information proprietor's composed assent prior to undertaking specific exercises. Beforehand the IT Act, 2000 had gone through specific changes which were presented by the Information Technology (Amendment) Act, 2008 and added section 43A and 72A to the Act. Section 43Aarrangements with execution of sensible security rehearses for sensitive Personal information or data and accommodates the compensation of the individual affected by unfair loss or wrongful gain. The Sensitive individual information or data as alluded in the arrangement incorporates passwords, monetary data, (for example, financial balance or credit card details), physical, physiological and emotional well-being condition, sexual orientation, clinical records and history, biometric information. Section 72A provides for imprisonment for a period up to 3 years and or a fine up to Rs. 5, 00,000 for a person who causes wrongful loss or wrongful gain by disclosing Personal information of another person while providing services under the terms of lawful contract. Under rule 5 of the IT Rules, 2011 any Body Corporate or individual for its benefit will not gather any private information or data except if it is gathered for a legitimate reason concerning any utilitarian action of the body corporate and that assortment of such data is important for that reason. Further, the individual whose data is shared should be made aware of the fact that the data is being gathered, the reason behind it, the planned beneficiaries of such data, the name and other subtleties of the agency gathering the data and the organization holding the data. Whatsapp-Facebook Privacy Issue: There are different specialist organizations having business in India for giving correspondence by connecting with private discussions and sharing media and different information. Whatsapp is one such cell phone application that is exceptionally well known in India. Whatsapp was presented in 2010 and was procured by the worldwide tech giant Facebook in 2014, contending that its protection strategy will stay unaltered. In 2016, changes in Whatsapp protection strategy were declared under which the record data of Whatsapp clients will be imparted to Facebook. An appeal was documented under the watchful eye of the Supreme Court against this changed security strategy because it encroached the right to protection of the clients after the choice of the Delhi High Court which permitted the data shared through Whatsapp to be accessed under its new security strategy. The Court, notwithstanding, coordinated Whatsapp to erase the information, until 25th September 2016, of clients who decide to erase the application as well as clients who decide to hold the application on the portable phones. In January 2021 Whatsapp declared its new protection strategy which has begun part of discussions. As per the new approach Whatsapp clients would not have the choice to quit their information being imparted to Facebook. In February 2021 an application was recorded on account of KarmanyaSareen v. Association of India which tested this new security strategy in view of the conflict that protection insurance norms being continued in India are a lot of lower than those being seen in European nations which adds up to a sheer separation for its Indian clients. The Supreme Court hosts gave notice to the gatherings and requested that they document their answers. Whatsapp, in view of grave analysis have stretched out the cut-off time to refresh till May 15, 2021. The matter is being tended to by a three judge bench which comprises of Chief Justice of India SA Bobde, and Justices AS Bopanna and V Ramasubramanian.The right to privacy is a basic right. It is a right which safeguards the inward circle of the person from obstruction from both State, and non-State entertainers and permits the people to settle on independent life decisions. It is appropriately communicated that the innovation has made it conceivable to go into a citizen's house without thumping at his/her entryway and this is similarly conceivable both by the State and non-State entertainers. It is an individual's decision with respect to who goes into his home, how he resides and in what relationship.

The security of the home should safeguard the family, marriage, procreation and sexual orientation which are extremely significant parts of pride. If the person grants somebody to go into the house it doesn't imply that others can go into the house. The main check and equilibrium is that it ought not to hurt the other individual or affect their freedoms.

VIOLATION OF PRIVACY: A CRITICAL APPRECIATION WITH RESPECT TO INDIA

SUBHANJANA ROY

Man is generally found to be possessive by nature and he used to keep his belongings such as valuable documents, treasures, etc. in a secretive place by inventing gullible methods in order to protect and prevent the intruders or strangers from getting access to. Now with the advent of science and technology, one tends to uplift himself and utilizes this very technology to meet his needs and for the sake of convenience. Like the other side of a coin, this technology with whom he befriends, betrays him like another Mir Jafar as all his private and personal information may go into the wrong hand and ultimately renders him haplessly helpless. Privacy of a woman's physical body has been taken care duly by the Indian Penal Code1 (*1) but technically, law remains handicapped when digital privacy is hampered, violated and may become a novel tool for exploitation. Through this article, the writer attempts to discuss the intricacies of digital privacy by putting emphasis upon its breach and violation.

Digitization deeply includes and involves the conversion of information into its digital format (i.e. computer-readable). The result is the depiction of an object, image, sound, document or usually an analogue signal obtained by generating a sequence of numbers that describe a distinct set of points or samples. It is called digital representation or, more precisely, a digital image, for the object, and digital form, for the signal. Nowadays, digitized data appears as binary numbers which makes processing easier through digital computers and other operations. The concept of digital privacy is best described in terms of protecting the information of citizens who use digital platform. However, when people speak about digital privacy, they often refer to it when it comes to the use of the Internet. However, digital privacy is based on the fact that the use of digital media to conduct business, either personally or professionally, can leave digital footprints. For example, many Internet users are unaware that their information and their Internet usage patterns are constantly being recorded and stored. The Internet Protocol (IP) address of a computer can be traced back to a particular user and, as such, its website browsing patterns can be monitored. Information like the date and time of one's use and access, what browser he used for accessing websites and even how long he accessed the websites may be kept on a search engine's server.

Following the terrorist attacks in Mumbai, the Information Technology Act was duly amended in February, 2009. Section 69 of the Information Technology Act, 2000 allows the designated government agency to track and collect data on Internet traffic, Information created, transmitted, received and stored on a computer. It also requires security agencies to shut down websites. The government allegedly requested email, chat, Voice-overInternet Protocol (VoIP) and Black Berry service providers to provide security agencies with real-time access to communications within their networks. The government also established a technical group to review the matter. However, generally, the State's intent behind any form of surveillance is in the national and public interest. A hacker could take control of one's computer and turn it into a "bot" through which countless illegal activities such as spamming, scamming online shoppers and attacking wellknown websites may be carried out. India is now the largest spam-producing country. Prohibiting the production and invention of technologies for this purpose is going to be very difficult. Laws should be dynamic enough to suit the need of time. It should mingle with the modern technology so that unauthorized use of such deceiving technologies is proscribed. Types of Data Breaches Generally, there are three different kinds of data breaches—a) physical, b) electronic, and c) skimming.

They all share the same level of risk and impact, but are unique when it comes to enforcement. They require measures such as document shredding or electronic media destruction services to maintain data security. A physical breach includes the physical theft of documents or equipment containing account information, such as cardholder receipts, records, personal computers and POS (Point of Sale) systems whereas an electronic breach is an unauthorized access or deliberate attack against a system or network environment in which cardholders' data is processed, stored or transmitted and thirdly, Skimming involves capturing and storing magnetic stripe data on the back of credit cards. This process uses an external device that is sometimes installed at a merchant's POS without them being aware of it. Skimming may also involve a dishonest employee using an external device to gather magnetic stripe data from the card. These identity 'thieves' gather and collect information and use it to create false credit and debit cards.

The need for privacy continues to advance with the passage of time, where images and personal information can be readily accessible to others, indefinitely. Data breaches and other cybercriminals are intruding in our life and making our life miserable by harming millions of people whose personal information is being plundered by fraudsters. It's not just the nightmarish process of erasing one's name and credit history, or fighting for credit or loans, housing, jobs, or medical services after a breach. Victims often suffer silently from feelings of helplessness and vulnerability. Sleep is disrupted due to disturbed thoughts. The energy levels of the victims go down abysmally. They medicate themselves with alcohol, drugs and food so that they remain oblivious from such disturbing thoughts. For some, the after-effects are more serious and they often undergo episodes of depression and anxiety, or post-traumatic stress.6 Status of right to privacy under the Indian Constitution The sacrosanct Indian Constitution clearly does not recognize the fundamental right to privacy. But the apex court has interpreted the right to privacy as part of other existing fundamental rights i.e. 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. The most recent landmark Supreme Court decision in K.S. Puttaswamy vs Union of India7 declaring privacy to be an integral part of fundamental rights subject to the satisfaction of some criteria and benchmarks. Privacy as a human right by virtue of International Conventions Guaranteeing a person's right to privacy continues to be a challenge to a nation's political system as privacy can sometimes hamper the investigative process. The right to privacy has therefore always been recognized as a right guaranteed by the Universal Declaration of Human Rights(UDHR) 1948. Article 12 of UDHR states that “no one shall be subjected to arbitrary interference with his privacy, everyone has a right to the protection of the law against such interference or attacks.” The wider interpretations of the said Article of UDHR totally fit into the periphery of an individual’s right to privacy along with certain limitations set by the government following the principle of due procedure established by law. Similarly, the privacy of individuals has also been recognized as a civil and political right under the provision of Article 17 of ICCPR (International Covenant on Civil and Political Rights). A historic 2017

ruling by the Supreme Court of India affirming the right to privacy as a fundamental right under Article 21 of the Indian Constitution was correlated with the two clauses mentioned above to which India is a signatory. Applicable Laws The only shield that protects citizens from privacy violations is the law along with awareness. At present, India has no direct laws governing data protection or privacy. However, the pertinent laws dealing privacy in India are the Information Technology Act, 2000, the Indian Penal Code,1860 and the Copyright Act, 1957. The Information Technology Act, 2000 is India's primary legislation on issues of technology law and aims to address compensation-related issues (civil) and punishment (criminal) in the event of unlawful disclosure and improper use of personal data and breach of contractual conditions relating to personal data. There are certain provisions of the Information Technology Act, 2000, (*2) which affect privacy. It should also be noted that a provision of the Information Technology Act, (*3) which is an exception to the general rule of maintaining the privacy and secrecy of information provides that the government or any of its agents specifically authorized by the government, if satisfied that it is necessary or appropriate in the interest of the sovereignty or integrity of India, the defence of India, and State security, friendly relations with foreign States or public policy or to prevent incitement to the commission of any cognizable offence relating to above or to investigate any offence, for reasons that must be documented in writing, by order, may order any governmental agency to Intercept, monitor or decipher any information that is produced, transmitted, received or stored within a computer resource. Since computer based data is included within the ambit of literary work (*4) of Copyright Act,1957, therefore copying of such database will invite infringement of copyright acts culminating in punishment. However, the parties to a contract may voluntarily include the appropriate clauses in a contract they enter for protection of data like confidentiality clause and obligation to maintain confidentiality. Certain provisions mentioned in the Indian Penal Code (*5) also provide protection to the privacy of individuals by explicitly defining certain acts as punishable crimes. Conclusion What is necessary is that the enacted law should be updated in a technical way and implemented properly by involving high-level technologically competent minds. If it is not done, then the possible consequences are that the evil will prevail, the wicked and the spooks will have the last laugh and unfortunately, the mighty law will remain a paper tiger.

