Cyber Security Internship 2016

GURUGRAM CYBER CELL

PROJECT REPORT
ON

SOCIAL MEDIA CRIME

SUBMITTED BY:

ROSHAN KUMAR GAMI
DHARMVEER SHARMA
SHANTANU SHASTRI
KUMAR SHIVAM
VAASUDEV KALA
VRINDA SHARMA
PRASANNA KUMAR DASH
PIYUSH GANGWAR
SATYENDRA KUMAR

Under the Guidance of:
Rakshit Tandon

PREFACE

As in the other areas of society, social media has an impact on the law. Some have gone so far as to say that "social media is having transformation effect on the law and the legal profession". While this statement comes across to some as hyperbolic, there is plenty of evidence to support that social media plays an important role with in the Legal system. Arguably the most telling example is displayed on the court room where legal disputes are being won or lost based on the attorney's mastery of the social media.

Social media's reach is even felt in academia where a small but growing no. of school's have started to offer courses like social media and criminal law. This is the significance that law schools have resisted curriculum changes, especially those geared towards teaching students practically, ready-to-use skills. Of different of law most likely to be transformed by social media, criminal law is high on that list. This is because the field of law reaches to all segments of the society and touches wide spectrum of the individuals. This project explores the social media influence on criminal law by looking at how the key players.

In the criminal justice system namely individual citizens, law enforcement, attorney and judges interact with and use social media.

To combat this problem this project will not only examine the thorny legal and ethical questions that arise in the day to day use of social.

Media in the criminal law context but also will provide 10,000 foot overview on the social media role in criminal justice system as a whole.

This also will forecast the changes that social media will bring in the field of criminal law. To the date social media is being used to empower crime victims, assists virtual deputies, impeach witness, prove motives, investigate criminals, and carry out crimes, monitor jurors ,violate court rules , commit ethical violations, enhance sentences and to run undercover sting operations.

One of the distinguish features of the social media is privacy or lack thereof. Social media, more so than any form of communication, works to erode the privacy of its users. This occurs in variety of ways

a. With social media that users create friendship with the people that they don't really know in the traditional sense. That is most people who use social media have not interacted or physically met all their online friends.

a. Social media has lowered the barrier for self-discloser. Social media has created a new paradigm that default persons is to share once life experiences from the most routine to most intimate with the rest of the world.

b. Social media makes information conveyed by its users readily available for the others to access and find.

c. Social media combines an individual personal and professional life, which results in sharing information between the two.

Besides privacy, other distinguishing features of the social media include the speed by which user can contact large no. of peoples.

INDEX

ACKNOWLEDGEMENT

It is with great pleasure that we find our self-penning down these lines to express my sincere thanks to various people who helped us a long way for completing this project.

The harmonious climate in the cyber cell and the Commissioner of Police office provided proper guidance for preparing the project. It was a privilege to have been guided by Mr Rakshit Tandon.

Thanks to Inspector Sudhir Kumar State Cyber Crime Branch, Gurugram Police for his induction and training on live case studies.

Thanks to all our fellow mates who helped us during the development of this project with their constructive criticism and advice.

We would also like to thank the honourable Commissioner of Police Shri Navdeep Singh Virk for giving us such a good opportunity to get exposed and updated with the latest technology in the field of the cyber security.

ABOUT THE GUIDE

Director – A&R Info Security Solutions Pvt. Ltd.

Research and Development, Gov. of India

✓ Visiting Faculty-Lecturer at DR. B.R. Ambedkar Police Academy - Mora□ Consultant – Internet and Mobile Association of India.

✓ Member Advisory Board- National Cyber Safety & Security Standards (NCSSS)

✓ Trustee - "Cyber & Law Foundation" An International NGO involved in Policy, Research & Training related to Cyber & Privacy Issues.

✓ Advisor- Cyber Crime Unit, Uttar Pradesh Police, Agra.

✓ Advisor – Cyber Crime Cell, Gurgaon, Haryana Police.

✓ President- JAT (Joint Action Team) for combating Cyber Crime against Women and Children.

✓ Consultant - AIWEFA (All India Women's Education Fund Association).

✓ Resource Person- BPRD Bureau for Police dabad (U.P) Haryana Police

✓ Academy -Karnal, Police Radio Training School, Indore, CDTS (Central Detective Training School)

Chandigarh, Jaipur and Ghaziabad, Rajasthan Police Academy, Internal Security Academy CRPF, Mount Abu.

