VOLUME 14 ISSN 2456-9704

RIGHT TO PRIVACY: SOCIAL NETWORKING SITES (SNS)

By Nikita
From Amity Law School, Noida

Introduction

Social Networking Sites is utilized as a means to connect with people by sharing their common interests, activities, backgrounds or real life-connections.

Since early 2000 it is evident that usage of social networking sites has expanded widely and the most common social networking sites in India are Facebook, Instagram, Twitter, & Snapchat.

Social networking has drastically changed the way of people to interact with their friends, family members and associates. Social networks like Facebook, Instagram, Twitter, Snapchat, Google+, Youtube plays a major role in our day to day lives.[1]

Social networks have opened up a new outlet of communications for millions of people around the world. The major cause of this technology to attract the people is the ease with which people can share their personal information with their friends.[2]

In any case, with such huge interconnectivity, meeting of connections, and data sharing by singular clients comes an expanded danger of security infringement.

The increased prevalence of use of information of the personal lives using communication technologies have transformed many people's lives regarding how they work, function, shape, plan, keep up their social relations. [3]

However, these media social sites could also pose certain serious privacy risks. While using these social sites it's become important to know about these social risks which can be obtained by using our own personal information.

Some people might think that sharing of their personal information is in their own hands, if you don't want any of your information getting out online, then don't put it on social media as simple as that. However that's not true and keeping information on their own is not depend upon our own choices but our friends choices too.

When somebody joins a social network, the primary request of business is, obviously, to discover companions. To help the procedure, numerous applications offer to import contact records from somebody's telephone or email or Facebook, to discover matches with individuals as of now in the system.[4]

Since sharing email-id and phone numbers with their friends isn't like they are doing something wrong as they want to stay in touch with those persons but so many times social media share information with such persons with whom the user doesn't want it

[1] https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html

[2] https://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Lack-of-Privacy-Awareness-in-Social-Networks.aspx

[3] https://www.tandfonline.com/doi/full/10.1080/15228831003770775

[4] https://www.sciencenews.org/blog/scicurious/social-media-privacy-no-longer-personal-choice

to get shared and which causes problems and the privacy of the user get affected.

Indian constitution and Right to Privacy

A nine - judge bench of the Supreme Court unanimously has ruled on 24 August 2017 that Right to Privacy is a Fundamental Right that it is intrinsic to life and liberty and enshrined under part 3rd of Article 21 of the Indian Constitution.

- Privacy is a naturally shielded right which develops fundamentally from the guarantee of life and individual freedom in Article 21 of the Constitution.
- Freedom and nobility are alternate perspectives protection which are ensured by the Fundamental Right.
- SC decision that security is the center of human poise.
- Privacy incorporates individual affections, holiness of family life, marriage, multiplication, home.
- Privacy likewise incorporates ideal to be allowed to sit unbothered.
- Having individual decisions representing a lifestyle.
- Protection of our way of life.[5]

Although the Indian supreme court has ruled right to privacy as a fundamental right but it lacks in many aspects that to which extent it would be applicable to human life. As today everything is digital, every minute, every action of humans can be determined by their gadgets. Anyone can trace the location of people via connecting them to any social site. All they have to do is just link their social site with the another one.

Both positive and negative norms are there of these social networking sites.

Positive aspect is that it can help to catch the criminal the way more easier by tracking the location of their gadgets and in other aspects also.

For ex. Nowadays, lots of people make fake social id's by putting the information of any other person and can misuse it any manner due to which the innocent user who has became victim suffers a lot but thanks to the modern digital by which the victim can go to the cyber crime (which handle cases of those who suffer mis happening regarding social sites) and then the officers their can locate the IP address of the gadget which can give information about the owner of the gadget and help the victims and officers to catch the criminal in faster way.

Negative aspect is any normal citizen can track down the location of anyone via digital system and can obtain information about them.

The thing is if the above statement is correct and the information of any person can be obtained so easily then how can privacy be protected and how would the right to privacy will work.