REFERENCES:

*1 Section 354C

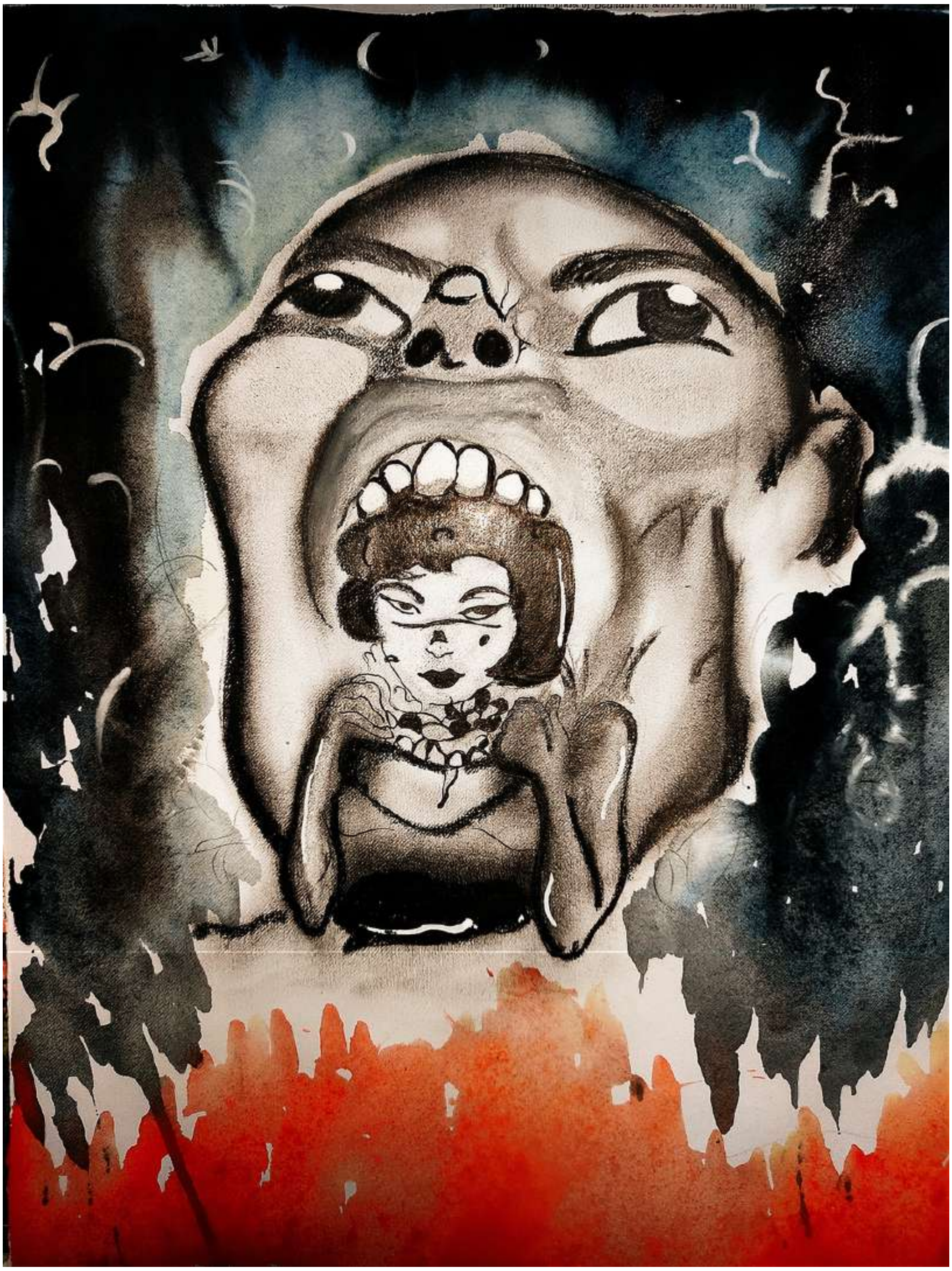
*2 Section 43A (Compensation for failure to protect data), Section 72 (Penalty for Breach of confidentiality and privacy), Section 72A (Punishment for disclosure of information in breach of lawful contract), Section 66C (Punishment for identity theft) ,Section 66D(Punishment for cheating by personation by using computer resource), Section 66E (Punishment for violation of privacy), Section 67 (Punishment for publishing or transmitting obscene material in electronic form), Section 67A (Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form) ,Section 67B (Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form

*3 Section 69

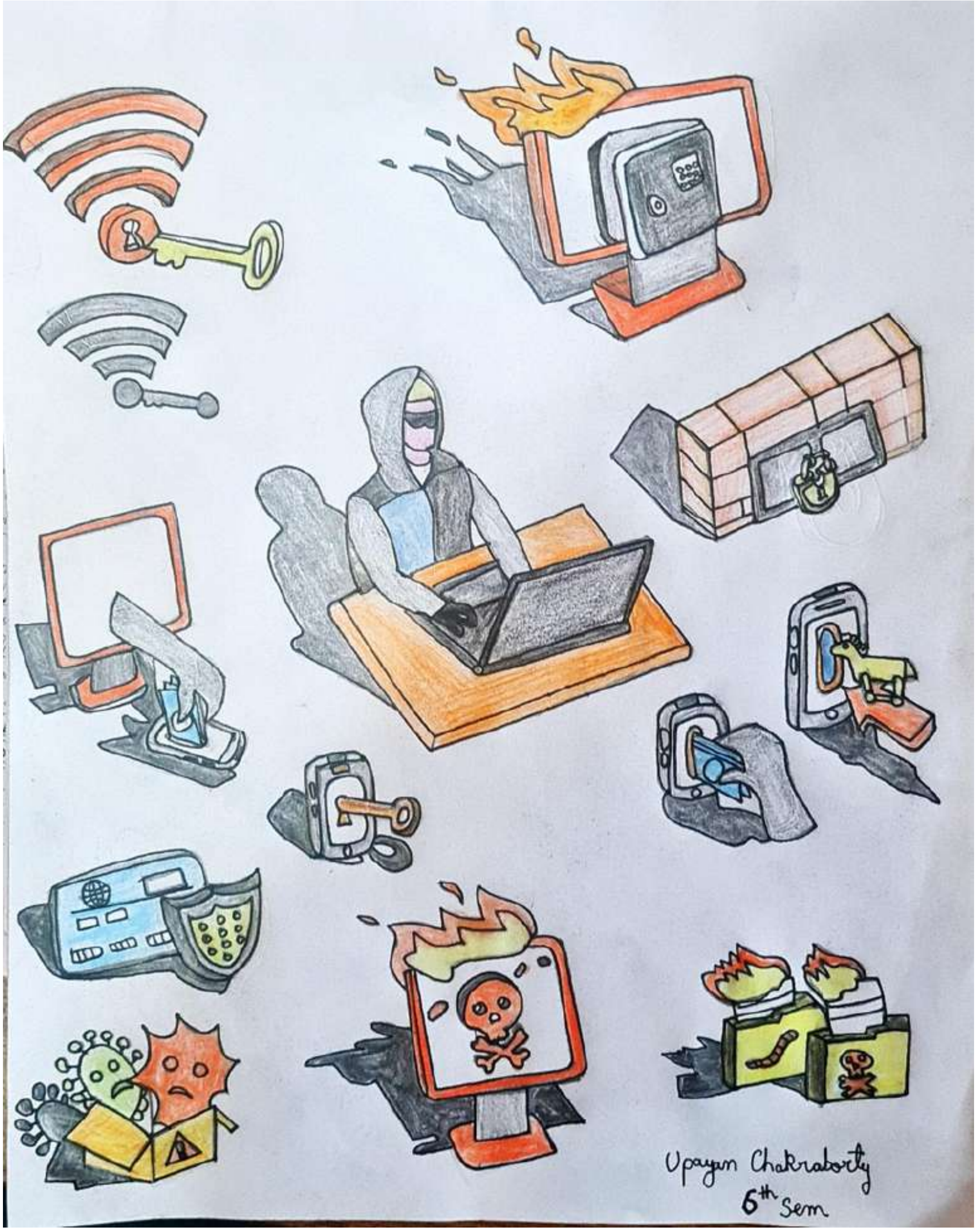
*4 Section 2(O)

*5 Section 354C. (Voyeurism), Section 354D (Stalking), Section 228A (Disclosure of identity of the victim of certain offences, etc.), Section 499 (Defamation)