✓ Guest Lecturer at Chandigarh Judiciary Academy.

ABSTRACT

The most popular form of social media is social networking, which consists of websites that allow users to create an online profile in which users post up-to-the-minute personal and professional information about their lives that can include pictures, videos, and related content.

Websites under this category include Facebook®, LinkedIn®, Twitter®, and the now nearly defunct Myspace®. Social networking is a potential gold mine for criminals who leverage the users' personal details into financial opportunity.

The attacker attacks on social media profile of a person & try to get some information by means of which they get access to their financial system as well as their personal life & start abusing(harassment, cyber stalking, defamation etc.). This project's aim is to create awareness among people & provide security to the social media.

1.0 INTRODUCTION

Social media has caught the imagination of India – no wonder, then, that Indians are among the most active on such platforms. The mobile revolution has further ensured that social media is growing as people now access social media through various applications and devices.

The easy availability of access to social media on the go has also triggered the phenomenon where people invariably post information on social media without understanding its ramifications. A number of times, people post content on various social media sites like Facebook, Twitter, Pinterest etc on the spur of the moment or on an impulse without thinking it through.

The tremendous rise in popularity of social media over the past five years has led to a drastic change in personal communication, both online and off. The popularity of sites such as Facebook®(750 million active users)1, YouTube® (nearly 500 million users)2, and Twitter® (200 million users)3 has made communication for people not only convenient, but downright instantaneous–allowing users to connect and communicate with anyone using the Internet in seconds. In addition to personal usage, businesses and the public sector use social media to advertise, recruit new employees, and maintain partnerships. In fact, social networking now accounts for 22% of total time spent on the Internet. With social media being adopted by so many in society, it's only fitting that white collar and hi-tech criminals adapt their skill set to the ever-changing landscape of the Internet. This white paper will discuss how criminals are using social media and Web 2.0 technologies to perpetrate new and classic white collar crimes.

2.0 SOCIAL MEDIA

Social media is difficult to define at times, but for the purposes of this paper, social media will be defined as any website or software that allows you to receive and disseminate information interactively. This especially includes websites that allow you to read social updates or an informative article and moments later being able to respond with a text update, post a video, or stream audio. There is a variety of different formats of social media that equip users with the ability to share information. The following will discuss these formats and their potential for criminal use.

The most popular form of social media is social networking, which consists of websites that allow users to create an online profile in which users post up-to-the-minute personal and professional information about their lives that can include pictures, videos, and related content. Websites under this category include Facebook®, LinkedIn®, Twitter®, and the now nearly defunct Myspace®. Social networking is a potential gold mine for criminals who leverage the users' personal details into financial opportunity.

3.0 SOCIAL MEDIA NETWORKING

A social network service is created to build online communities of people who share interests. They are Web- based and provide a variety of ways for users to interact, such as e-mail and instant messaging services. Social networking has encouraged new ways to communicate and share information. Such Web sites are used by millions of people every day.

The popularity of social networking sites has grown tremendously in the last few years. They help people stay in touch. They help small businesses connect with other businesses and clients. They give people the chance to network with people they'd never be able to meet otherwise. However, with the growing popularity and mainstream use of these sites, there's also a dangerous side. There have been many hackers and scammers. People can create fake profiles. It becomes easier to break privacy and copyright laws. And most recently, these sites have become an avenue for crimes. Criminals have even used social networking sites to boast about crimes they've committed.

4.0 SOCIAL MEDIA CRIME

The popularity of social media has also attracted criminals. 81 percent of Internet-initiated crime involves social networking sites, mainly Facebook and Twitter. These platforms are ideal sources for criminals to obtain personal information from unsuspecting people. The vast majority of cyber crimes consist of identity theft, phishing schemes, fraud, and data mining. One in five adult online users report that they were the target of cyber crime, while more than a million become victims of cyber crime every day. Estimates regarding the financial cost of cyber crime range from $100 billion to an enormous $1 trillion a year in the U.S. This shows how difficult it is to measure the exact financial damage caused by cyber crime. Yet, Internet-initiated crime doesn't always play out online. Social networking sites are also very helpful platforms for burglars, sex offenders and other crooks. For instance, 78 percent of burglars admit that they use social media to seek out their victims. Google Street View allows them to gauge their victims' properties over the Internet. Moreover, the smartphone apps for Facebook, Twitter, Instagram, Vine and Foursquare all operate with geotags which can reveal your exact whereabouts, thus informing potential burglars when you're away from home. It is highly recommended that you disable the geotagging function on your smartphone, at least when it comes to the social networking apps you use.