Article 19(1)(a) of Indian constitution gives the citizens to freedom of speech and expression. But nowadays if any social user update anything socially and if it doesn't seem appropriate to the society , they tracked down the user address and the user can be arrested.

[5] http://www.financialexpress.com/india-news/what-fundamental-right-to-privacy-means-and-what-it-doesnt-10-points-from-supreme-court-verdict/823334/

Hence these online sites doesn't only seize the privacy of humans but also seize the right of freedom of speech and expression.
In India, no less than one digital assault was accounted for at regular intervals in the initial a half year of 2017. In 2017, according to the Indian Computer Emergency Response Team (CERT-In), an aggregate of 27,482 instances of cybercrimes have been accounted for over the world.

- **OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKED[6]**

Vice president Minister and Home Minister R.R. Patil affirmed that the Maharashtra government site had been hacked. He included that the state government would look for its assistance and the Cyber Crime Branch to explore the hacking.

The state government site contains itemized data about government offices, brochures, reports, and a few different themes. IT specialists taking a shot at reestablishing the site revealed to Arab News that they expect that the programmers may have pulverized the majority of the site's substance.

As indicated by sources, the programmers might be from Washington. IT specialists said that the programmers had distinguished themselves as "Programmers Cool Al-Jazeera" and guaranteed they were situated in Saudi Arabia. They included this may be a red herring to divert examiners from their trail.

As per a senior authority from the express government's IT office, the official site has been influenced by infections on a few events previously, yet was never hacked.

- **Three people held guilty in on line credit card scam**

Clients charge card points of interest were abused through online means for booking air-tickets. These offenders were gotten by the city Cyber Crime Investigation Cell in Pune. It is discovered that points of interest abused were having a place with 100 individuals.

Mr. Parvesh Chauhan, ICICI Prudential Life Insurance officer had sobbed for the benefit of one of his client. In such way Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were gotten. Lukkad being used at a private establishment, Kale was his pal. Shaikh was utilized as a part of one of the branches of State Bank of India .

As showed by the information gave by the police, one of the customer got a SMS based alert for getting of the ticket despite when the charge card was being held by him. Customer was alert and came to know something was fishy; he enquired and came to consider the manhandle. He achieved the Bank in this regards. Police watched commitment of various Bank's in this reference.

The tickets were book through online means. Police asked for the log subtle elements and got the data of the Private Institution. Examination revealed that the points of interest were acquired from State Bank of India . Shaikh was working in the Master card office; because of this he approached charge card subtle elements of a few clients. He gave that data to Kale. Kale consequently passed

[6] http://www.cyberlawsindia.net/cases.html

this data to his companion Lukkad. Utilizing the data acquired from Kale Lukkad booked tickets. He used to pitch these tickets to clients and get cash for the same. He had given couple of tickets to different establishments.
Digital Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate got accompanied with eight days of examination lastly got the guilty parties.
In this respect different Banks have been reached; likewise four aircraft businesses were reached.

Privacy risks on social media

When someone joins a social network then that site aids a process to find phone numbers or friends in your contact list so that the site can make a connection between the user and the friends in their contact list to make the process easy for the user so that the user can connect with their friends easily and can stay in connect with them. However, in such process the network also get information of the user from their data which might the site is not supposed to.
This extra ability of collection of extra data of social platforms and curate this extra information is called shadow profiles which first came into light in 2013 as a Facebook bug. The bug unwittingly shared the email-id and phone numbers of the users of around 6 million with all of their friends which the users didn't even made the information public.

However, the Facebook immediately addressed the bug but even so, many of users found their phone numbers on the social sites which they didn't even filled on Facebook.

Garcia chased for designs in the information. A great many people don't have an arbitrary arrangement of companions. Hitched individuals have a tendency to be companions with other wedded individuals, for instance. In any case, individuals additionally have associations that entangle the capacity to foresee who's associated with who. Individuals who distinguished as gay men will probably be companions with other gay men, yet in addition liable to be companions with ladies. Straight ladies will probably be companions with men.