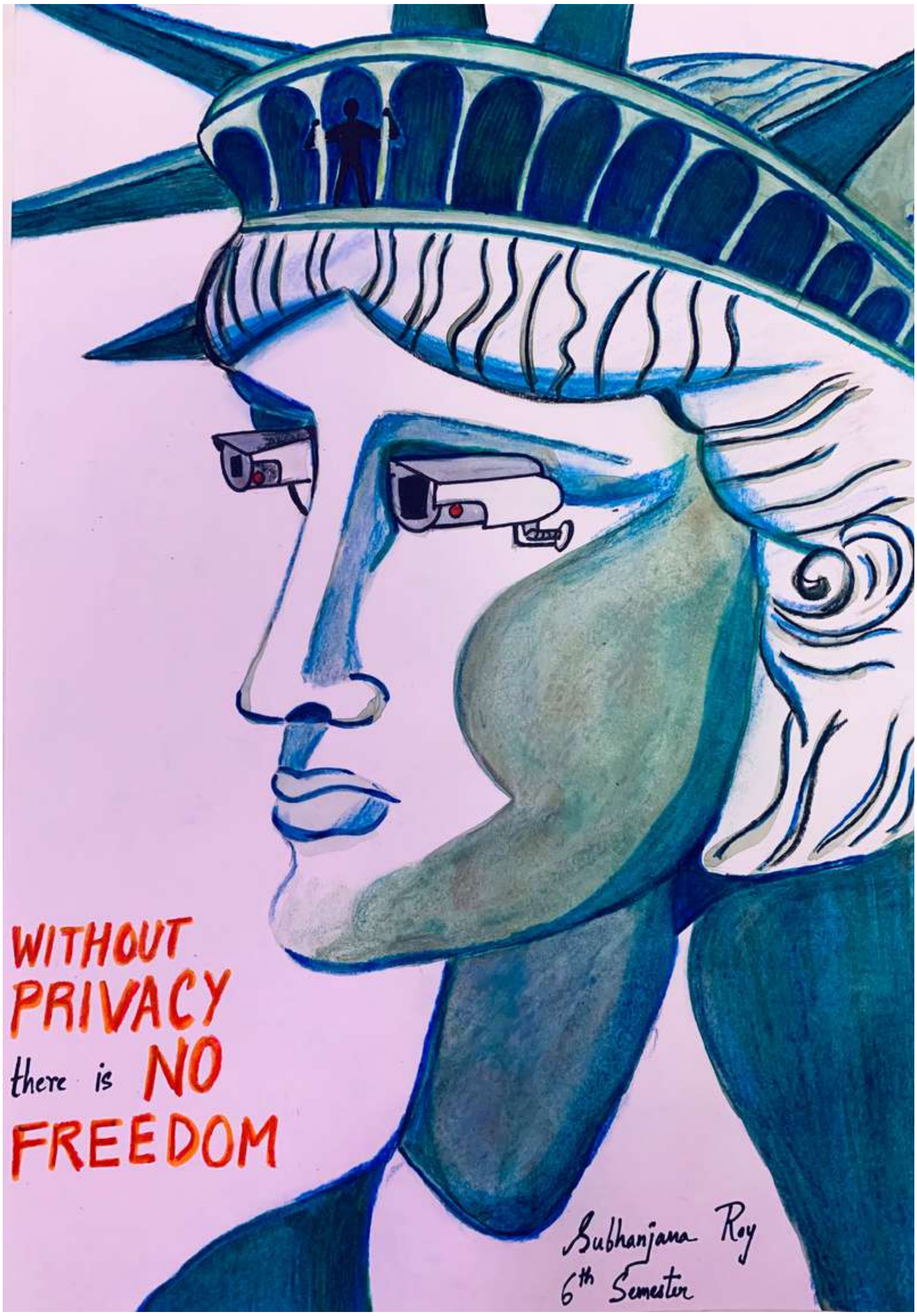
IMAGE GALLERY



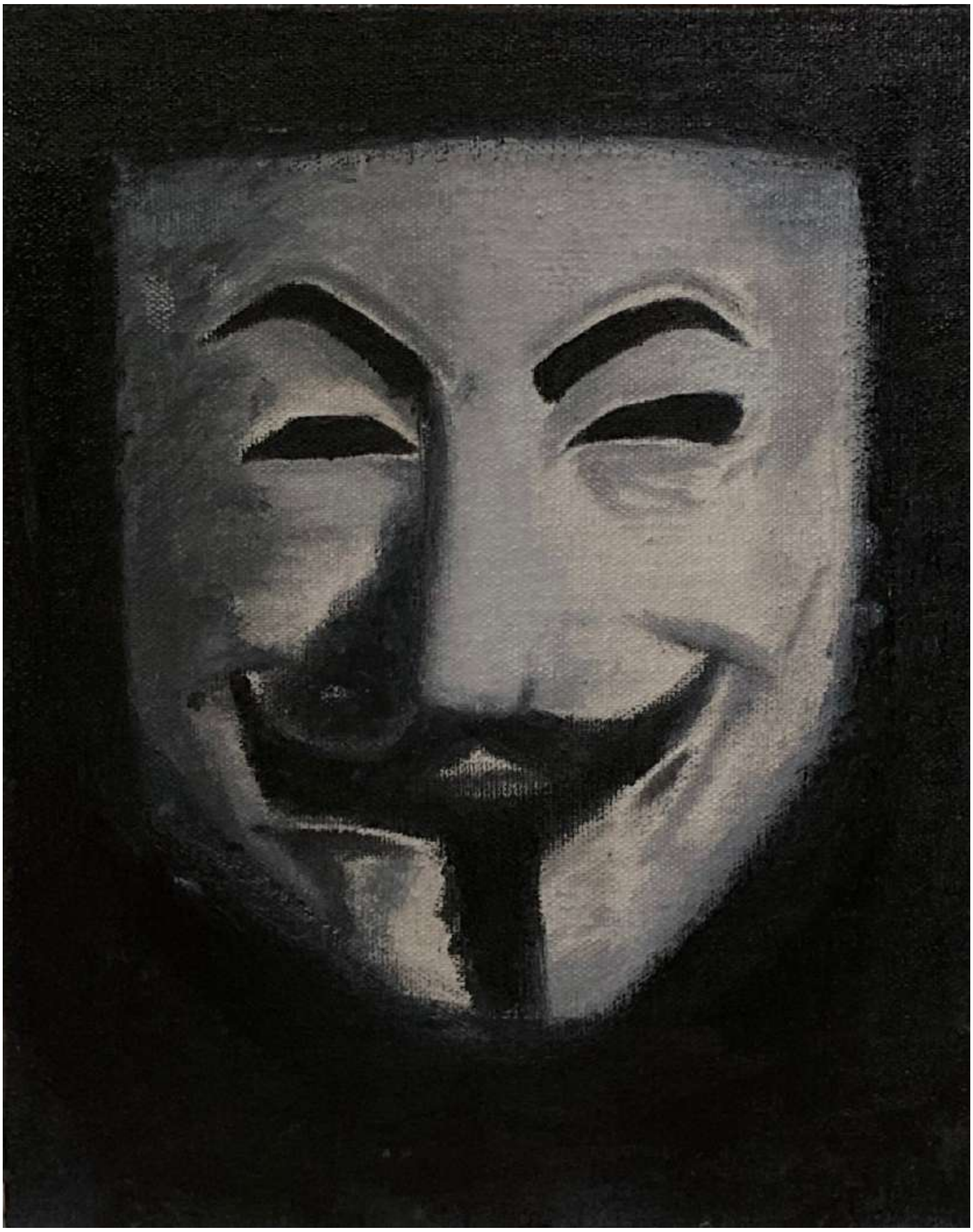
ANANYA DE



UPAYAN CHAKRABORTY



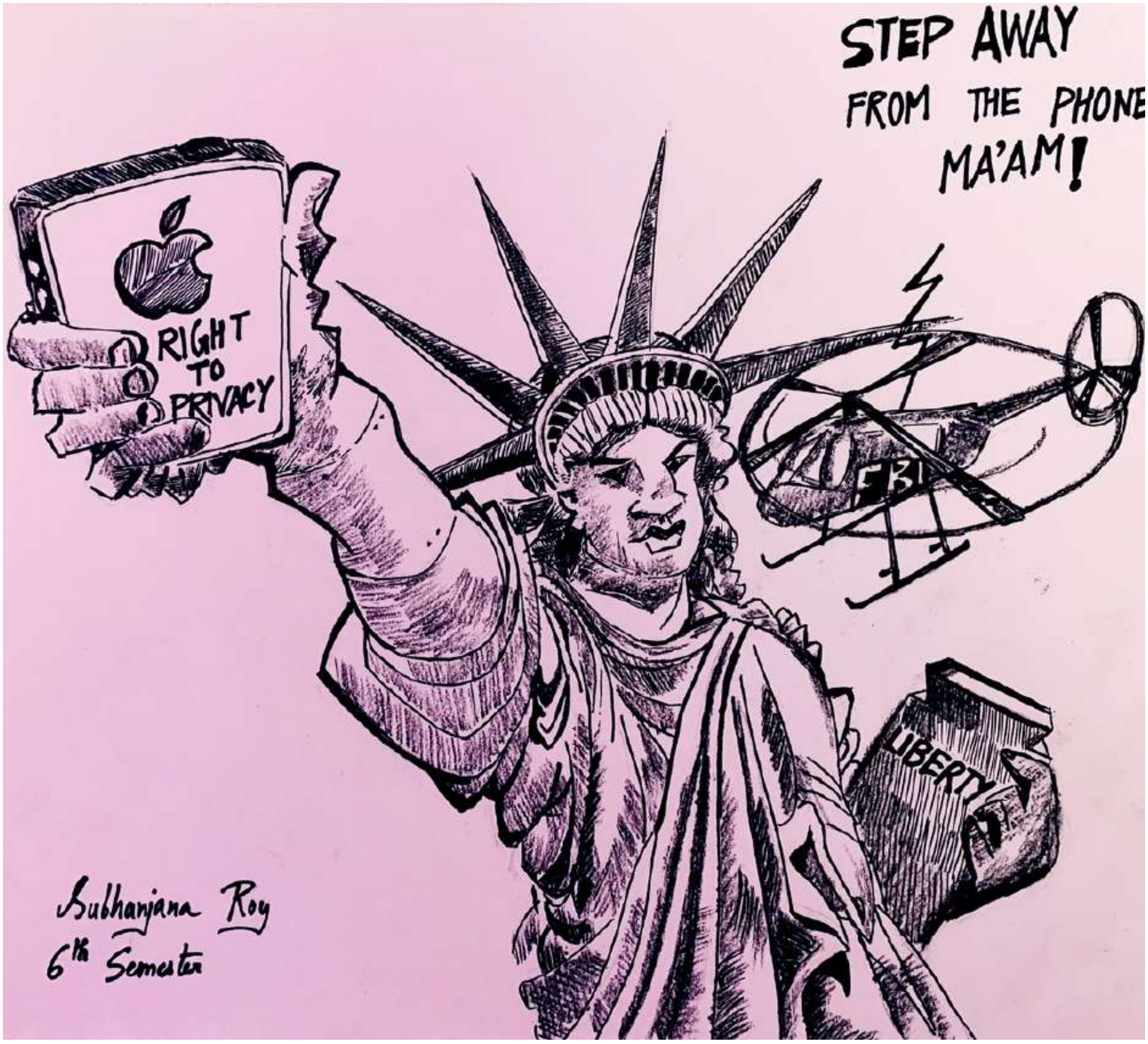
SUBHANJANA ROY



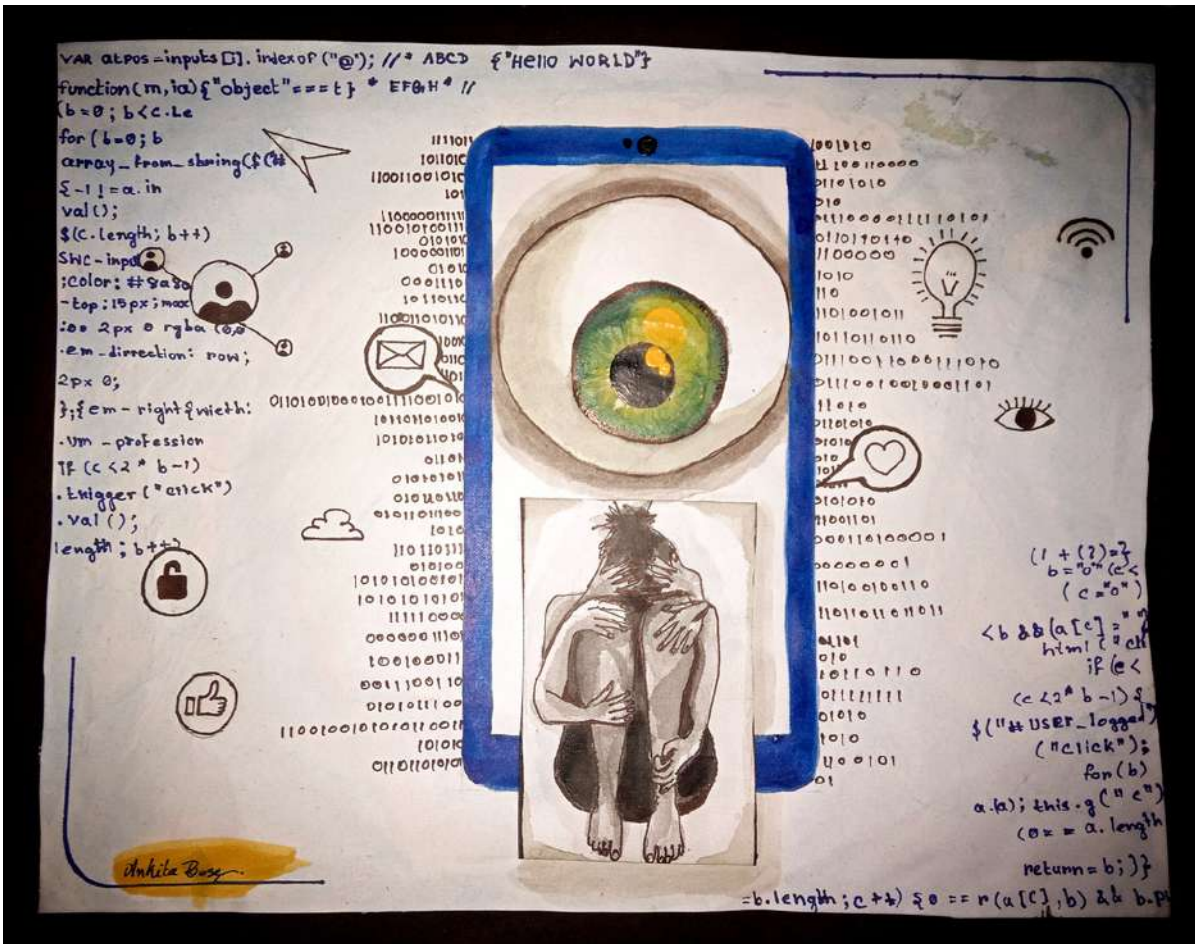
AFREEN AZAD

http:
www
G+
http:
G+
www
FRAUD CRIME FAKE
HACKER DARK WEB
PRIVACY
DARK WEB
FRAUD CRIME
FAKE HACKER
DARK WEB
PRIVACY
FRAUD CRIME FAKE
HACKER DARK WEB
PRIVACY FAKE CYBER
CRIME
CYBER CRIME
FRAUD CRIME
FAKE HACKER
DARK WEB
PRIVACY

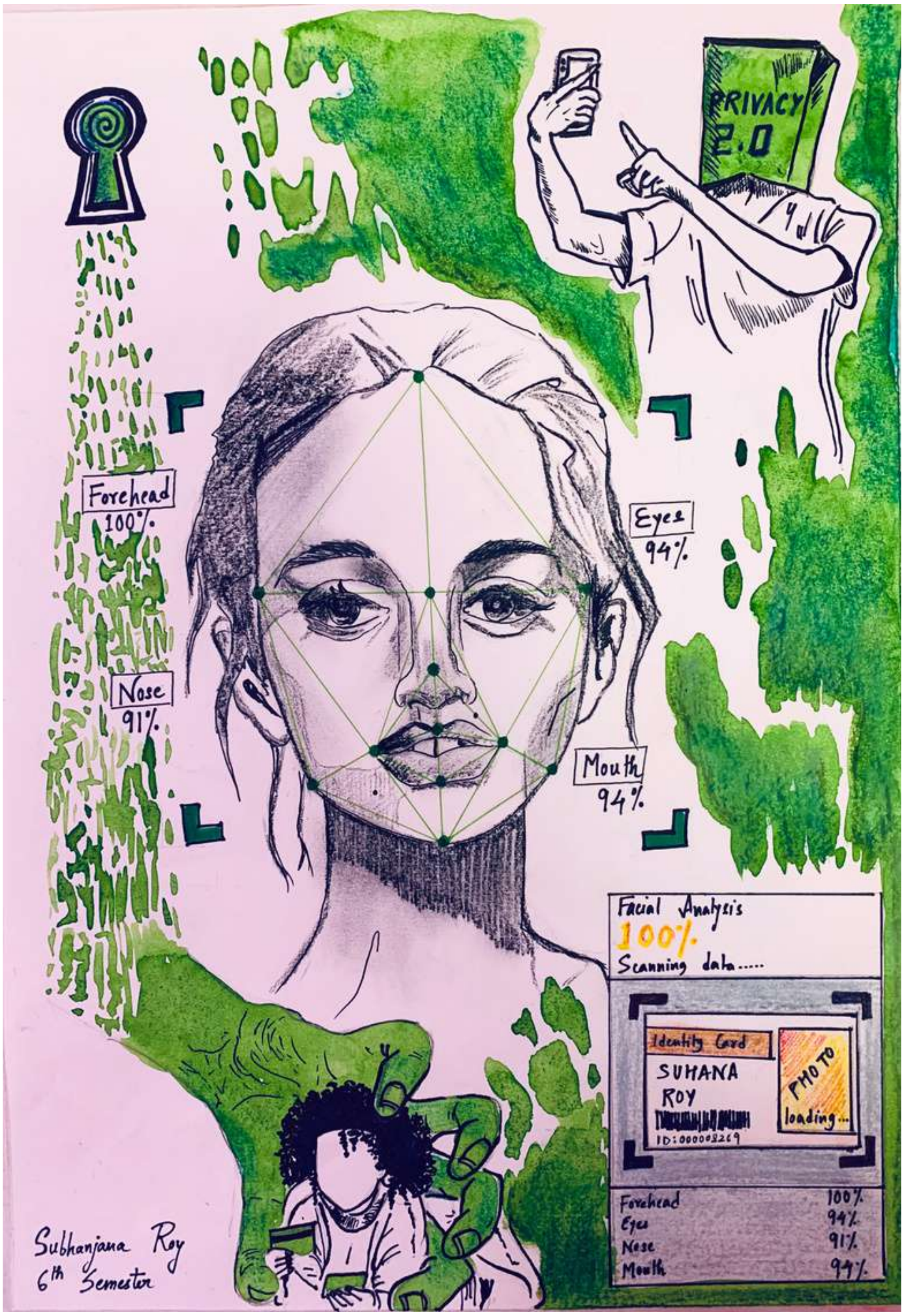
SOUPAMA SEN



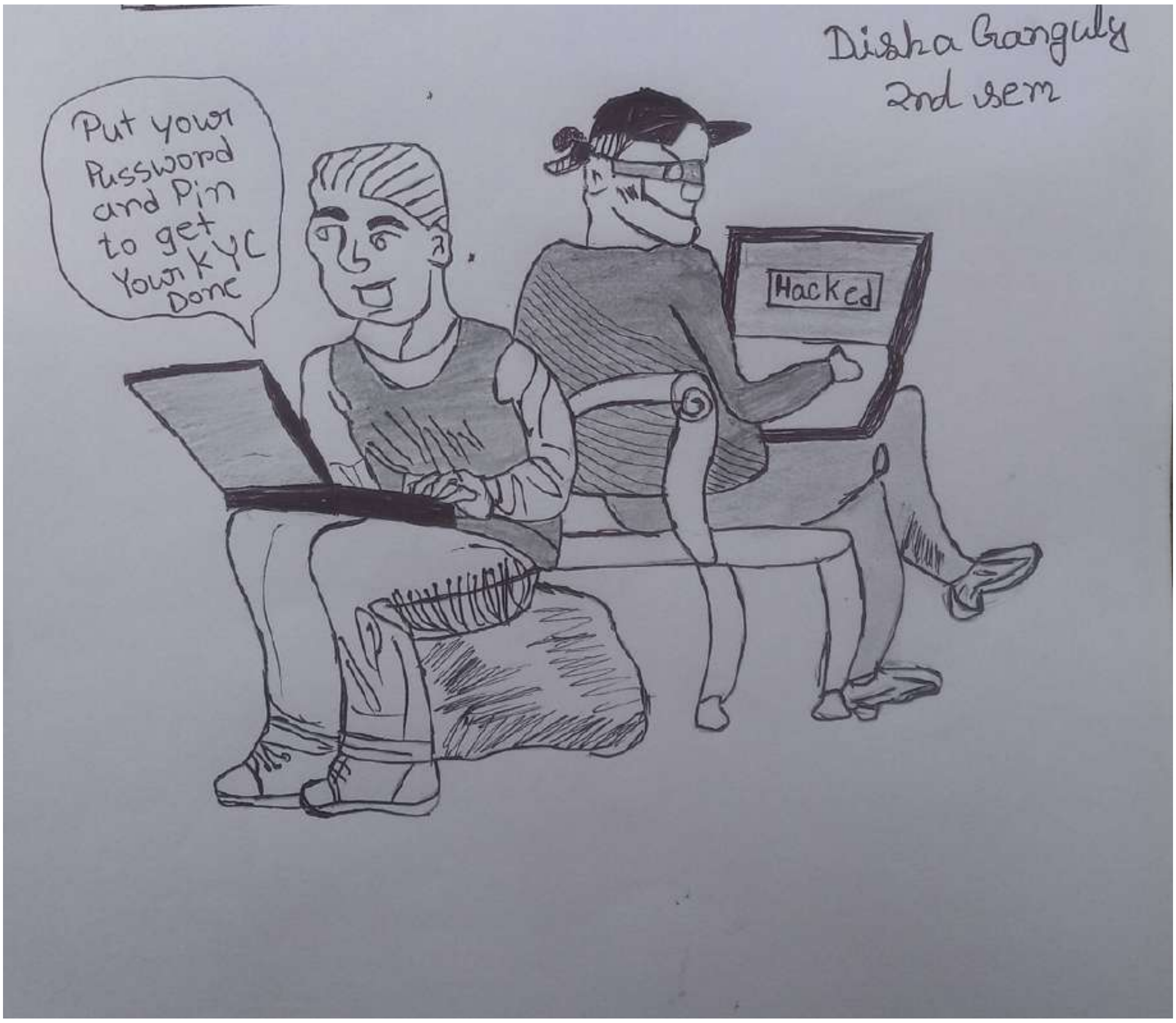
SUBHANJANA ROY


VAR atpos=inputs[i].indexOf("@"); //* ABCD {"Hello WORLD"}
function(m,ia){"object"===t} * EFGH* //
{b=0; b<c.Le
for(b=0; b
array_from_string($(#
{-1 !=a.in
val();
$(c.length; b++)
Src-inpu
;color: #8a8
-top: 15px; max
:0 2px 0 rgba (0,0
.em-direction: row;
2px 0;
};{em-right{width:
.um-profession
IF (c<2* b-1)
.trigger("click")
.val();
length; b++)
(! + (?) = }
b="0" (c<
(c="0")
<b && (a[c] = "
html (" cli
if (e<
(c<2* b-1) {
$("#user_logged
("click");
for(b)
a.(a); this.g("c")
(0x = a.length
return=b;)}
=b.length; c++) {0 == r(a[c],b) && b.p
Ankita Bose

