INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

Dr.S.Krishnan
Associate Professor
Seedling School of Law & Governance
Jaipur National University, Jaipur

Ms. Loria Sharma
1st Year Student of BALLB
Seedling School of Law & Governance
Jaipur National University, Jaipur

Abstract:

The Internet is at once a new communications medium and a new locus for social organization on a global basis. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. The Internet is an unprecedented mechanism for delivering government and social services, from education and healthcare to public information. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu. However, it remains an open question whether the Internet's democratic potential will be achieved. The Internet exists within social, political, and technological contexts that can impede its democratic potential. Governments tout the Internet, but worry about its threat to their traditional authority. The private sector sees the economic potential of the Internet, but anti-competitive impulses are also part of the landscape. Users bring not only their social aspirations to the Internet, but also their potential for antisocial behavior. Adopting the frontier metaphor, we are now witnessing the struggle over governance of the Internet. After the revolution, what type of constitution do we want? Will it be pluralistic and democratic? Will it incorporate a bill of rights that protects individual liberty and equality?

Protection of privacy is one of the critical issues that must be resolved. Will the "Digital Age" be one in which individuals maintain, lose, or gain control over information about themselves? Will it be possible to preserve a protected sphere from unreasonable government and private sector intrusion? In the midst of this uncertainty, there are reasons for optimism. Individuals operating on the Internet can use new tools for protecting their privacy. From anonymous mailers and web browsers that allow individuals to interact anonymously, to encryption programs that protect e-mail messages as they pass through the network; individuals can

ISSN: 2582-6433

harness the technology to promote their privacy. Equally important is the new found voice of individuals. Using e-mail, Web sites, listservers, and newsgroups, individuals on the Internet are able to quickly respond to perceived threats to privacy.

Keywords: Privacy, Social Media, Liberty, Access to Information

Introduction

The current study elaborates on the shift in the conceptualization of 'privacy' across time from the concrete private domain to that abstract complex and diversified concept of the 'right to privacy' that needs to be protected against malpractices and violations. Now, the right to privacy has incorporated the individual's right to control their own personal information although this has become quite challenging in the era of digital platforms.

Privacy, in its foundational understanding, denotes freedom from incursion and has long been seen as an inalienable natural right of humanity. The inception of the right to privacy stems back to the 1890s, when influential thinkers like Samuel D. Warren and Louis Brandeis proposed that the "right to privacy" ought to be incorporated into the horizon of right to life.

The acknowledgement of the "right to privacy" as a fundamental right in India took time and was subject to judicial scrutiny from the inception of the Indian Constitution. Initially, in Kharak Singh v. State of U.P., Justice Subba Rao's minority opinion deemed the right to privacy as "an essential ingredient of personal liberty." However, at that point, it was not officially recognized as a "fundamental right", and its status remained uncertain.

Nevertheless, a nine-judge Supreme Court panel in the case of Justice K.S. Puttaswamy v. Union of India in 2017 restated the recognition of the right to privacy as a fundamental right under Article21 of the Constitution of India. They went on to emphasize that the right to privacy was not only intricately linked to the liberties safeguarded by diverse fundamental rights but also represented an intrinsic aspect of dignity, autonomy and liberty. In the global arena, the right to privacy is likewise seen as a critical and fundamental human right and is bolstered by an effective foundation. Article 12 of the Universal Declaration of Human Rights, 1948 (UDHR) and Article 17 of the International Covenant on Civil and Political Rights, 1966 (ICCPR) are two influential and authoritative international treaties that ensure and protect individuals from "arbitrary interference" in their private matters and personal lives.

ISSN: 2582-6433

The significance of the “right to privacy” has heightened in contemporary times, owing mostly to the growing influence of social media and the internet in today’s digital landscape. A substantial amount of concern and fear has been voiced in recent times around the enormous amount of private information stored in computer files. The “right to privacy” “pertains to an individual’s right to regulate the collection, utilization, and dissemination of their private information.” Social media has evolved into a potent instrument that facilitates individuals in connecting, collaborating, and sharing ideas and information globally. It has garnered widespread popularity worldwide, connecting millions of individuals through the digital medium.