Utilizing this data, Garcia could demonstrate that he could foresee attributes, for example, the conjugal status and sexual introduction of clients' companions who were not on the web-based social networking system. Also, the more individuals in the interpersonal organization who shared their very own data, the more data the system got about their contacts, and the better the forecast about individuals not on the system got.[7]
Also a user is not in full control of their own privacy, if their family or friends are on the social platform and do share some pictures or information related to the user then the user can't do anything in that matter. The more you connect with other people, more is the probability of the leakage of information of the user, protecting privacy isn't something in your hands but also with whom the user is connected.[8]

Sharing pictures, videos, location, music is very common nowadays. Everything we

[7] by Bethany Brookshire

[8] Supra(4)

share violates our privacy. More sharing of data with more people increase the risks by privacy attackers and every piece of data we share hinders our privacy which violates our fundamental right.

Technically, violation of fundamental right remark as the grievous crime in our Indian constitution, however, violation of right to privacy by using these social sites happens in our day to day lives and no action can be taken against them. Thus, the enshrinement of right to privacy as fundamental right seems really absurd.

- **Puttaswamy vs. Union of India**[9]
  In this case justice K.S. Puttaswamy retired judge filed a petition in the supreme court in 2012 against Aadhaar project by saying that it infringes the right to privacy of citizens and challenged the constitutionality of Aadhaar.

  Aadhaar project, which aims to assemble a database of individual personality and biometric data covering each Indian. It issues a 12 digit number to every individual which is unique using specific biometric such as eye scan and finger prints. It was made mandatory by linking with filling tax returns, purchasing of 50,000 or above, securing loans, opening bank accounts, selling property etc.

  In August 2015, the case came in front of 3 bench judges who referred it to the larger bench of the court. In July 2017 5 bench judges ordered the matter to be heard by the 7 bench judges.

  Judgment : It is held that security is an unavoidably ensured right which rises, basically, from Article 21 of the Constitution. This isn't a flat out right yet an obstruction must meet the triple requirement of (ii) Legality; (ii) the requirement for a honest to goodness point and (iii) proportionality.

- **Kharak Singh vs. State of UP**[10]
  In this case the petitioner Kharak Singh was challenged in a case of dacoity, but got released as no evidence could be found against him. The police officers of Uttar Pradesh opened up a history sheet against him and brought him under surveillance.
  a) Secret picketing of the house
  b) Domiciliary visits at night
  c) Used to go through under inquiries on daily basis for all the activities, income, expenses, occupation
  d) Every movement was reported by chaukidars and constables, if there is an absence from home
  e) Verification of movements
  f) Collection and record of history sheet of all information

  Then the petition was filed in the supreme court by the petitioner under article 32 of Indian constitution, he challenged the constitution validity under chapter XX that the fundamental right has been infringed under articles 19(1)(d) i.e. right to freedom of movement and Article 21 i.e. right to life and personal liberty by the powers of police conferred to them.[11]

[9] https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/

[10] https://indiankanoon.org/doc/619152/

[11] http://indianexpress.com/article/explained/m-p-sharma-and-kharak-singh-the-cases-in-which-sc-ruled-on-privacy-4756964/

In the defence the defendant stated that there hasn't been any infringement of the fundamental right of the petitioner and even if they were, then they should be framed under the interests of the general public and public order and they should have been given the right to exercise there rights in the reasonable manner under the following circumstances.

Judgment : The petition was adjudicated by 6 bench judges in which they held that clause (b) i.e. domiciliary visits at night must be struck down as unconstitutional which is violative under Article 21 and the petitioner has right of *mandamus* against defendant to not continue domiciliary visits where the rest of the clauses could be upheld.
It was also stated that right to privacy is not guaranteed right under the Indian constitution therefore the attempt to check on the movements of someone can be in the manner of invaded the privacy but can't be stated as the infringement of the fundamental right under part III of the Indian constitution.