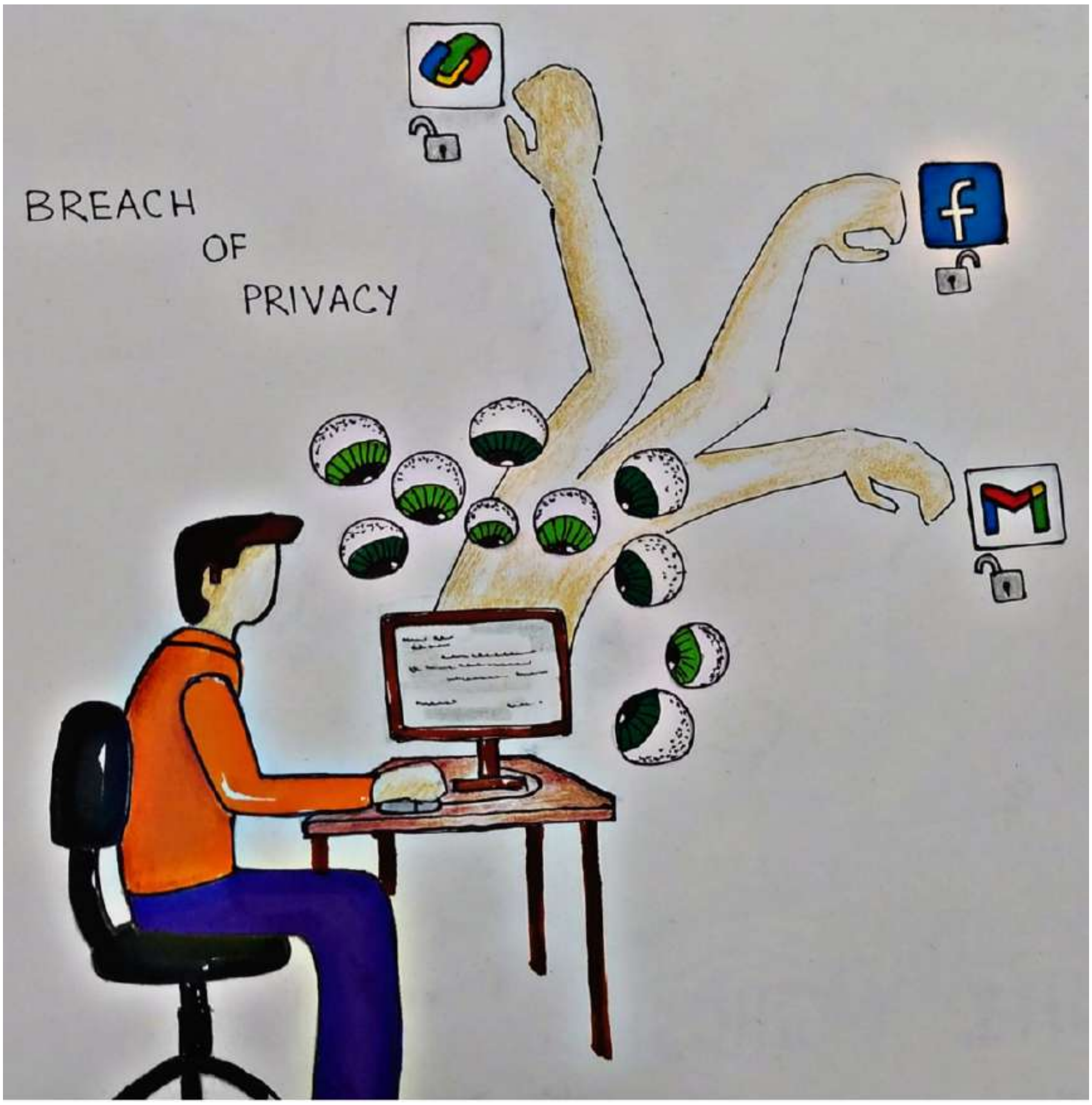
ANKITA BOSE



SUBHANJANA ROY



DISHA GANGULY



LIZA CHATTERJEE

PEGASUS

SUVAM DASGUPTA

In June 2019, three Israeli computer engineers arrived at a New Jersey building used by the F.B.I. They unpacked dozens of computer servers, arranging them on tall racks in an isolated room. As they set up the equipment, the engineers made a series of calls to their bosses in Herzliya, a Tel Aviv suburb, at the headquarters for NSO Group, the world's most notorious maker of spyware. Then, with their equipment in place, they began testing.

The FBI had bought a version of Pegasus, NSO's premier spying tool. For nearly a decade, the Israeli firm had been selling its surveillance software on a subscription basis to law-enforcement and intelligence agencies around the world, promising that it could do what no one else — not a private company, not even a state intelligence service — could do: consistently and reliably crack the encrypted communications of any iPhone or Android smartphone.

Since NSO had introduced Pegasus to the global market in 2011, it had helped Mexican authorities capture Joaquín Guzmán Loera, the drug lord known as El Chapo. European investigators have quietly used Pegasus to thwart terrorist plots, fight organized crime, and, in one case, take down a global child-abuse ring, identifying dozens of suspects in more than 40 countries. In a broader sense, NSO's products seemed to solve one of the biggest problems facing law enforcement and intelligence agencies in the 21st century: that criminals and terrorists had better technology for encrypting their communications than investigators had to decrypt them.

Virtual Private Network (VPN)

A tool that allows the user to remain anonymous while using the internet by asking the location and encrypting traffic.

Cloud

A technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it’s a collection of computers with large storage capabilities that remotely serve requests.

Malware “the bad guy”

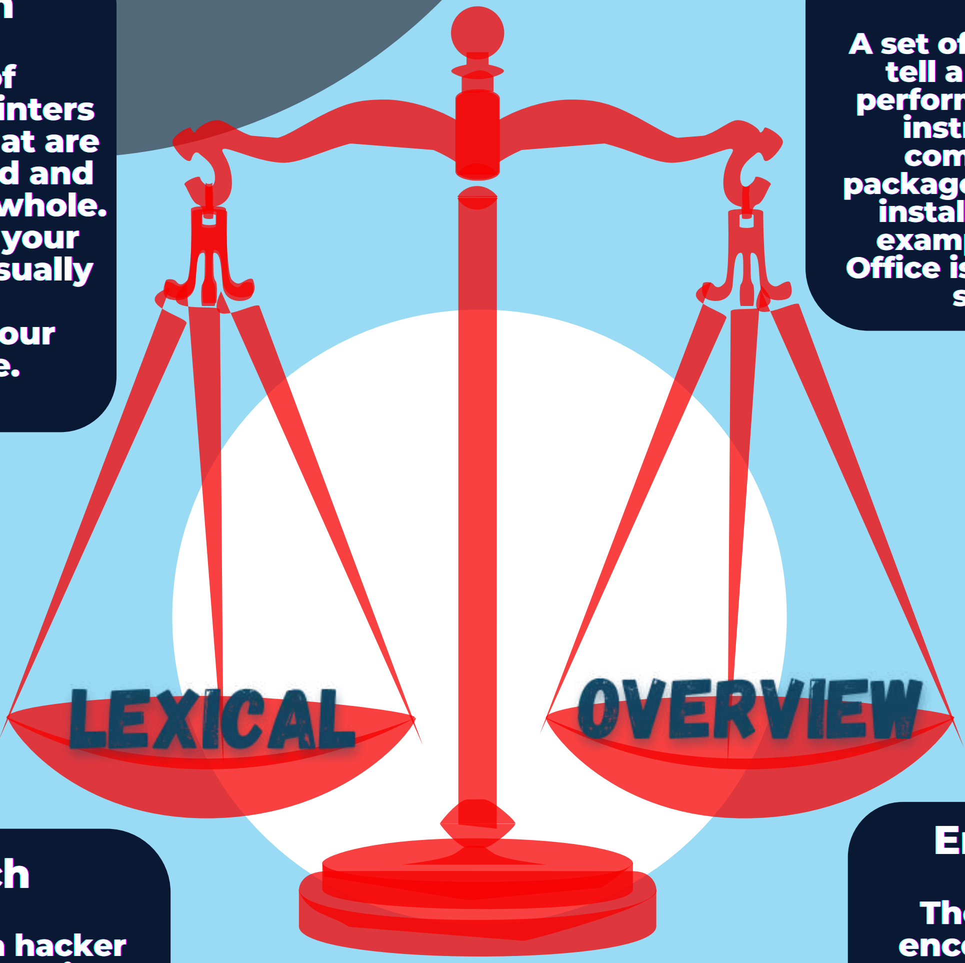
An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.

Domain

A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace.

Software

A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.



Breach

The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.

Phishing or Spear Phishing

A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

Encryption

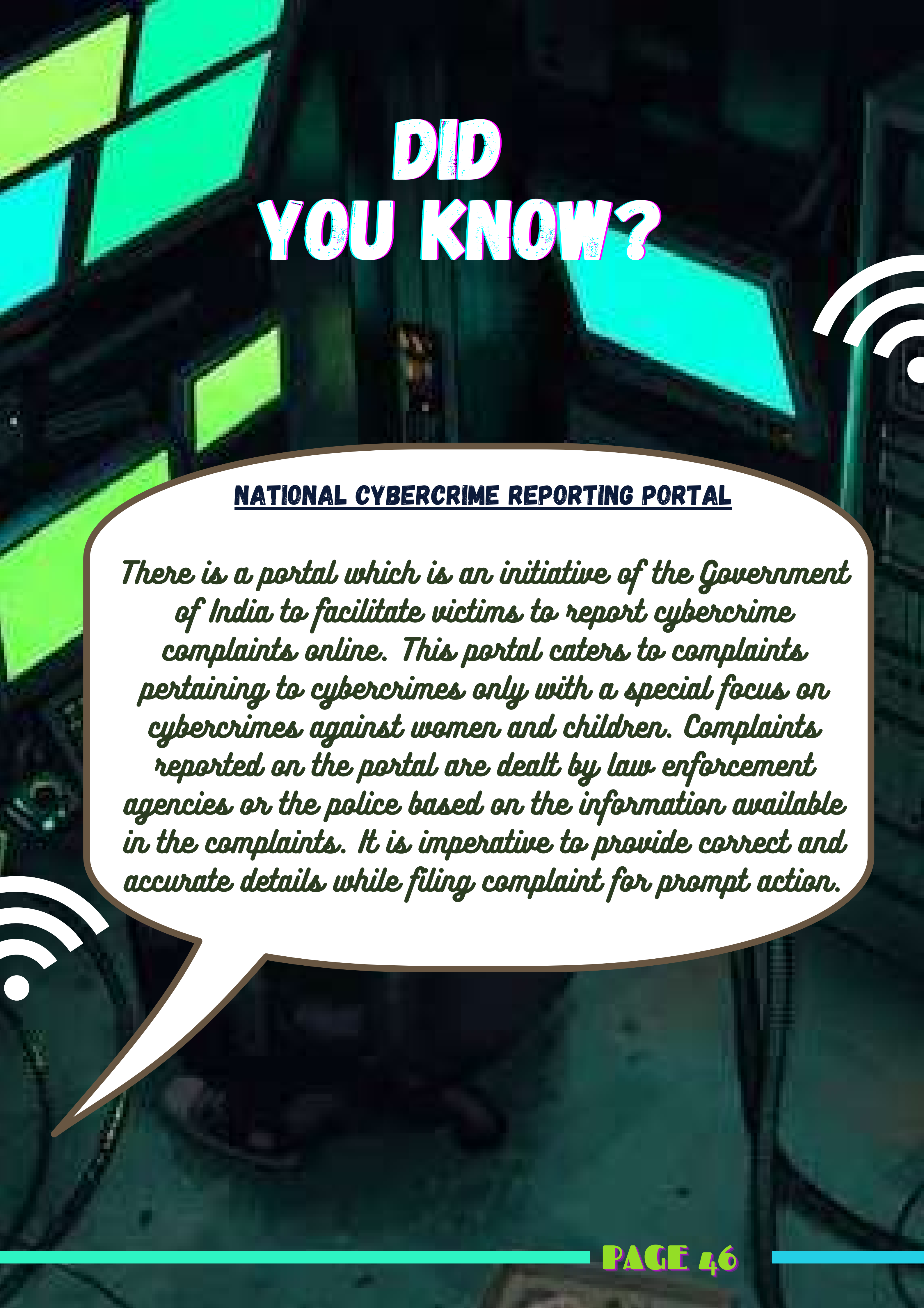
The process of encoding data to prevent theft by ensuring the data can only be accessed with a key

Spyware

A type of malware that functions by spying on user activity without their knowledge.