Social media networks extract private information on individual actions, hobbies personality traits, perspectives on politics, and internet patterns and misuse of such private information poses a grave threat to the “right to privacy” of individuals as enshrined in the Indian Constitution.

Our Dystopian Present

Living in modern society, we are profiled. We accept the necessity to hand over intimate details about ourselves to proper authorities and presume they will keep this information secure- only to be used under the most egregious cases with legal justifications. Parents provide governments withinformation about their children to obtain necessary services, such as health care. We reciprocatethe forfeiture of our intimate details by accepting the fine print on every form we sign- or button we press. In doing so, we enable second-hand trading of our personal information, exponentially increasing the likelihood that our data will be utilized for illegitimate purposes.

Often without our awareness or consent, detection devices track our movements, our preferences,and any information they are capable of mining from our digital existence. This data is used to manipulate us, rob from us, and engage in prejudice against us- at times legally. We are stalked byalgorithms that profile all of us. This is not a dystopian outlook on the future or paranoia. This is present day reality, whereby we live in a data-driven society with ubiquitous corruption that enables a small number of individuals to transgress a destitute mass of phone and internet media users.

In this paper we present a few examples from around the world of both violations of privacy

ISSN: 2582-6433

and accomplishments to protect privacy in online environments. The examples provided are not exhaustive, representative, nor the gravest examples. Further research is necessary that will incorporate a systematic review to categorically identify universal values of digital rights and promote policies to thwart perpetrators of them. We conclude with a recommendation that the UN host free, open-access, digital platforms that will promote transparency among organizations thatcollect users' data and assist everyone to safeguard their identities. We must recognize the violations of human rights that are taking place in digital environments and engage in pragmatic steps as an international community to ensure the right to privacy.

Growth of Social Media and its Increasing Influence on Youth

From a thirteen-year-old child to a seventy-five-year-old senior citizen, from a daily wage worker to a software engineer, everybody is on social media. Social media sites like Facebook, Instagram, Twitter, Youtube, have made almost every mobile phone in their home. Among all these kinds of people, it is the youth who is most involved in social media. This involvement may have positive repercussions for some, these include easy accessibility to a wide variety of information, providing an encouraging platform to showcase their creativity, skills and also voicing their opinions on issues which may be social, political or economic. Therefore, it may serve as a source of empowerment for the youth.

With this flexibility, every person has access to a platform where he or she may share information or voice his or her opinions. However, it has to be kept in mind that this free flow of information is by no means an all empowering process for everyone. This may prove to be a bane for some innocent people who may fall prey to others mal intentions. Yes, flowing of false information, intentionally or unintentionally has become a commonplace on social media. We often hear news of fake allegations like that of sexual harassment, fraud etc particularly to defame someone. There are also many cases where someone’s personal information is made available on the internet for public view. All this amounts to a breach of the fundamental right to privacy.

Social Media And Right To Privacy: How To Strike A Balance?

Privacy, in the simplest sense, is the state of being secure from public intervention, without one’s permission. Recognition of the right to privacy as a fundamental right was a bone of contention for years for the Indian judiciary. In the earlier judgments of M.P Sharma vs Satish

ISSN: 2582-6433

Chandra and Kharak Singh vs the State of U.P, it was held that the right to privacy is not a fundamental right guaranteed under the Constitution of India.

The internet has permeated every facet of existence, modern technology skillfully weaving it all together. People establish connections with others and employ social media as a medium for communication. Furthermore, digital space functions as a platform for engaging in business transactions, procuring goods and services, accessing new information, and streamlining ordinary operations such as banking. With every internet transaction, the user unknowingly leaves electronic tracks that contain powerful means of information that provide knowledge about the user and their interests. In such an information age, which has been purported as "as era of ubiquitous dataveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology," there exists a greater threat to the right to privacy of people as underscored in the Justice K.S Puttaswamy v. Union of India.