Furthermore, 33 percent of all Internet-initiated sex crimes are orchestrated through social networking sites, and 50 percent of sex crimes committed against a minor involve the perpetrator obtaining information/pictures from the victim's social media profile. The latter becomes even more disconcerting if you consider that more than a quarter of Facebook users are under the age of 10 and almost 40 percent are under the age of 13 (the minimum age requirement for most social networking sites). These young Internet denizens use social networking platforms largely without their parents' supervision. They often disclose sensitive information like their real age, pictures, the city they live in or the school they attend, making them easy targets for potential predators. The core elements of contemporary performance crimes are that they are created for distribution via social media and involve both willing and unwilling performers. Performance crime can be of two types. The first is a sort of 'informed consent' performance where the actors are aware of the production (sometimes recording or filming it themselves) and at least tacitly support its subsequent distribution — in this sense a crime performer is 'behaving for the camera' similar to an actor in a play. The second involves an uninformed, unwitting performance produced without performer knowledge or acquiescence — here a person is being recorded in a production similar to a nature documentary. Social media have caused performances of both types to explode.

These performances are no longer rare events place and time bound to physical stages and scheduled broadcasts; they are now ephemeral renditions constantly created and digitally distributed. This change came about with the transition from legacy to new media which in turn has brought about changes in society and created new stressors on criminal justice systems. The content and portrayals of crime and justice in new and legacy media look similar and the transition from one to the other has been largely seamless. The result has been a muted recognition of the substantial impact of the shift on crime and justice and the subsequent emergence of performance crime.

4.1 TYPES OF SOCIAL MEDIA CRIME

There’s no doubt that social media has completely revolutionized the way people interact. But there’s a dark side to the world’s love affair with social media. Criminals are finding new ways to commit new and disturbing crimes that authorities don’t necessarily know how to police. That’s why if you want to continue to enjoy social media, you should be aware of the common crimes committed on it so that you can avoid becoming a victim. Here are the seven most common social media crime:

4.1.1 Scams

Criminals have been utilizing the scam for centuries. In the social media world, scams are particularly effective at drawing people in by simply enticing an individual to click on a link that would interest almost anyone, such as an innocent-looking notification that you’ve won a free prize like a gift card. Then, in order to claim the prize, scammers require you to submit some information, such as a credit card number or Social Security number. This description may make it seem like scams are easy to spot, but even the most savvy social media user has to be on the lookout for illegitimate requests for information.

4.1.2 Cyberbullying

Cyberbullying is a common occurrence among teenagers on social media and one that can result in serious criminal charges if it goes far enough. Cyberbullying on social media has contributed to the deaths of several teens who either committed suicide or were killed by a peer. Cyberbullying that involves hacking or password and identity theft may be punishable under state and federal law. When adults engage in this kind of online behaviour it is called cyber-harassment or cyber-stalking.

4.1.3 Stalking

The term “stalking” is thrown around a lot on social media, and it is often meant as a joke for regularly looking at someone’s profile. However, the actual act of cyberstalking is a common crime on the social networking site and can result in a serious offense. Cyberstalking typically involves harassing a person with messages, written threats, and other persistent online behaviour that endangers a person's safety. Although cyber stalking may seem like nothing more than annoying behaviour, it is a legitimate cause for concern in many cases and can even lead to in-person stalking or endangerment if not treated seriously.

4.1.4 Robbery

It doesn't take much for a thief to find out where you live, go to school, work, or hang out if you make that information readily available on social media. If you use Facebook's check-in or Google Maps feature, then you could be in a heap of trouble if a robber is paying attention. This person isn't always a complete stranger either; they may be an old acquaintance or someone else you'd never expect to come rob you.