Cyber crimes and the IT laws

As the usage of computers became more popular which gave rise to the technology also and more people became familiar of the word Cyber. The advancement of data innovation offered ascend to the internet wherein web gives rise to chances to every one of the general population to get to any data, information accumulation, investigate and so on with the utilization of high innovation. What's more, because of the addition of the utilization of innovation abuse of innovation additionally raised up and the need of cybercrimes appeared at both local and universal level.
As the word crime describes its general meaning as legal wrong, cybercrimes would be described as unlawful acts relating to the computers, technology or accessing the internet in the wrongful manner.

There are certain types of crimes which affect the personality of individuals can be defined as :

- **Harassment via e-mails :** it is one of the most common type of harassment includes letters, sending messages, files via email. Harassment is common as usage of social sites like Facebook, Twitter, G-mail.
- **Cyber – stalking :** it creates fear of physical threats by using computer technology like Facebook, g-mail, phone calls, texts, webcam, website videos.
- **Dissemination of Obscene Material :** it includes obscene or lewd material like child pornography or indecent material to corrupt the mind of the adolescent to torture them.
- **Hacking :** it includes the unauthorized access or control over someone's computer system through which they can get in the touch of the data of the system by which they can black mail an adolescent or torture them, can also destroy the whole data of the system.
- **E-Mail Spoofing :** sometimes users get mail through unknown identity which represent their fake origin i.e. the mail shows origin of e-mail which is different from the actual origin.
- **SMS Spoofing :** it includes unwanted uninvited messages. Here a wrongdoer takes personality of another as cell phone number and sending SMS by means of web and recipient gets the SMS from the cell phone number of the casualty.

- **Carding :** it includes unauthorized use of ATM cards, can be credit card or debit card which the offender steals and misuse the cards for their monetary benefits.
- **Cheating & Fraud :** here the offender steals the password of someone's system and data storage with guilty mind to misuse them which results into fraud and cheating.
- **Child Pornography** : It includes the utilization of PC systems to make, appropriate, or get to materials that sexually misuse underage youngsters.
- **Assault by Threat :** here the offender threatens a person with fear of their lives or their family members lives via phone, texts, videos, e-mails etc.[12]

Need of Cyber Law:

Information technology has spread all through the world. The PC is utilized as a part of every last division wherein the internet gives measure up to chances to all to financial development and human advancement. As the client of the internet becomes progressively assorted and the scope of online cooperation extends, there is development in the digital violations i.e. rupture of online contracts, execution of online torts and wrongdoings and so on. Because of these results there was have to embrace a strict law by the internet expert to manage criminal exercises identifying with digital and to give better organization of equity to the casualty of digital wrongdoing. In the cutting edge digital innovation world it is particularly important to manage digital violations and in particular digital law ought to be made stricter on account of digital psychological warfare and programmers. [13]

Penalty For Damage To Computer System:

- According to **section 43**[14] of Information technology act 2000, whoever tries to commit any offence by hacking another system and tries to steal the data or try to destroy the system, deletes, alters or cause any disruption with the intention to harm someone's system or tries to misuse them without the permission of the owner then that person would be liable to pay fine up to Rs. 1 crore to the person who has been affected by the offender.
- According to the **section 43A**[15] which was inserted in 2008 under Information technology act where a body corporate maintains and protects the data and information of the users provided by the central government, if there is any negligent act in part of the corporate body which fails to protect the data or information then that body will be liable to compensate the person who got affected by this.
- **Section 66** deals with "hacking with computer system" which provides imprisonment for 3 years or fine which may extend up to 2 lakh rupees or both.