The consideration of incorporating the "right to privacy" into the Indian Constitution has been a subject of judicial scrutiny since its establishment, as it was never explicitly stated. The matter of recognising the "right to privacy" under Part III of the Constitution was raised during the M.P. Sharma v. Satish Chandra case, wherein the court decided not to make that determination. In the Kharak Singh v. State of U.P., although privacy was acknowledged, it was not yet deemed as an essential right, however, in PUCL vs Union of India, the court affirmed citizens' private interests and implemented legal safeguards to protect people's right to privacy against telephone tapping.

The landmark decision in Justice K.S. Puttaswamy v. Union of India, which revolved around Aadhaar, a government initiative providing a unique identification to Indian residents, confirmed the "right to privacy as a fundamental right" under Article 21. Article 21 safeguards the "Right to life and personal liberty" as part III of the Indian Constitution.

In the digital age of today, the "right to privacy" is significantly jeopardized by the growing dependence of individuals on the internet, particularly on social media platforms and such potential risk to private data becomes pronounced as individuals interact with technology. The watershed ruling of the nine-judge bench underscored concerns about the potential loss of privacy for individuals, cautioning against both state and non-state entities. This heightened risk arises from the increased interaction of individuals with technology, which has the

ISSN: 2582-6433

capability to gather, archive, and mine information for the purpose of profiling individuals. On the one hand, social media portals give an effective platform for freely expressing oneself to an extensive demographic; however, on the other hand, they risk exposing the crucial confidential personal information of consumers.

The utilization of "electronic tracks" by various social networking platforms to gather data from users for personalization or targeted adverts poses an enormous threat to individual privacy. Moreover, extensive broadcasting of personal information on social media outlets is intrinsically injurious to individual privacy. Platforms like Facebook have frequently been embroiled in controversies regarding privacy and user security. Even during its nascent years, it was observed that Facebook's algorithm was saving the incomplete posts and comments of the user even before it could be posted as "metadata." These concerns regarding user data were substantiated, particularly after the notable data privacy breach incident in the 'Cambridge Analytica Scandal,' in 2018, where the data and records of millions of people were harvested from Facebook by the data-harvesting enterprise Cambridge Analytica leading to infringement of "right to privacy" of the users.

Concerns over possible invasions of people's "right to privacy" have been prompted by recent privacy policy amendments made by X (formerly Twitter), which permit the collection of users' biometric data. In a similar vein, the Supreme Court of India is currently reviewing the privacy regulations that WhatsApp notified in 2016 and in 2021 after its takeover by Facebook in the case of Karmanya Singh Sareen & Anr. v. Union of India & Ors. The lawsuit seeks to uphold Indian residents' data and "right to privacy." According to WhatsApp's 2016 privacy policy, any consumer data published with the app will also be transmitted to Facebook, the parent organization. The amended policy in 2021 stipulated that consumers would be unable to opt out of transferring data with Facebook if they intended to keep using the app; otherwise, their profile would be terminated. The present situation constitutes an imminent risk to the citizens' "right to privacy."

Another cause of concern regarding privacy is the long-term preservation of information on social networking services. For instance, Facebook's terms of use render it the liberty to archive private data indefinitely, establishing an irreversible extent of control over personally identifiable information. Consequently, even when a user wishes to cease using the social network, the data they provide remains beyond their control. Even the social media apps that

ISSN: 2582-6433

are no longer operational in India, such as Tik-Tok can reportedly continue to access data of Indian users from the app and are able to mine updated data and information of the individuals using the previously existing data which was stored on the app even after the app has been banned in India since 2020. This presents an enormous threat to the privacy of users' data, which nevertheless remains readily obtainable in the contemporary digital landscape and can be exploited by networking software to mine and profile updated information that relies on existing data. If unauthorized parties were to obtain such sensitive data, the implications may be catastrophic while jeopardizing people's safety and causing a grave infringement on their right to privacy as guaranteed by Article 21 of the Indian Constitution.

In an unprecedented and historic judgment, in the case of Puttaswamy v. Union of India, right to privacy was declared as a fundamental right, falling well within the boundary of Article 14, 19 and 21 of the Constitution of India. It particularly exists intrinsic in the right of life and liberty. It was declared that this is a fundamental and inalienable right protecting all personal information of every individual, from even state scrutiny. Therefore, any act by anyone, including the state, which infringes on the right to privacy of an individual is subject to strict judicial scrutiny.