4.1.5 Identity theft

With the large amount of personal information swarming around social media these days, it has become fairly easy for criminals to steal users' identities. Hackers often break into users' e-mails and make fake Facebook accounts. From there they can access personal and bank information and cause havoc to your sense of security. Protect yourself from identity theft on Facebook by keeping your profile very secure and free of personal information that a criminal would love to have.

4.1.6 Defamation

An individual commits the crime of defamation when they communicate a false statement to a third party that paints another individual or entity in a negative light. Social media makes communicating defamatory statements frighteningly easy, and the exposure Facebook provides makes it more likely that businesses or individuals will be harmed by the defamatory statement, and thus more likely to pursue legal remedies. Be careful what you say on Facebook; you may be committing a crime without even knowing it.

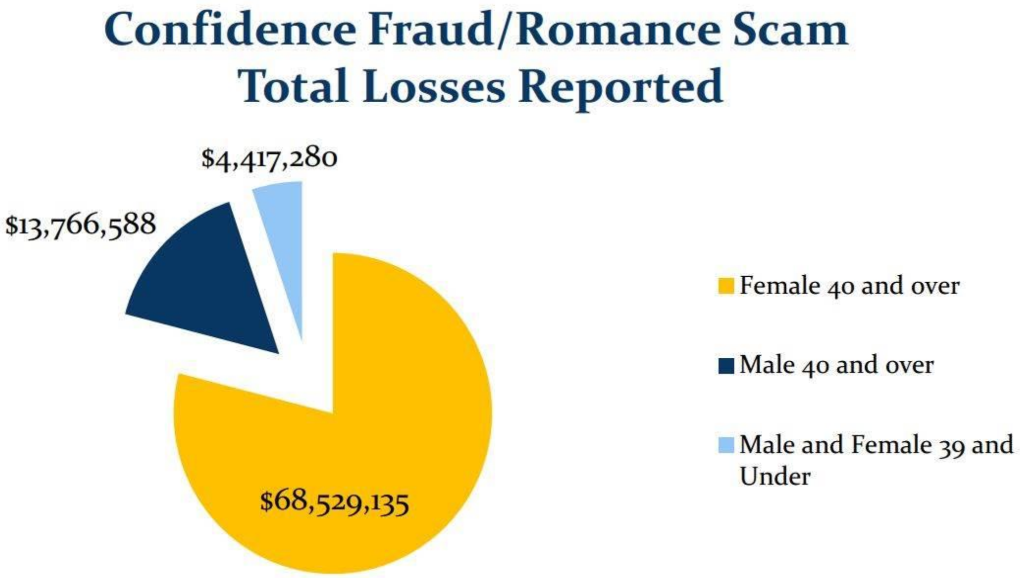
4.1.7 Harassment

Harassment happens all the time on social media. From sexual harassment to assault threats, there has been a significant increase in the number of harassment cases happening on Facebook. It's not uncommon for sex offenders and sexual predators to prey on unsuspecting victims on Facebook and even pose as a teen or college student. Harassing messages, inappropriate comments, and other persistent behaviours should be reported to Facebook and your local police station.

4.2 STATUS OF INDIA ON SOCIAL MEDIA CRIME

Creation of Attractive messages which lure the user to click a malicious link that compromises private data.

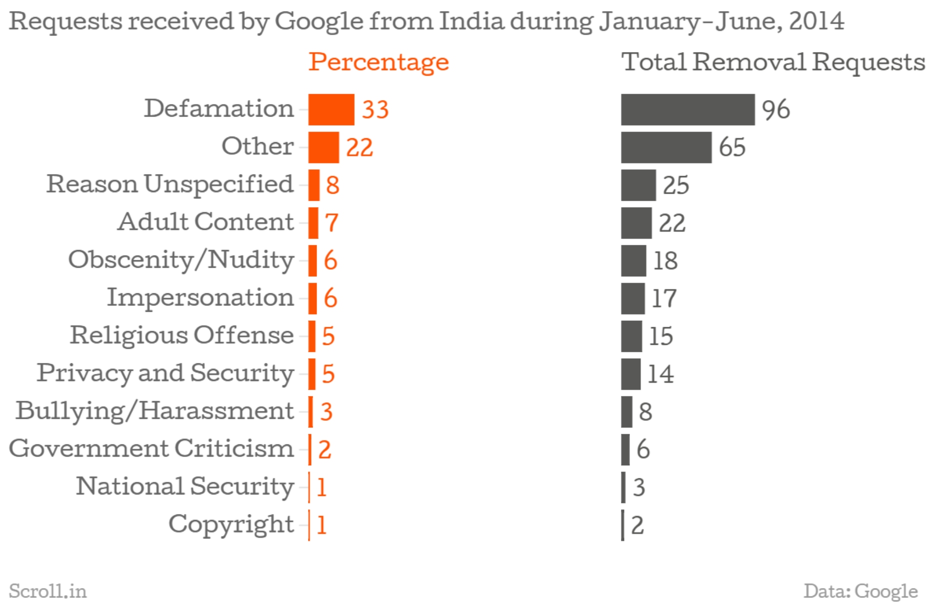
These messages on social media contain exciting offers which asks the users to make payment for availing the offer, the amount is taken and none of the users are entertained.