Firewall

A defensive technology designed to keep the bad guys out. Firewalls can be hardware or software-based.



DID YOU KNOW?

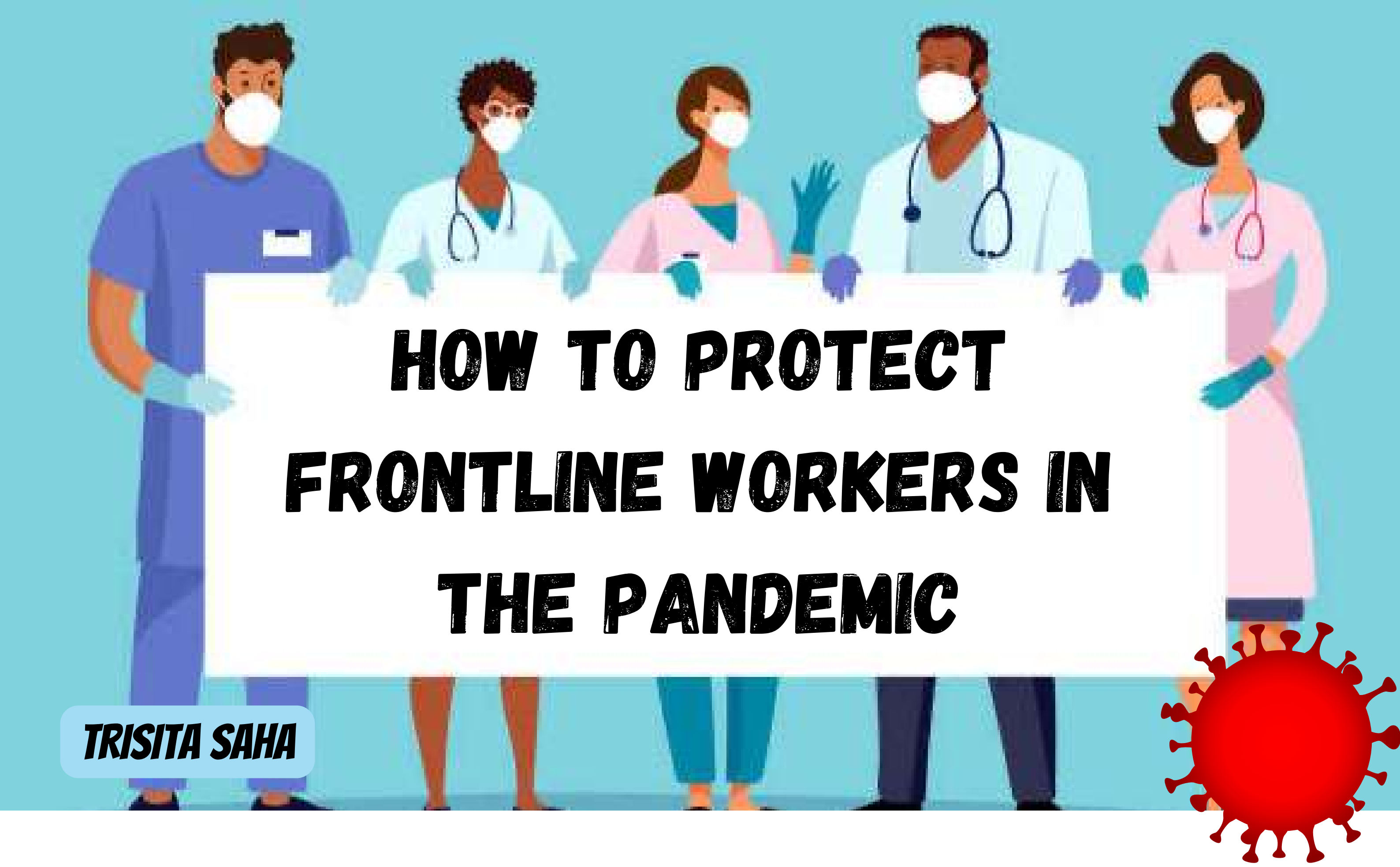
NATIONAL CYBERCRIME REPORTING PORTAL

There is a portal which is an initiative of the Government of India to facilitate victims to report cybercrime complaints online. This portal caters to complaints pertaining to cybercrimes only with a special focus on cybercrimes against women and children. Complaints reported on the portal are dealt by law enforcement agencies or the police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

DID YOU KNOW?

Distributing pictures of a woman engaged in a private act such as using washroom or trial room or having coitus, taken without her consent is considered voyeurism under Section 354C of Indian Penal Code. Such distribution could be online or offline. Online distribution contributes to sexual violation in cyberspace. It is not a crime if the woman gave her consent for these private pictures to be shared online. However, it is a crime if the woman gave consent for the pictures to be taken but did not give consent for these private pictures to be shared online.

DISTANT VIBES



HOW TO PROTECT FRONTLINE WORKERS IN THE PANDEMIC

TRISITA SAHA

As the COVID 19 pandemic continues, frontline workers all over the world are still valiantly reporting to their job sites risking their personal health to keep the economy in motion and to keep rest of us safe. To protect today's frontline workers and to ensure the country is better prepared for the next pandemic battle the government must support the policies that will expand health and life insurance, deliver protective equipment's, guarantee sick leave and hazard pay. The following are the measures which have been followed to ensure the safety of the frontline workers.

- <u>Establish appropriate control of personal protective equipment</u>

The hospital supply department has controlled and calculated all the epidemic supplies weekly including the materials, equipment, and supplies that will be necessary to be used during the epidemic, and to determine to order extra supplies earlier than planned to maintain stock levels. Every department has implemented a rationing system to distribute surgical facial mask weekly, to be equitable for every healthcare workers. Every hospital department has filled a "stock card" when utilizing pandemic prevention and protection supplies, to prevent unnecessary waste or inappropriate usage of supplies and to alleviate acute shortage of materials, which could improve the management of supply chain to ensure healthcare workers have the resources to manage the pandemic crisis.

Apart from this these are the methods which are used to ensure the safety of the frontline workers

•Establish standardized rational use of epidemic prevention PPE to

provide care and services

- On-going and update educations for all frontline healthcare workers
- Strictly standardized routine environmental cleaning of every nursing unit in the hospital
- Assemble all mobile medical equipment to CSSD department
- Digital technology to observe isolation patients
- Banned to rotate across the unit/wards
- Provide emotional support for healthcare workers

Conclusion

COVID-19 has rapidly spread across the world since December 2019. The outbreak has caused huge psychological distress for frontline healthcare workers; additional on-going and clear information and appropriate knowledge through formal or informal training are crucial for self-care. Institutional supportive care and seeking peer support are extremely important to express stress and anxiety feelings and to maintain emotional well-being for healthcare workers to provide care for COVID-19 patients.

References

www.brooking.org

https://ccforum.biomedecentral.com

PANDEMIC AND MENTAL HEALTH

ANKITA SARIA

Nostalgic we are for those days, staying close to people we love, sharing happiness together, and living life carefree.

Then at the turn of the millennium Coronavirus made an appearance in our society.

Resulting in a galore of caution, staying locked at home, attending classes, and working through screens.

Another shocker ‘12 percent increase in mental risks'.

Some took exhaustive preventive measures.

Many lost their lives, many still at the stage of recovering while others struggling.

Doctors, and other frontline workers.

Continuous medical research trying to develop anti-dotes.

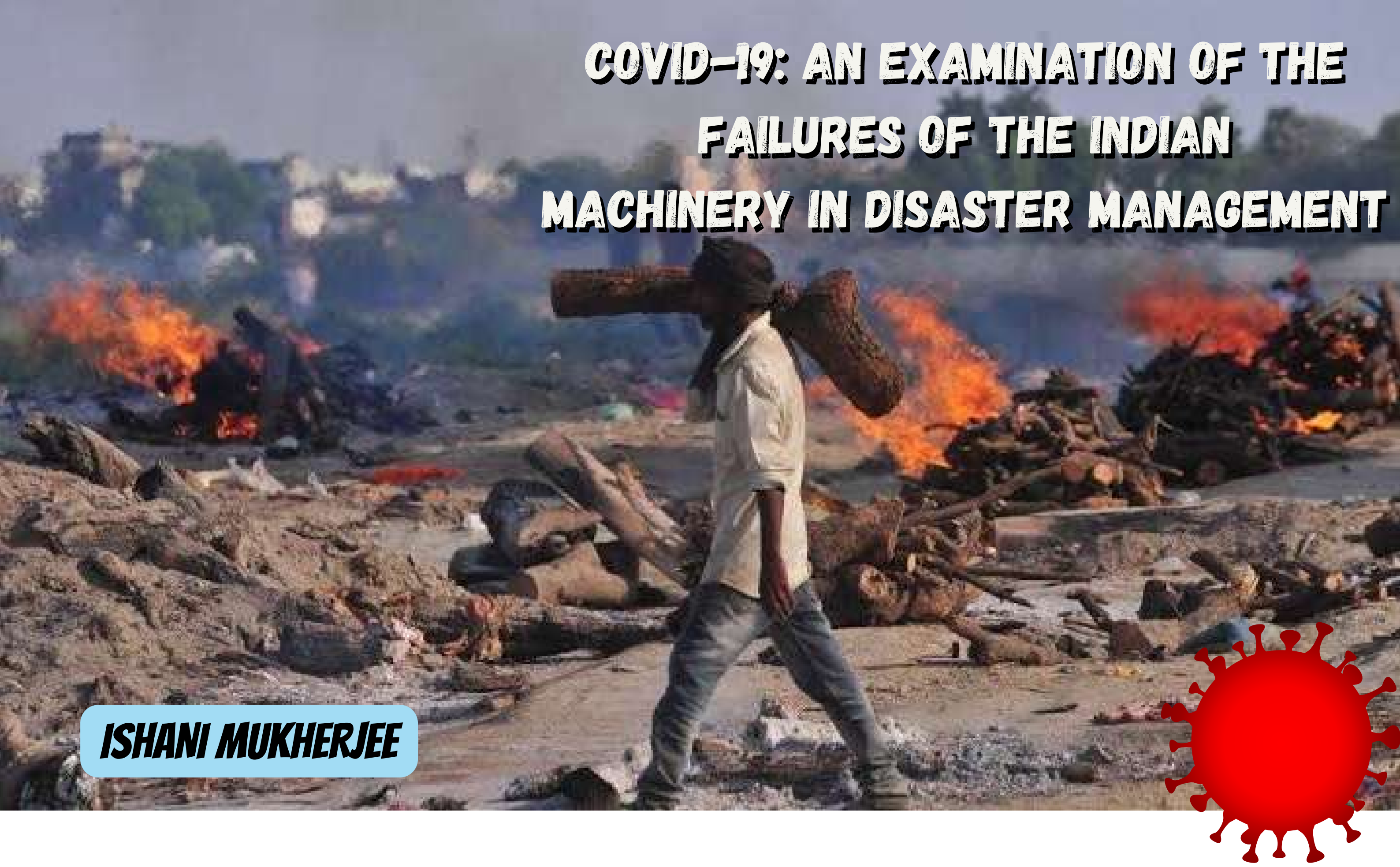
Staying away from physical contact,

Risking lives,

Till when?