Impact Of Social Media On the Right To Privacy

Social media is basically a form of communication via the internet. Its main goal, when it came into being, was to create a virtual kinship network throughout the world. The major social networking sites are Instagram, Facebook, WhatsApp, etc. The users of these social networking sites were untroubled until the coming of the 1990s. This was when cybercrime was born.

Believe it or not, it is us who give away our personal information online. Intentionally or unintentionally, we give away a lot of our personal information. This can be by signing up for Amazon prime, Facebook, Instagram etc. Out of the internet users, one third admit to knowing nothing about their personal information which is available online. Tons of cyber information available online has opened the gates for new legal challenges for which adequate laws are yet to be framed.

Also, it just doesn't stop with not saving your passwords online or not giving away any of your personal information online. Much more is splayed across cyberspace ranging from the people

ISSN: 2582-6433

you are connected with on social media, your buying patterns, to the frequent visiting of some website etc.

If you fail to protect your personal information from online hackers, the damage caused to you can be huge. These can range from stealing your social security benefits, filing of compensation claims using your credentials and using your names for making monetary transactions in their name to using your credentials for making fake passports, PAN cards etc. More importantly, the cases of sexual predators, cyberstalking, defamation and identity thefts have come into focus.

It has been noted that the younger generation falls prey to such cybercrimes the most. This is because usually, they see no harm in giving out even their personal information. This is major because of their immaturity, which is easily identified by these criminal minds.

It is shocking to note that one of the largest social networking sites, Twitter, has admitted that they have scanned the contacts of all their users so that they can get more information regarding their users. Another example of this is Facebook, giving contradicting statements about its own nature. One the one hand, it takes the firm stand that it owns all the contacts available, and on the other hand, it grants users the right to access any contacts available.

Social Media and Privacy Related Laws In India

Laws related to social media and privacy in India are clearly insufficient. The Indian judiciary and legislature have proved to be far behind expectations when it comes to the framing of laws in this arena. Some rules and legislations have been issued, those too are primarily related to defamation.

In the *Kharak Singh v State of UP*, often called the *PUCL* case, it was held that tapping of phones amounts to a breach of privacy. Extending this reasoning, it can be reasonably held that sharing of information by WhatsApp with Facebook, post its update, is an obvious breach of privacy of its users.

Now let's come to the Information and Technology Act, 2000. The concept of privacy in this act is comprehended in a very liberal and traditional sense. The act of knowingly sending pictures of a person's private parts, without his permission, then Section 66E of this act is

ISSN: 2582-6433

violated. Social media finds only a mention in Section 79 of this act. This section clarifies that if any person posts or uploads anything derogatory to some other, then the medium on which it is posted, that is Twitter, Facebook etc, is not to be held liable for the acts of such person. Beyond this, nothing is mentioned in the whole article with regard to social media. Let us understand this by a simple example- If X, a Facebook user posts something derogatory to Y, another Facebook user, then Facebook is not to be blamed for X's act.

This concept has however evolved with time, in the case of *Shreya Singhal*, it was held that it is Facebook's duty to remove any material posted by them which is objectionable. This has to be done by Facebook, applying its discretion, after complaints regarding the same are received.

One concept to be noted here is the growing popularity of meme culture. Memes of famous personalities carrying derogatory comments and comparisons can be safely termed as an invasion of the privacy of such individuals. To check such incidents is urgently required.

Next, let's learn about the recent Whatsapp- Facebook Privacy Case or *Karmanya Singh v. Union of India*. Constitutional rights were meant to deal primarily with the relationship between the state and individuals. However, this concept has seen a marked change due to the boom of privatisation in India. Private companies have taken up many functions which are traditionally associated with the state. Our Constitution makers, however, had framed laws according to the situation of the country which was prevailing at that time.

Due to these changed conditions, these private actors when performing state-like actions are subjected to the same Constitutional scrutiny. In the case at hand, the contract between two social networking sites, Whatsapp and Facebook was challenged, both private parties, invoking the above-mentioned ideology.