4.1.1 Defamation:

a. Fake Profiling: Creating a profile with the name of an existing user and organization and publish contents in the name of the person/organization.

b. Abusive Posts: Sharing posts which contain abusive words, slangs, or any vulgar morphed images which aim at defaming the person.



c. Obscenity**:** Any offensive, pornographic or disgusting content in the form of post or advertisements come under this category.

Unique Case of Obscenity in India

In 2012, two girls were arrested because of a post that one of them wrote. The post questioned why the entire city had to be shut down on account of the death of Shiv Sena’s Head, Bal Thackeray.

4.1.2Stalking/Harassment/Blackmailing:

This is the case where psychopathic or ego-concerned people stalk other people through their social media profiles and carry out criminal activities. Cases mostly include Boys (who had previously been in a relationship). Once they get their ego-hurt; they upload compromising pictures, videos and morphed images of the victim. Blackmailing HER for ransom in exchange of not sharing the private content on social media or websites.

a. Honey Trap:

It’s one of the trending crimes over social media. Females (mostly over the age 22 single/divorced) are targeted and lured towards a friendship. Further, the friendship gets converted into *“attractiveness or love”*. This all is done after creating a fake profile in the name of a rich foreigner (mostly divorced parent).Then, the following cases happen:

a. Sharing of compromising pictures and videos from the feminine side.

b. Blackmailing HER for ransom in exchange of not sharing the private content on social media or websites.

OR

c. The criminal gains complete confidence of the victim through his friendship.

d. The criminal asks the victim to pay CUSTOM DUTY AMOUNT for the shipment (an expensive gift sent by him).

e. The victim pays a huge amount of money under the trust that the person is really sending an expensive gift.

f. The money is withdrawn and there doesn’t exist any trace of the so called “foreigner”.

(i) Anti-Religious Posts/ Hate Speeches:

Sometimes, for the motive of creating riots and influencing people to follow uncontrolled mob to disturb law and order in a particular area, hate speeches are posted on social media.

An unauthentic source posts something vulgar/disturbing about a community or an influential person and this goes viral on social media.

Morphing the images of Gods and Goddesses for the purpose of revoking hatred in the religious beliefs of other people. This leads to disturbance among law and order.

(ii) Pornography :

Sharing pornographic content on social media is a punishable offence. Any content shared, if without the consent of the person involved in pictures/videos is also criminal offence.

(iii) Human Trafficking :

Deep Web is not accessible to everyone. But it has been proven that somewhere, online human trafficking takes place and children and women are sold within and to foreign countries.

(iv) Arms Smuggling:

Similar to human trafficking, terrorists and other criminals are buying weapons online. If this type of facility is not banned, it will definitely destroy world peace.

(v) Terrorist Activities :

Terrorists are interacting on private chat windows of online games. As the cellular networks or calls can be traced, they have now started using chat windows like Sony PsP forums, Clash of Clans chat windows. It is very difficult to trace such chats or monitor them.

(vi) Radicalism :

Many people are being radicalised online by the means of videos which try to encourage and motivate the viewer towards terrorist activities.

This can be very destructive if watched very seriously or if it saves a message in the users' minds.

(vii) Sexting :

"Virtual Sex" or Sexting refers to chats between people which contain private compromising messages, semi-nude/nude images and videos being shared between two people.