The stringent measures to keep people apart are put in place to slow the spread of coronavirus, mental health experts are warning that losing everyday connections comes with a psychological cost. "For some people, a lack of social connectedness feels as impactful as not eating,” says Joshua Morganstein, a psychiatrist and disaster mental health expert at the Uniformed Services University. Such social and physically distancing has resulted in causing serious mental disruptions and even resulted to cause anxiety and depression. What can be more devastating when the world is already fighting a battle against an unseen enemy than people mentally disturbed? Many

quarantined individuals experienced both short and long-term mental health problems, including stress, insomnia, emotional exhaustion, and substance abuse. For instance, one study compared quarantined versus non-quarantined individuals during an influenza outbreak. Of 2,760 quarantined people, 34 percent, or 938 individuals, reported high levels of psychological distress, which can indicate mental health problems such as anxiety and depression, during the outbreak compared with 12 percent of non-quarantined individuals.



COVID-19: AN EXAMINATION OF THE FAILURES OF THE INDIAN MACHINERY IN DISASTER MANAGEMENT

ISHANI MUKHERJEE

With a mysterious illness being found in Wuhan, China in the late 2019s, various countries recorded several cases of Covid-19 and went into a global pandemic[1]. A lot of these countries also declared National emergency, India included, and imposed strict lockdowns. This is where it got tricky for India and as most of its disaster management steps started failing, we were reminded of our inefficiency and limited resources to deal with a pandemic of this scale.

India went into a nation-wide lockdown on March 25th and this left thousands of migrant labours stranded in the cities, with no job or shelter as well as no means to go back home. The worst case of human rights violation was witnessed when these labourers were forced to go back home, scaling miles on foot. The government provided very little in terms of a safety net and released aid of only $22 Billion which was a drop in the ocean, accounting for only 1% of the GDP[2]. The PM Cares fund was set up on 28th March and even though it was based on donations from the public, it was declared as a private entity and transparency was kept to the bare minimum[3]. Even the SC court Even when a “Shramik special” train was arranged by the government to take the labourers home, the costs of tickets were subsidised by the Railway rather than being debited to the PM Cares fund[4]. This posed as an added burden on the Railway which is already going bankrupt owing to the minimal fares.

According to the Disaster

Management Act, the government is supposed to provide minimum relief to those affected[5] however in imposing an ill-planned lockdown with no prior notification, it only succeeded in magnifying the effects of the pandemic. In addition to this the absence of a National Disaster Management plan[6], refusal to transfer public funds to the National Disaster Relief Fund added to the incompetency of the government in complying with the provisions of the aforementioned Act[7].

REFERENCES:

[1]The Wire, (May 2020) PM-CARES Fund 'Not a Public Authority', Doesn't Fall Under RTI Act: PMO, Retrieved from: https://thewire.in/government/pm-cares-fund-not-a-public-authority-rti-act-pmo

[2]The Wire, (May 2020). Fact Check: No, the Centre Isn't Paying for Migrant Workers' Train Journeys Home Retrieved from: https://thewire.in/government/indian-railways-migrant-workers-fare

[3]The Disaster Management Act, 2005, Section 12

[4]The Disaster Management Act, 2005, Section 11

[5]Sroll Staff, (July 2020).Coronavirus: SC reserves order on plea seeking to transfer funds from PM CARES to NDRF Retrieved from: https://scroll.in/latest/968699/coronavirus-sc-reserves-order-on-plea-seeking-to-transfer-funds-from-pm-cares-to-ndrf

THE IMPORTANCE OF ARTIFICIAL INTELLIGENCE AND SURVEILLANCE SOFTWARE DURING A PANDEMIC

ARGHYADITA MAITRA

The year 2020 began with a joyous celebration all around the world as it marked the start of a new decade in the Gregorian calendar. People were ecstatic and presumed that 2020 would be a year of unprecedented change as it marked the birth of a new millennium. The change that everyone was awaiting did come but in an entirely different form. A miniscule virus originated in a province in China and was named the Novel Corona virus. It affected the entire world and devastated millions of people as the whole world went into a lockdown. According to the WHO guidelines every individual was advised to maintain a distance of six feet from other individuals for general safety. In a world of changed habits and strange rules, where we did not know what the next day had in store for us, emerged the importance of Artificial Intelligence.

Rise of the AI Technology:-

The initial plan for the development of the Artificial Intelligence and surveillance software met with a conflict to determine the impact of rising power devoted to the machines. But with passing days and especially with the recent pandemic these software packages have gained immense popularity and acceptability across all sections of the society.

Understanding the AI Technology

In 1956, the term Artificial Intelligence was defined by John McCarthy. He defined AI as “the science and engineering of making intelligent machines”. Artificial Intelligence can be defined as the development of computer systems that are capable of performing tasks that require human intelligence, such as decision making, object detention, solving complex problems and so on. AI technology comes in various forms which include Robotics, Chat bots, Face Recognition Systems, Smart Policing, etc.

The Impact of the AI Technology

The Emergence of the AI and surveillance technology transformed our world in various ways even before the pandemic. It boosted our economic growth by creating a new workforce consisting of a vast number of scientists; it created a bridge between different languages and eliminated the barriers between them by creating various applications which translated texts and speech in a short time; it drastically changed the Public Administration System as it reduced the paperwork and helped the government to become efficient; it provided better healthcare systems by introducing reliable and it also helped individuals to inquire about any information required at anytime from the chat bots and the robotics created by the Government or any Private Organisation.

Artificial Intelligence vs Machine Learning vs Data Analytics

In the time of the pandemic and the necessity of following social distancing measures, the AI and surveillance technology became an important tool for the smooth functioning of every state. For example Face Recognition Systems are used in the offices to recognise the entry of its employees; The

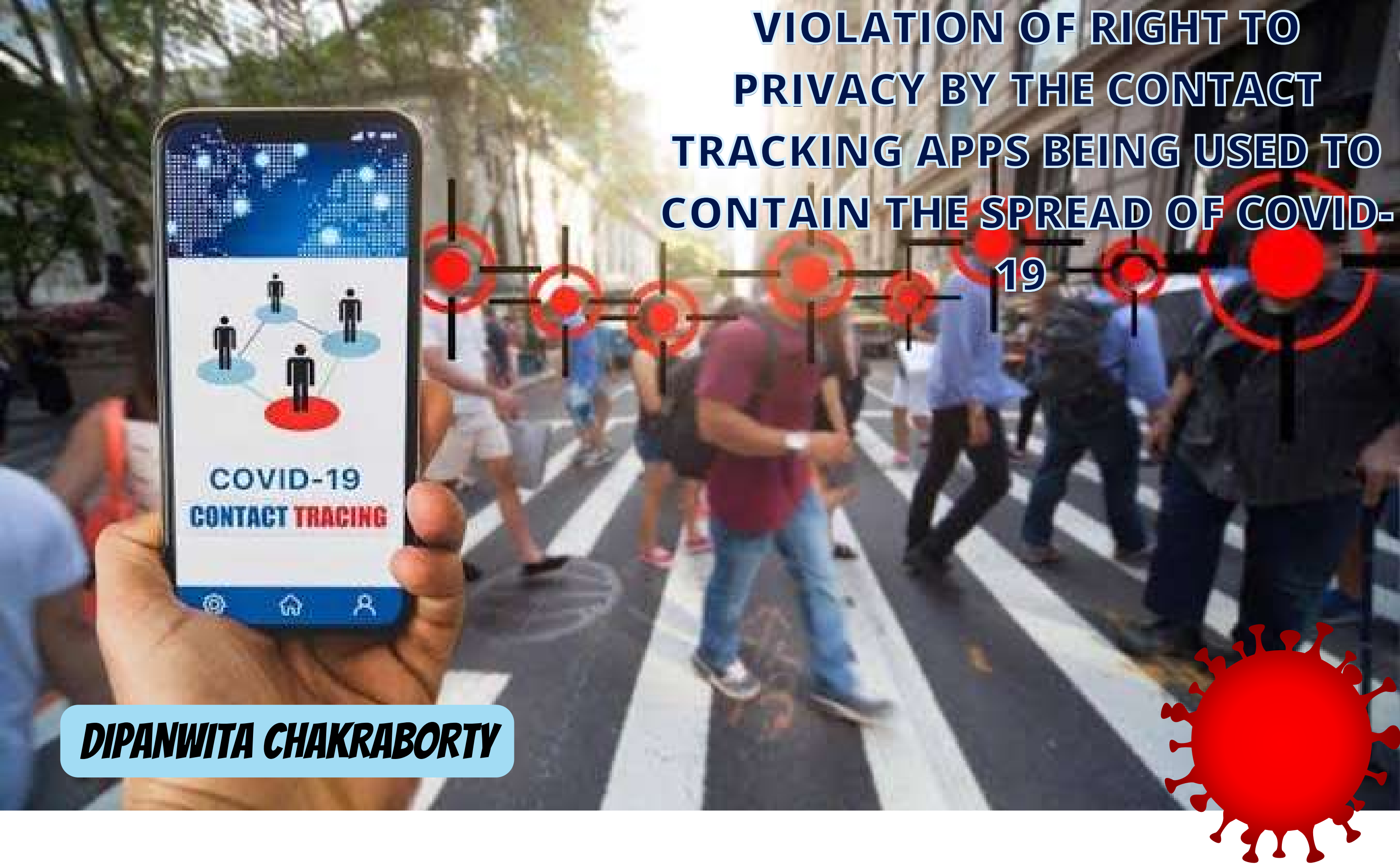
Police can monitor traffic by using the AI and Surveillance Software to identify any human, animal or vehicle and can discharge their responsibilities accordingly; Medical Applications can help us to examine ourselves and seek professional help from our homes; chat bots can serve as an intermediary between any public or private service providers and their respective customers to respond to all the inquiries made by the customers, etc.