The facts of this case are – Whatsapp contends that now Facebook is its parent company, and hence data of its users can be sent to the latter. Examples of the data in question are- names, phone numbers, credentials, location, status etc. This vulnerable data may be used for a number of purposes of which the users would not even be made aware of. The most harmful one being the risk of uncalled for surveillance. It was also noted that this update of WhatsApp would affect a wide variety of users, most of whom would not even be aware of the damage that can be caused to them.

ISSN: 2582-6433

This case is presently pending before the Supreme court of India. The question of privacy as a fundamental right was then referred to a larger constitutional bench. This bench ruled that privacy has a tripartite structure namely, intimate, public and private zones of privacy. The intimate zone includes physical and sexual privacy, the private zone encompasses ATM number, PAN number etc. These two zones, held by the Supreme court of India are beyond the facts of the case at hand. The zone of public privacy, it was held, has to be dealt with on a case to case basis. The present case falls under this zone and is pending before the Supreme Court.

I. Violations of Privacy

a. Search and Seizure of Digital Property

Governments and militant organizations utilize internet censorship to shape the public's beliefs and curb dissent. From the most developed countries to the least, examples are prevalent of bloggers, activists, and political opponents being harassed and silenced [1]. In the name of internet security, users are analyzed for characteristics that predict problematic behaviors. Data is saved, which can be used to profile individuals or groups who appear rebellious. During major protest movements around the world, such as the Arab Spring, Occupy protests, and the Umbrella Movement, governments were able to extract data from mobile phone users. Social media and other online correspondence were routinely blocked or tracked to dissuade protesters. While lawsexist in most nations to protect search and seizure of physical property, such laws often do not abide for digital property. As a result, without a search warrant, it becomes permissible to insist that individuals forfeit access to social media accounts to gain services such as a visa to visit another country. Repressive regimes scrutinize specific individuals as a method of discrimination.

b. Profiling of Marginalized Groups

Police in the modern age can target specific ethnic, gender, and age groups. The Chicago police department implemented a "Strategic Subject List", which predicts potential perpetrators and victims of gun violence [2]. Individuals can be intimidated or arrested based on characteristics about them or those they associate with. There is a dangerous potential for big data mining to be used to repress minorities. Online profiling enables police to invade the digital property of strategicsubjects [3]. These policing practices broaden disproportionate incarceration of marginalized groups. China has started a "Police Cloud", which appears capable of tracking social and ethnic groups [4]. Not only the police profile marginalized groups, legal and illegal organizations do so as well. Some of them aim to exploit, such as by

ISSN: 2582-6433

luring women into prostitution rings or refugeesinto forced labor. Disadvantaged groups are easy targets of financial scams and more easily takenadvantage of.

c. Biometric Dangers

We have an overarching concern for the fate of the free world in a computer, cloud-driven societythat preserves biometric data. Such data will develop the capability to penalize vast amounts of thepopulation for minor infractions, especially those that lack the technological and financial means to protect their privacy. The discrimination of Nazi Germany reminds us how dangerous it can be for countries to collect registries that track minorities. Biometric data is a centralized command that pretends to have complete control, but in reality unlocks a door for data to be hacked and abused. In Brazil it is now obligatory to be included in the biometrical database, which also enablesvoting in elections [5]. In an example of how biometric data is abused, the Brazilian Federal Policein 2017 made a deal with the Electoral Court for sharing this database without announcing the practice previously [6].

d. Censorship

It was more difficult for autocracies to track down and burn books than it is for modern governments to remove content from the internet. In Turkey, China, and many other countries theinternet is censored to such a point that self-censorship takes place. Individuals willing to express themselves online are exposed to reciprocity. In most countries, some level of censorship exists. In Israel a bill was introduced recently that would provide the court with automatic access to remove content from online platforms [7]. Such actions are justified as a defense against conflictswith organizations such as Hezbollah in Lebanon that use internet platforms to initiate violent actions and recruit agents among Arabs who hold Israeli citizenship [8]. However, the Israel Democracy Institute (IDI) argued against the law, as it is liable to create disproportionatecensorship in an improper legal process that has no precedent in other countries [9]. Governmentsattempt to restrict social media, but companies themselves also censor content. The internal rulesof such censoring also deserve oversight [10].