4.3 Statistics of Social Media Crime In India In 2015

- India ranks 2nd in social media scams
- India ranked 3rd in Asia for ransomware attacks
- India is 6th most bot-infected country
- About 65% of bot infections reported in metros
- 34% of cyber-attacks in India were targeted at small businesses
- India saw seven ransomware attacks per hour; 170 per day; about 60,000 in 2014
- Cyber criminals are using social media, apps
- Globally, 70% of social media crimes fooled users to manual sharing of scams

While emails are still the more prevalent means of cyber-attack, the report said attackers are using social media as a "ready base" for crime as they continue to experiment with new attack methods that reach more people with less effort.

Globally, 70 per cent of the attacks on social media fooled users to manually share scams, followed by fake offerings, hitting the "like" button, commenting or through fake applications.

Separately, the report said, seven internet users in India faced "ransomware" attacks every hour in 2014, in which their devices were restricted by attackers who demanded ransom to remove the restrictions. India saw 170 ransomware attacks a day in 2014, taking the number of such attacks to 60,000 during the full year, the report said.

Ransomware is a type of malware that restricts access to the device that it infects, and demands a ransom paid to the creators of the malware for the restriction to be removed.

"While social media scams can provide cyber criminals with quick cash, some rely on lucrative and aggressive attack methods like ransomware. Last year, ransomware rose 113 per cent globally. India reported the third highest ransomware in Asia, with an average of more than seven attacks every hour," Symantec said.

Unlike the ransomware attacks in the US where attackers pretended to be law enforcement, seeking a fine for stolen content, the attacks in India were more crypto-ransomware where files, Photographs and other content of the user are held hostage without masking the attacker's intention, the report said. As many as 86 per cent of all the ransomware attacks in India were crypto-ransomware, posing a threat to consumers as well as companies.

5.0 Legal Aspects

The law in India is crystal clear regarding your publications on social media. The Information Technology Act, 2000, categorically makes you liable should you post any incriminating or illegal content or material on social media. In fact, the law has gone even further and recognises you, providing content on social media, to be a content service provider and network service provider. Hence, the law recognizes social media users as network service providers and hence, intermediaries under the law.

Indian cyber law requires intermediaries, including users of social media, to exercise due diligence while they discharge their obligations under the law.

Of late, we are witnessing tremendous misuse of social media. The recent case of a man being lynched to death on mere rumours of his storing beef has caught national headlines. Investigations by the Police have revealed that the said incident has also lead to fuelling of social media activities. That is the reason Uttar Pradesh Chief Minister Akhilesh Yadav directed his administration to take stern action against those “creating disharmony and inciting hatred” by circulating “baseless” content on social media. As such, the police have written to Twitter to disable and remove pictures and content that might create communal disharmony. Twitter as an intermediary is duty bound under Indian cyber law to comply with these directions.

Seen from a holistic perspective, the present case represents a new trend. We have seen earlier cases where people have posted objectionable or illegal content on social media sites like Twitter, but there has not been much action in this regard. The action by Uttar Pradesh Police authorities represent a new trend where increasingly now service providers and intermediaries can be called upon by governments to remove or disable access to communally sensitive content, as well as also force them to give the details of the persons behind the same.

At a time when various elements are misusing social media, such an exercise is essential so as to not only bring to book the guilty people as also to ensure that people do not continue to misuse social media with impunity.