3 Important Cases That Highlight the Need to Take Care :[16]

[12] *Dhawesh Pahuja Advocate in Banglore*

[13] https://www.legalindia.com/cyber-crimes-and-the-law/

[14] Information technology act 2000

[15] Information technology (amendment) act 2008

[16] Andrew Hutchinson, Social Media, Privacy and Scams - 3 Recent Cases That Highlight the Need to Take Care *available at* ; https://www.socialmediatoday.com/news/social-

Every now and then a news story comes up that reminds you precisely how revealed we overall are through relational associations. Or then again perhaps not 'revealed', but instead 'accessible'. All that we say or do on social is traceable , prepared to be attributed back to us and there's a broad assortment of conduct by which people can use this information for wiped out purposes, if they were so arranged. In this manner, there were three news stories this week that went about as something of a refresher on the reliably contracting data region of our related world. Each case, in a surprising path, fills in as a sign of the ought to be careful in what we say, what we do and how we respond by methods for social stages - and the essentialness of remaining aware of how our data can be gotten to.

- **Arizona Facebook Scammers**

For this situation an Arizona lady was held subject for detainment for a long time for engineering an expense refund plot where she with her countrymen utilized Facebook information to discover and target individuals for identity burglary.
The procedure as follows :

- The scammers generally target unemployed people in their local area by using Facebook data.
- Then they contact their targets by using the information which they found using Facebook data by saying that, they are government officers or from some government agency who seek to help them out.
- The con artists at that point attempt to get more data through them with the goal that they could utilize it to influence an expense to guarantee for their benefit.

In this case the culprits were able to entangle dozens of people by obtaining their personal information which they used to make false tax claims. The motive of targeting the unemployed people was to reduce the risk of detection. There were many cases where the victims were unaware that their information had been stolen till they go to submit their own tax returns.

This sort of data fraud is on the ascent. By utilizing individual data accessible by means of Facebook profiles, sharp con artists can display exceptionally bona fide exchanges that would propose they are, indeed, authorities who approach your own records and can be trusted with your information. They'll frequently utilize qualifying questions the way official outlets would - something like "would i be able to simply put forth a couple of inquiries to affirm your personality?" Then they have a qualified posting of inquiries and answers that they've possessed the capacity to set up from your social profiles. With a particular accumulation of the information focuses they'll require, and with an offer being displayed, similar to a financial boost program, you can perceive how jobless individuals who may require a couple of additional bucks could be hoodwinked into giving over their information.

Key lesson : The case highlights the facts that no one should give detailed personal information to just any random person

media-privacy-and-scams-3-recent-cases-that-highlight-the-need-to/454720/

without having knowledge that who they are and where are they from.

- **F1 Driver Robbed**[17]

Formula 1 driver Jenson Button house had robbed in St. Tropez where Button and his wife were staying in rented holiday villa, where the thieves broke into and cleaned out and other things. The perspective was that the robbers might know about the location of Button and his wife and by keeping that in mind they broke the house when they were outside their villa.

The main question was that how could they have possibly know their location. The fact was that Michibata, wife of Jenson was broadcasting it via her Instagram account by tagging the location with all her pictures and that's how the robbers came to know about their location. This is how the burglars determined the best time to target the couple. It highlights that the users must be aware before sharing their location in public as it can be misused by anyone.
The same goes for pictures posted inside your home - on the off chance that you post a photo of your most recent DIY venture and there's a look at your costly home studio out of sight, you may very well make yourself an objective.

Key lesson : To guarantee you're just offering conceivably delicate data to individuals you know and trust. Likewise abstain from posting content that may connote that you're out of the house for a broadened time frame.

- **Imprisonment for 30 years for Facebook posts**[18]

In this case a 48 years old man, insulted the Thai Monarchy via Facebook which resulted him sentencing for 30 years imprisonment. The man posted 6 different Facebook posts and the original sentence for this was 60 years which further reduced to 30 years after admitting the commission of offence.

There are few nations which carry strict punishments in order to post contents on social media. People should consider what they are posting on social media as every picture or thought you post on social media even if it as a joke can come back to you.
This is especially applicable on account of those searching for work - while bosses need to apply some level of rational in surveying competitors in light of their online networking action, spotters are, undoubtedly, judging applicants on that substance. In case you're posting about how you 'loathe your activity', about how you're getting squandered each night, about participating in criminal movement, that substance will be utilized as a part of any appraisal of you, and keeping in mind that you may think not all businesses are doing this, investigate demonstrates that the developing dominant part are.