e. Business Surveillance

Facebook today has over two billion users. It enables people to share private data about themselveswith others they know and trust. The company protects a large amount of user data. However, owing to unclear consent and sharing of data with third-party applications, many have discoveredthat detailed information about them, such as contacts, phone numbers, and

ISSN: 2582-6433

likes, was being collected and shared without their consent or awareness [11]. Furthermore, Facebook provided administrative staff controls to erase messages, while users do not have the same controls over their own information [12]. Facebook is not alone in being accused of violating users' privacy. Agencies such as Equifax, which collected credit ratings for millions of people allowed its systemsto be breached. Health insurance companies purchase big data from health care facilities to create predictive formulas for identifying risk pools and determining rates [13]. More and more businesses are utilizing big data for customer analytics. The USA, once a leader of restricting invasions of privacy, adopted regulations in 2017 that will remove the tradition of net neutrality. The ramifications of this decision will reduce freedom of expression [14] and increase the power of big data businesses to conduct mass surveillance and sell information about users' viewing content, purchases, and other personal information. Google and other large internet search sites already engage in such practices. They sell our information to advertisers, insurers, and lobbying groups, crafting the world that we are exposed to with almost no external ethical oversight.

II. Efforts to Protect Privacy

a. Multinational Efforts to Protect Privacy

Despite negative trends in the digital age, the right to privacy is still championed as an ideal by most of us. Multinational collaboration to protect digital rights is on the rise. Nations are bondingtogether to establish privacy-by-design controls that will protect data according to commonly agreed fundamentals. Governments, businesses, and criminal organizations have profited byinvading our privacy, and supranational bodies are a potential buffer- a last line of resistance. TheEuropean Union recently adopted the General Data Protection Regulation (GDPR), which will gointo effect in 2018. The regulation demands that individuals retain control of their data, that they can see the information about them that is being collected and ask to remove this information frominternet platforms [15]. Organizations that collect data must employ a data protection officer, whowill oversee that privacy standards are upheld and personal data of those who request to be forgotten are removed. A variety of multinational organizations aim to protect our digital rights, including the organization that we represent, Pirate Parties International [16]. Multinational initiatives are made possible by member states who participate. The International Conference for Data Protection and Privacy Commissioners (CDPPC), for example, has been bringing together government stakeholders since 1979 to assist them fulfill their mandates [17]. Each member statesends data protection officers to collaborate, which furthers our goal of harmonizing data protection. The present

ISSN: 2582-6433

UN Resolution on the Right to Privacy in The Digital Age also exemplifies a positive multinational effort to protect privacy.

b. Government Efforts to Protect Privacy

While governments are demonized as infiltrators of our privacy, they are also guarantors of our digital rights and can reprimand those who violate them. Legislation that safeguards sensitive datais important, and many countries are struggling to keep pace with innovations in information technology that have expanded the realm of digital rights. Governments must both protect privacyand promote transparency, tasks that may seem at odds with one another but often function in tandem [18]. Governments can ensure that citizens are made aware of private information that is collected about them, as well as displaying information about what it does with that data and its own work. Medical data, for example, is private data that governments often enact legislation to protect. Otherwise, individuals could be discriminated against for employment and insurance.An important question that has been posed on the right to privacy is whether to provide people with access to medical records that show genetic dispositions to disease, as this information may not provide positive assistance when preventative precautions do not exist [19]. Governments mustdebate the levels of privacy and transparency that are in the best interests of its citizens. Voter rights to privacy are also important in democratic nations, as they guarantee the free choice underlying the spirit of elections. Cybersecurity is also a national responsibility as international conflicts between nation-states often spill over into digital environments. Recent examples of government legislation to provide greater transparency of privacy practices, include the Canadian Parliament's Privacy Commissioner’s Guidelines for Online Consent [20] and Brazil's "Internet Bill of Rights" [21]. Such legislation often seeks to regulate user consent and establish oversight into the interactions of individuals with internet providers and platforms.