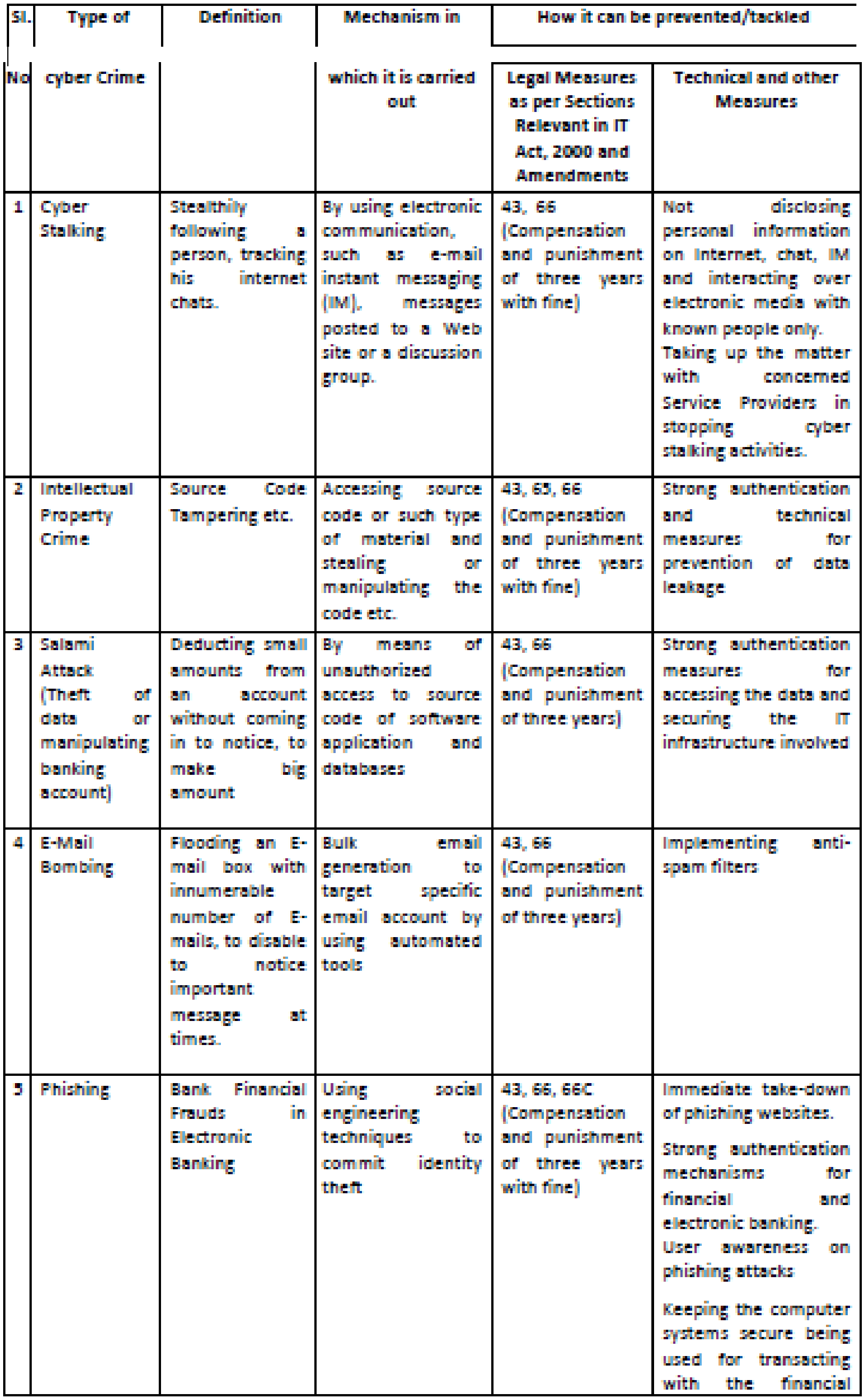
In the Shreya Singhal case, the Supreme Court has already held that the intermediaries are duty bound when they are called upon by any order of the government to move or disable access to any information as well as provide relevant connected information pertaining to identity of the offenders. I believe this power is a very special power which has been conferred under the Information Technology Act, 2000, and needs to be more frequently used.

We should also be realistic that given the rapid growth of social media in India, it will take some time before the maturity curve acquires a stable basis. Till such time as adequate self-policing mechanisms are not built within the social media networks, it is but natural that powers like those given to the government to give directions to service providers will be used more frequently.