Key lesson : People should always be wise enough of what they are putting on social sites, if any post seems like an offensive one whether against public policy or seems insulted against government can be later used as assessments.

As our reality turns out to be more associated and is united through web-based social networking and online correspondence, so too are we more presented to mis-

[17] *ibid*

[18] Supra(16)

employments of our information and judgments in light of the substance we distribute. In the lion's share, this shouldn't be a noteworthy concern - the advantages of an online networking availability far exceed the negative ramifications on most fronts - however it is something we as a whole should know about. Stories like these help us to remember the should be cautious and receptive to potential issues as we approach our every day advanced communications.

Tips For Protecting Privacy On Social Media

- **Password :** By creating strong password; the stronger the passwords are, the harder it will be to crack down. One can make password strong by using some symbols, capital letters, using special characters or something personal which can't be easy to find out by any random person.
- **Avoid sharing sensitive information :** One should pay close attention while putting their information on social sites and try to avoid sharing any sensitive mater which could be mis used against them.
- **Privacy settings** : Social sites like Facebook gives us the opportunity for restricting access to certain friends, family members and colleagues. We can use the enhanced private setting options to reduce the harm like blocking the messages of strangers.
- **Antivirus software :** One must install a good antivirus software and antivirus- spyware that will protect the system from malware, viruses and spyware. Keep in mind to update the software time to time with all the latest malware definitions.
- **Online posts :** When you utilize web-based social networking, you are essentially posting individual data on the web. Exactly when that information gets posted on the web, it is never again private, and may end up falling into wrong hands. Despite whether you have set up the most dumbfounding possible well being endeavors, some of your sidekicks, partners and associations you speak with by means of online systems administration media, can end up discharging your own information. Thus, you ought to be greatly wary about what you post on the web, else, you will end up giving the possible hoodlums, stalkers, advanced oppressive bastards and identity tricks the information they require to cause hurt.[19]
- Watch your mailbox : Sometimes we get mails from unknown origins which contain links to be clicked , one should be aware of that , cause sometimes the viruses spread through links are so strong which can destroy our system very badly.
- Don't be too personal : Nowadays almost everyone put their date of birth, residence, phone number, schools or colleges they get on social sites as information. Imagine how easy for some random person to find about you which can be misused in any way. Thus one must think before post anything on social media.
- **Lock your phone :** Your phone can end up in any stranger's hand, and as all the social sites can be easily accessed through mobile phones, the stranger can obtain your e-mail address, target your friends and can be mistreat in any way. Thus one must lock their phones.[20]

[19] Sam Cohen, Privacy Risk with Social Media, *available at; https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html*

[20] https://us.norton.com/internetsecurity-privacy-5-tips-for-social-media-security-and-privacy.html

- **Location :** It has became hobby of people to post their location wherever they go, though they do it just for fun but it can put them in danger situation or can say it's like a welcome board for kidnappers. So keep in mind before posting anything unusual.
- **Contest : "**Free iPad if you share this post, fill this form and get a new Playstation, win a trip to Switzerland if you visit this site…. We could go on and on. Are you really buying this?"
  As most of the messages we get are spams and other harmful intrusions, so one should not fall for this.
  Make sure that the contest really exists (a quick Google search), and make sure that the post is actually coming from the official account of a reputable company.[21]

Not Referring to Other Social Media Accounts : Numerous online networking stages enable you to fill in a profile field connecting over to your other interpersonal interaction accounts. Be that as it may, it can be a smart thought to keep up a detachment between accounts, particularly in the event that they include distinctive individual and expert characters. For instance, you won't not need LinkedIn groups of onlookers to discover your Facebook account. Abstain from associating these records to build the protection and security of your advanced characters.**Use two-factor authentication :** One can lock down their social sites like Facebook, Google, Twitter, Microsoft and other accounts with two- factor authentication. It means when one log in to their account, they will also need to enter a special code which site texts to their mobile phones. Some sites requires it each time when one log in, however, some sites only requires when one is using new device or web browser. Two-factor confirmation works perfectly to keep others from getting to your records, albeit a few people feel it's excessively tedious. In any case, in case you're not kidding about security, you'll endure the rubbing.