c. Business Efforts to Protect Privacy

Effective online businesses realize the importance of customer trust, and they often provide their users with data protection and transparency about how they collect and use data. Single-sign- on frameworks present a challenge and opportunity for protecting individuals' privacy. Users are accused of a "privacy paradox", whereby they are willing to give up their rights to privacy for thesake of convenience but are nonetheless outraged to learn their data was utilized [22]. By allowingusers to opt-in, companies are mitigating some privacy invasion, but they must carefully weigh theadvantages and disadvantages of trading customer data with external

ISSN: 2582-6433

services [23]. Data-driven technology is an important phenomenon, which can assist us in our lives. Standardizing the privacypolicies for single-sign-on frameworks helps to ensure that user data is not misused by secondaryservice providers [24]. Privacy enhancing technologies assist us to protect our data, and such services are often provided free of cost. Facebook, which has already been utilized as a negative example of violating privacy, has also made positive efforts to protect our privacy by allowing users to delete accounts [25] and promising to enable users to also be able to delete specific data in the future [12]. The development of encryption services has also expanded the right to be "out of the system", providing individuals with a digital platform to congregate without fear of government interference. Furthermore, blockchain technology is expanding the right of individualsto establish financial networks that are not government regulated. Efforts by businesses to protectdigital privacy must provide mutual benefits for individuals and organizations.

Conclusion

We hope that the situation might improve for the right to privacy, but the future appears bleaker. Since the advent of a digital society with online accounts, organizations that harvest user data haveamassed tremendous powers. While certain merits can be argued for collecting user data, an equivalent responsibility remains to regulate and secure any stored personal data. Our identities are the most valuable thing we own. They are a form of wealth: identity capital. We should expectour identities to be protected from embezzlement and exploitation.

Unfortunately, both staggering breaches of privacy take place and personal data is used for corruptpurposes. We would like to believe that infringements are rare and negligible, but we have all beenvictims of privacy invasion. Our identities are abused by companies who track customers to sell products, interest groups who manipulate social media to shape elections, and governments that seek omnipotent powers. Online businesses are often multinational and can hide between borders.Neither small organizations nor large governments can be trusted to restrict themselves. The rightto privacy in the digital age demands a united, multinational alliance that will ensure all individualsin the world share an inalienable right to protect their identities.

We urge the United Nations High Commissioner for Human Rights and international communityto enforce accountability measures that ensure privacy invasions are monitored according to universal regulations. We must admonish governments who conduct

ISSN: 2582-6433

indiscriminate mass surveillance and curtail their abilities to collect and utilize private information about individuals. We must penalize companies and individuals who steal our information or use it for illegitimate gains. While there are valid utilitarian reasons to enable minimal surveillance to enforce protectiveand punitive laws against heinous criminal activity, we must not allow individuals to become slaves of an oppressive system akin to George Orwell's Big Brother [26].

The UN must be proactive and provide a forum for those whose privacy is threatened. It is the responsibility of the international community to foster privacy-enhancing technologies that will protect all individuals equally. Regulations must restrict online entities from accessing all of our personal information. Unwitting users should not be compelled into giving up their privacy or nothaving access to a technology. We must ensure that our data is not used without our knowledge orconsent, nor for purposes that were not explicitly stated. Positive efforts are being made, but we are playing a game of catch-up.

References

[1] Flock, Elizabeth. "What Internet censorship looks like around the world". Washington Post.April 5, 2012: https://www.washingtonpost.com/blogs/blogpost/post/internet-censorship-what- does-it-look-like-around-the-world/2012/01/18/gIQAdvMq8P_blog.html?utm_term=.d0ebce509827

[2] Asher, Jeff and Arthur, Rob. "Inside the Algorithm That Tries to Predict Gun Violence in Chicago". The New York Times. June 13, 2017: https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos- high-risk-list.html

[3] Patton, D. U., Brunton, D. W., Dixon, A., Miller, R. J., Leonard, P., and Hackman, R. (2017).Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations. Social Media+ Society, 3(3), 2056305117733344: http://journals.sagepub.com/doi/full/10.1177/2056305117733344

[4] Human Rights Watch. "China: Police 'Big Data' Systems Violate Privacy, Target Dissent" November 19, 2017: https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

