



ORIGINAL RESEARCH PAPER

Law

“RIGHT TO PRIVACY IN DIGITAL SCENARIO AND ITS PROBLEMS & REMEDIES: LEGAL STUDY”

KEY WORDS: Right to Privacy, Digital Scenario, Legal study

Mr. Vashistha Maheshkumar Joshi

Research Scholar, Gokul Global University, Siddhpur - Gujarat

Dr. Hemant kumar K. Patel

Research Supervisor, Gokul Global University, Siddhpur - Gujarat

ABSTRACT

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 with information about their children to obtain necessary services, such as health care. We reciprocate the 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. In this paper we present a few examples from around the world of both violations of privacy 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.

INTRODUCTION

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 by algorithms 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. We conclude with a recommendation that the UN host free, open-access, digital platforms that will promote transparency among organizations that collect 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.

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. 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. Social media and other online correspondence were routinely blocked or tracked to dissuade protesters. While laws exist 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. 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 strategic subjects. These policing practices broaden disproportionate incarceration of marginalized groups. Some of them aim to exploit, such as by luring women into prostitution rings or refugees into forced labor. Disadvantaged groups are easy targets of financial scams and more easily taken advantage of.

c. Biometric Dangers:

We have an overarching concern for the fate of the free world in a computer, cloud-driven society that preserves biometric data. Such data will develop the capability to penalize vast amounts of the population for minor infractions, especially those that lack the technological and financial means to protect their privacy. 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 enables voting in elections. In an example of how biometric data is abused, the Brazilian Federal Police in 2017 made a deal with the Electoral Court for sharing this database without announcing the practice previously.

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 the internet 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. Such actions are justified as a defense against conflicts with organizations such as Hezbollah in Lebanon that use internet platforms to initiate violent actions and recruit agents among Arabs who hold Israeli citizenship. However, the Israel Democracy Institute (IDI) argued against the law, as it is liable to create disproportionate censorship in an improper legal process that has no precedent in other countries. Governments attempt to restrict social media, but companies themselves also censor content. The internal rules of such censoring also deserve oversight.

e. Business Surveillance:

Facebook today has over two billion users. It enables people to share private data about themselves with 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 discovered that detailed information about them, such as contacts, phone numbers, and likes, was being collected and shared without their consent or awareness. Agencies such as Equifax, which collected credit ratings for millions of people allowed its systems to be breached. Health insurance companies purchase big data from health care facilities to create predictive formulas for identifying risk pools and determining rates. More and more businesses are utilizing big data for customer analytics.

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 bonding together to establish privacy-by-design controls that will protect data according to commonly agreed fundamentals. Governments, businesses, and criminal organizations have profited by invading our privacy, and supranational bodies are a potential buffer- a last line of resistance. The European Union recently adopted the General Data Protection Regulation (GDPR), which will go into 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 from internet platforms. Organizations that collect data must employ a data protection officer, who will 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. 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. Each member state sends data protection officers to collaborate, which furthers our goal of harmonizing data protection. The present 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 data is 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 privacy and 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.

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 the sake of convenience but are nonetheless outraged to learn their data was utilized. By allowing users to opt-in, companies are mitigating some privacy invasion, but they must carefully weigh the advantages and disadvantages of trading customer data with external services. Data-driven technology is an important phenomenon, which can assist us in our lives. Standardizing the privacy policies for single-sign-on frameworks helps to ensure that user data is not misused by secondary service providers. 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 and promising to enable users to also be able to delete specific data in the future.

6. 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 have amassed 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. We should expect our identities to be protected from embezzlement and exploitation. Unfortunately, both staggering breaches of privacy take place and personal data is used for corrupt purposes. We would like to believe that infringements are rare and negligible, but we have all been victims 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. The right to privacy in the digital age demands a united, multinational alliance that will ensure all individuals in the world share an inalienable right to protect their identities.

REFERENCES

1. Flock, Elizabeth. "What Internet censorship looks like around the world". Washington Post. April 5, 2012.
2. Asher, Jeff and Arthur, Rob. "Inside the Algorithm That Tries to Predict Gun Violence in Chicago". The New York Times. June 13, 2017.
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).
4. Constine, Josh. "Facebook retracted Zuckerberg's messages from recipients' inboxes". Tech Crunch. April 5, 2018.
5. The EU General Data Protection Regulation (GDPR) Portal.