- **Turn on private browsing :** In the event that one doesn't need anybody to get to physically their PC then they should empower "private browsing" a setting accessible in each web program with the goal that nobody can perceive what were your history records or where you were hanging on the web. It erase treats, brief web documents, perusing history after they close their window.
- **Set up a Google alert for your name :** This is a basic method to watch out for anything somebody may say in regards to you on the web. It's simply an issue of disclosing to Google what to search (for this situation, your name), and in addition what sorts of site pages to seek, how regularly to look and what email address the web crawler giant should use to send you notices. Set up a Google alarm here. [22]

Conclusion

Social networks are a great way to make connection with others and to express the views with oneself and others. It helps the users to connect with the whole world and to remove the barriers between them because of space and time. It provides opportunities in vast manner and many organisations are making use of this medium in a better

[21] By Enric Oon, Ways to Protect Your Privacy on Social Media, *available at* ; https://en.softonic.com/articles/7-ways-to-protect-your-privacy-on-social-media-z

[22] http://techland.time.com/2013/07/24/11-simple-ways-to-protect-your-privacy/

practice. The world is getting closer by connecting through these mediums.

People are no longer depends on the media for the advertisement of any news as the internet is providing every information in very easy manner.

However, these social networking sites have its danger side too which can be proven very dangerous to humans by violating their right as right o privacy.

These perils are considerably to a greater extent a danger presently on account of the inexorably boundless pattern of enrolling on a few locales utilizing a solitary client account. In response to this situation, each Internet user must remain vigilant and governments must put more pressure on the operators of these sites in order to safeguard the security of Internet users.

Bibliography

- **Primary Source**
  - Section 43 and section 66 of information technology act, 2000
  - Section 43A of information technology (amendment) act, 2008
  - Article 21 i.e. Right to life and personal liberty of Indian constitution
  - Article 19(1)(d) i.e. right to freedom of movement of Indian constitution

- **Secondary Source**

- https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html
- https://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Lack-of-Privacy-Awareness-in-Social-Networks.aspx
- https://www.tandfonline.com/doi/full/10.1080/15228831003770775
- https://www.sciencenews.org/blog/scicurious/social-media-privacy-no-longer-personal-choice
- http://www.financialexpress.com/india-news/what-fundamental-right-to-privacy-means-and-what-it-doesnt-10-points-from-supreme-court-verdict/823334/
- http://www.cyberlawsindia.net/cases.html
- https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/
- https://indiankanoon.org/doc/619152/
- http://indianexpress.com/article/explained/m-p-sharma-and-kharak-singh-the-cases-in-which-sc-ruled-on-privacy-4756964/
- https://www.legalindia.com/cyber-crimes-and-the-law/
- Andrew Hutchinson, Social Media, Privacy and Scams - 3 Recent Cases That Highlight the Need to Take Care *available at ;* https://www.socialmediatoday.com/news/social-media-privacy-and-scams-3-recent-cases-that-highlight-the-need-to/454720/
- Sam Cohen, Privacy Risk with Social Media, *available at; https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html*
- https://us.norton.com/internetsecurity-privacy-5-tips-for-social-media-security-and-privacy.html
- By Enric Oon, Ways to Protect Your Privacy on Social Media, *available at ;* https://en.softonic.com/articles/7-ways-to-protect-your-privacy-on-social-media-z
- http://techland.time.com/2013/07/24/11-simple-ways-to-protect-your-privacy/

*****