[5] Tribunal Superior Eleitoral. "Biometria". Setor de Administração Federal Sul (SAFS): http://www.tse.jus.br/eleitor-e-eleicoes/eleicoes/biometria

[6] Tribunal Superior Eleitoral. "Parceria entre TSE e PF visa maior eficiência da gestão

ISSN: 2582-6433

pública". Setor de Administração Federal Sul (SAFS): http://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/parceria-entre-tse-e-pf-visa-maior-eficiencia-da-gestao-publica

[7] Schwartz Eltsholer, Tehila. "חוק הפייסבוק. תזכיר חוק הסרת תוכן המהווה עבירה מרשת האינטרנט התשע"ו-2016" [The Facebook Law. A memorandum on the law for the removal of content that constitutes a crime on the internet]: https://www.idi.org.il/knesset-commities/12069

[8]The Israeli Security Agency. "Kalkilya Resident Linked to Hezbollah Arrested and Charged".March 9, 2017: https://www.shabak.gov.il/english/publications/Pages/296.aspx\

[9] Hopkins, Nick. "Revealed: Facebook's internal rulebook on sex, terrorism and violence". The Guardian. May 21, 2017: https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence?CMP=share_btn_tw

[10] Sydell, Laura. "FTC Confirms It's Investigating Facebook For Possible Privacy Violations" NPR. March 26, 2018: https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftc- confirms-its-investigating-facebook-for-possible-privacy-violations

[11] Constine, Josh. "Facebook retracted Zuckerberg's messages from recipients' inboxes". TechCrunch. April 5, 2018: https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/

[12] Thielman, Sam. "Your private medical data is for sale – and it's driving a business worth billions". The Guardian. January 10, 2017: https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business- report-warns

[13] Miles, Tom. "U.N. freedom of speech expert concerned about net neutrality". Reuters. December 20, 2017: https://www.reuters.com/article/us-usa-internet-un/u-n-freedom-of-speech-expert-concerned-about-net-neutrality-idUSKBN1EE2DA

[14] The EU General Data Protection Regulation (GDPR) Portal: https://www.eugdpr.org/

[15] Jääsaari, J., & Hildén, J. (2015). Piracy & Social Change| From File Sharing to Free Culture: The Evolving Agenda of European Pirate Parties. *International Journal of Communication*, *9*, 20.

[16] The International Conference of Data Protection and Privacy Commissioners Website: https://icdppc.org/

[17] Gutwirth, S. and De Hert, P. (2008). Regulating profiling in a democratic constitutional state. In *Profiling the European citizen* (pp. 271-302). Springer, Dordrecht.

[18] Tavani, H.T. (2004). "Genomic research and data-mining technology: Implications for personal privacy and informed consent", *Ethics and information technology,* 6(1): 15–28

ISSN: 2582-6433

[19] Office of the Privacy Commissioner of Canada. "Privacy and Social Media in the Age of Big Data: A Report of the Standing Committee on Access to Information, Privacy and Ethics". April, 2013: https://www.priv.gc.ca/media/2105/gl_oc_201405_e.pdf

[20] Arnaudo, D. (2017). "Brazil , the Internet and the Digital Bill of Rights" Igarapé Institute. Strategic Paper 25. April 2017: https://igarape.org.br/marcocivil/assets/downloads/igarape_brazil-the-internet-and-the-digital-bill-of-rights.pdf.

[21] Bashir, M., Hayes, C., Lambert, A., and Kesan, J. (2015). "Online Privacy and Informed Consent: The Dilemma of Information Asymmetry." *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10.

[22] Davenport, Thomas H. and Harris, Jeanne G. (2007). "The Dark Side of Customer Analytics." Harvard Business Review 85(5): 37–48: https://hbr.org/2007/05/the-dark-side-of-customer-analytics

[23] Hoven, J., Blaauw, M., and Warnier, M. (2016). "Privacy and Information Technology." Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/lawphil-nature/

[24] Curtis, Sophie. "How to Permanently Delete Your Facebook Account." The Telegraph. March 21, 2018: https://www.telegraph.co.uk/technology/0/permanently-delete-facebook-account/

[25] Orwell, George (1949). Nineteen Eighty-Four. New York: Harcourt, Brace & Co.