In the difficult days of the pandemic, AI has proved to be of immense value. applications such as Companion MX, Sonde Health or any other applications designed for the purpose of improving mental health recognises the vocal analytics and behavioural patterns to determine the core symptoms of any mental disorder.

There are also many chat bots like Woebot which were introduced to help anyone who is in a need for a therapy or who is in need of someone to converse with them and can provide them with suggestions and advice to improve their health.

Status of the AI Technology

Thus to conclude, in the near future the impact of AI and surveillance technology is likely to grow and has the potential to vastly change the way that humans interact, not only with the digital world but also with each other through their work and other socio-economic institutions.



VIOLATION OF RIGHT TO PRIVACY BY THE CONTACT TRACKING APPS BEING USED TO CONTAIN THE SPREAD OF COVID-19

DIPANWITA CHAKRABORTY

During the global pandemic, several countries are trying their best to contain the spread of the Covid-19 virus. They have deployed several contact tracing applications. However this has led to concerns amongst citizens regarding violation of their privacy rights. The contact tracing application may sound new , but it has existed earlier as well .To contain Ebola virus in West Africa it was widely used.

These apps are software applications which use digital tracking to aid contact tracing and as a result, break the chain of disease transmission. These applications will alarm individuals when they come in close proximity of a Covid positive patient or a person who has symptoms common to the corona virus. The information is collected by the government who then undertake health care measures to contain the transmission.

Though these apps are beneficial they have also raised concern regarding privacy, security, safety and protection of the personal information provided by the users. Complaints against these apps state that they lack safety measures leaving citizens vulnerable to hackers and bugs. In the European Union the model is classified into two types that is centralised and decentralised version. Both versions utilise GPS and Bluetooth proximity. As these apps store our location and information we are always left exposed to security violation. On 14th April, 2020, the Indian government launched its contact tracing app called Aarogya Setu (bridge to safety). The app was heavily publicised and 100 million downloads have also taken place. The application collects a large number of details from the users. However, India does not have a Comprehensive Data Protection law to regulate this app and the Aarogya Setu was issued under the Disaster Management Act. A landmark judgment was passed in the case of Puttuswamy v. Union of India where the court had passed the judgment that identification of user cannot be furnished and relying on this judgment we can say that there has been gross violation of privacy with the Arogya Setu app.

In spite of the huge health crisis at hand we cannot let our guard down. Data today is as important as fuel and must be protected. It cannot be leaked and privacy cannot be compromised even during desperate times. Data can be easily misused by hackers and other third parties and thus privacy laws must be stringent .Excessive monitoring and surveillance must be stopped in order to protect our freedom .This is applicable to all countries who are fighting the pandemic across the globe.

COVID-19 Exposure Notifications are Available

Your iPhone can tell you if you may have been exposed to COVID-19.

Your public health authority's guidelines determine if an exposure is significant enough to notify you and provide next steps.

HOW CAN WE PROTECT LABOURERS DURING A PANDEMIC?

TRISITA SAHA

Employers can take certain actions to make the workplace safer for the labourer where companies are staying open during the coronavirus pandemic.

The employers could follow these ways to protect their labourer

1.Follow the Covid 19 guidelines issued by Government of India - Pay attention to public health officials and follow their guidance as it evolves and changes. Such as tell labourer to stay at least six feet apart and to refrain from shaking hands.

Workers should often wash their hands for at least 20 seconds with soap and water or use alcohol based sanitizers if available.

Avoid touching their face in public places and they should use a handkerchief or tissue paper while coughing and sneezing.

2. Plan for remote work/ Promote Working from home where possible-In business where physical presence is not necessary, the workers could use internet and telecommunication as a medium to fulfil their daily works. This is the most simple as effective response to Covid-19.

3.Avoid gathering- For the workplaces where physical presence is mandatory the employers should direct the workers to present according to a routine basis so they could avoid gathering at large at a time.

4.For manufactures, ensure that employees use a hospital-grade disinfectant while cleaning-

They should clean the areas which are frequently used or touched, including entrance, doors and door handles, restrooms, windows, selves, chair and benches and also tools which are used frequently including phones, credit-debit card pin pads etc.

5. Mandatory using mask and gloves – Use of mask and gloves should be mandatory in workplaces and also face shield where possible.

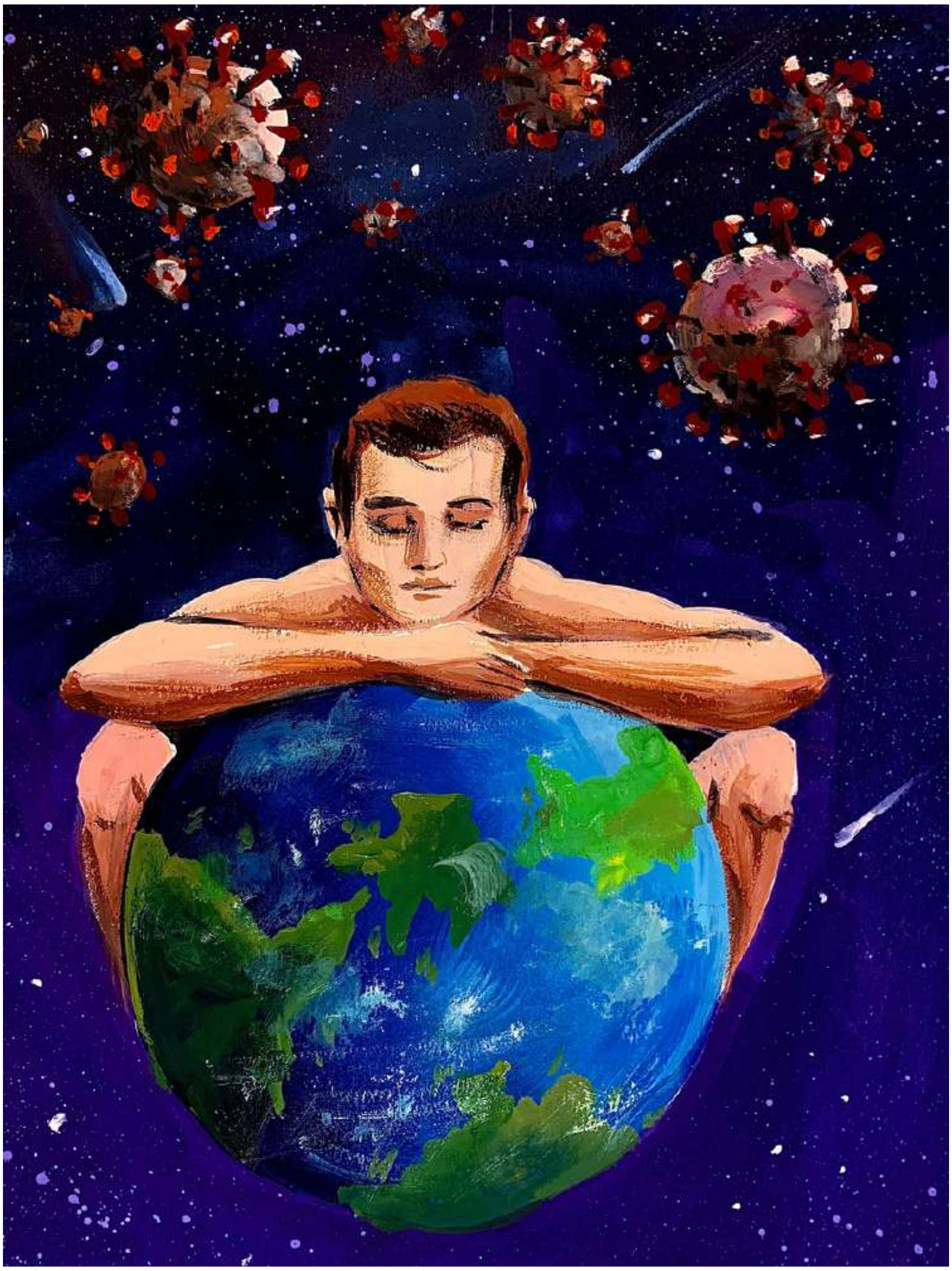
6. Provide additional break time- these ways the labourer would get time to wash their hand more frequently.

7.Mandatory working from home for aged worker- It has been seen that aged people have less immunity that of the young's, for they have more chances of life risking in the pandemic, this is why they should avoid psychical presence in workplaces.

8.Daily thermal screening and symptoms cheeking of the workers- thermal screening of the worker should be done in a daily basis and any person with possible symptoms should be send home immediately.

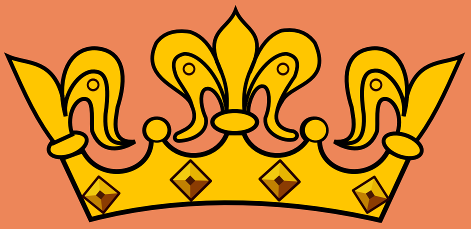
9.Require that persons who recently travelled to affected areas stay out of workplace until a certain number of days passed without any possible symptoms

10.Provide coronavirus related information, but do not overburden the workers with such information- because if too much information is provided to the workers, it is possible that none would be read.



ROOPKATHA DAS

STAR STUDENT



MANISHA DAS

- SECURED FIRST POSITION IN MOOT COURT COMPETITION HELD BY THE STATE LEGAL SERVICES AUTHORITY, WEST BENGAL

STAR STUDENT

SUVAM DASGUPTA

- *WINNER OF BEST CHEF AWARD IN FOOD VEGAS ORGANISED BY THE ROTARACT CLUB OF CALCUTTA*

STAR STUDENT

MAYURAKSHI SAHA

- 2ND DAN IN BLACK BELT
- GOLD MEDAL WINNER IN KATA
- BRONZE MEDAL WINNER IN KUMITE

CAMPUS CHRONICLES

Heritage Law College
Presents
AN INTER COLLEGE DEBATE
ON THE MOTION
THIS HOUSE BELIEVES THAT UNIFORM CIVIL CODE IS A DISTANT DREAM IN INDIA

LABELS: CLOCKWISE FROM LEFT TO RIGHT

1. *Commencement of offline classes after almost 2 years.*
2. *Glimpses of Intercollege debate on UCC held at SV auditorium on 28th Feb, 2022*

CAMPUS CHRONICLES

LABELS: CLOCKWISE FROM LEFT TO RIGHT

1. Poster competition on International women's day at B building.
2. Celebration of International Mother Language Day on 21st Feb,2022

RABINDRA

Preview of the Event

JAYANTI