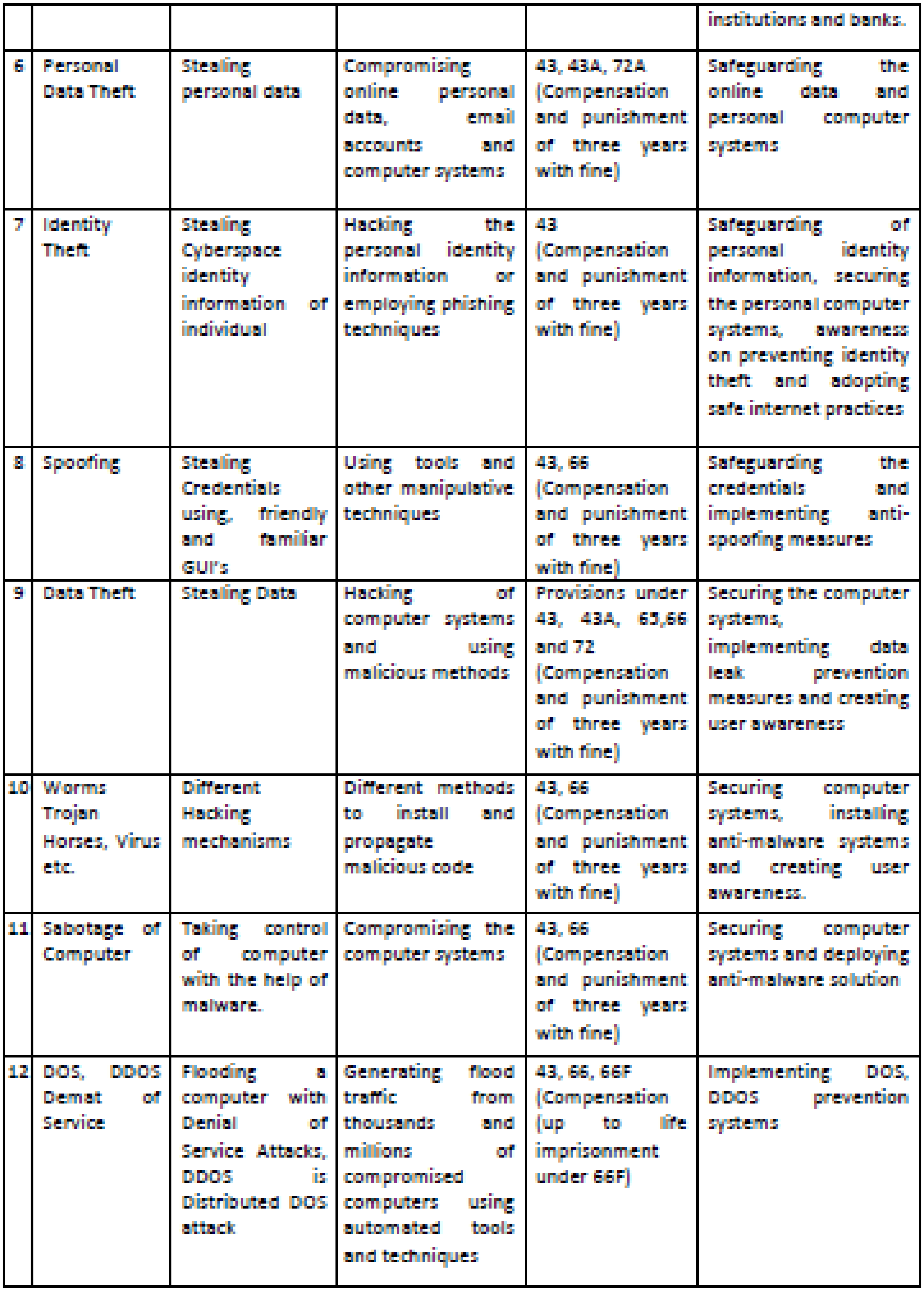
The learnings from the present episode are crystal clear. No one should ever feel that the Internet is the ‘wild, wild West’ and that they can hide behind the so-called cloak of anonymity on the Internet or social media to engage in any illegal or criminal activities. Any illegal or criminal activity done by any person on social media leaves electronic footprint or trails which can always be used for the purposes of identifying the real person and prosecuting him for legal consequences. Due diligence has to be the only mantra for all the social media users. It is always wise to never publish any content on social media on an impulse or when one is in an emotional state of mind. One should always revise content which one needs to upload and see whether there could be any potential legal consequences. It is always better to take precautions rather than being adventurous and facing undesirable legal consequences later.

The jurisprudence on social media misuse in India is only beginning to evolve. As a nation, we have just very few cases pertaining to misuse of, and cybercrime on, social media. However, given the speed of adoption of social media, it is but natural to expect that more and more cases of misuse of social media need to be registered, investigated and prosecuted. Further, the focus of the prosecution must be to try to get convictions so as to give a message to the entire community that social media is not a free-for-all ecosystem but a medium that is appropriately regulated by rule of law. The entire issue of social media misuse is a constantly evolving paradigm. It will be interesting to see how jurisprudence on social media misuse in India evolves with the passage of time.

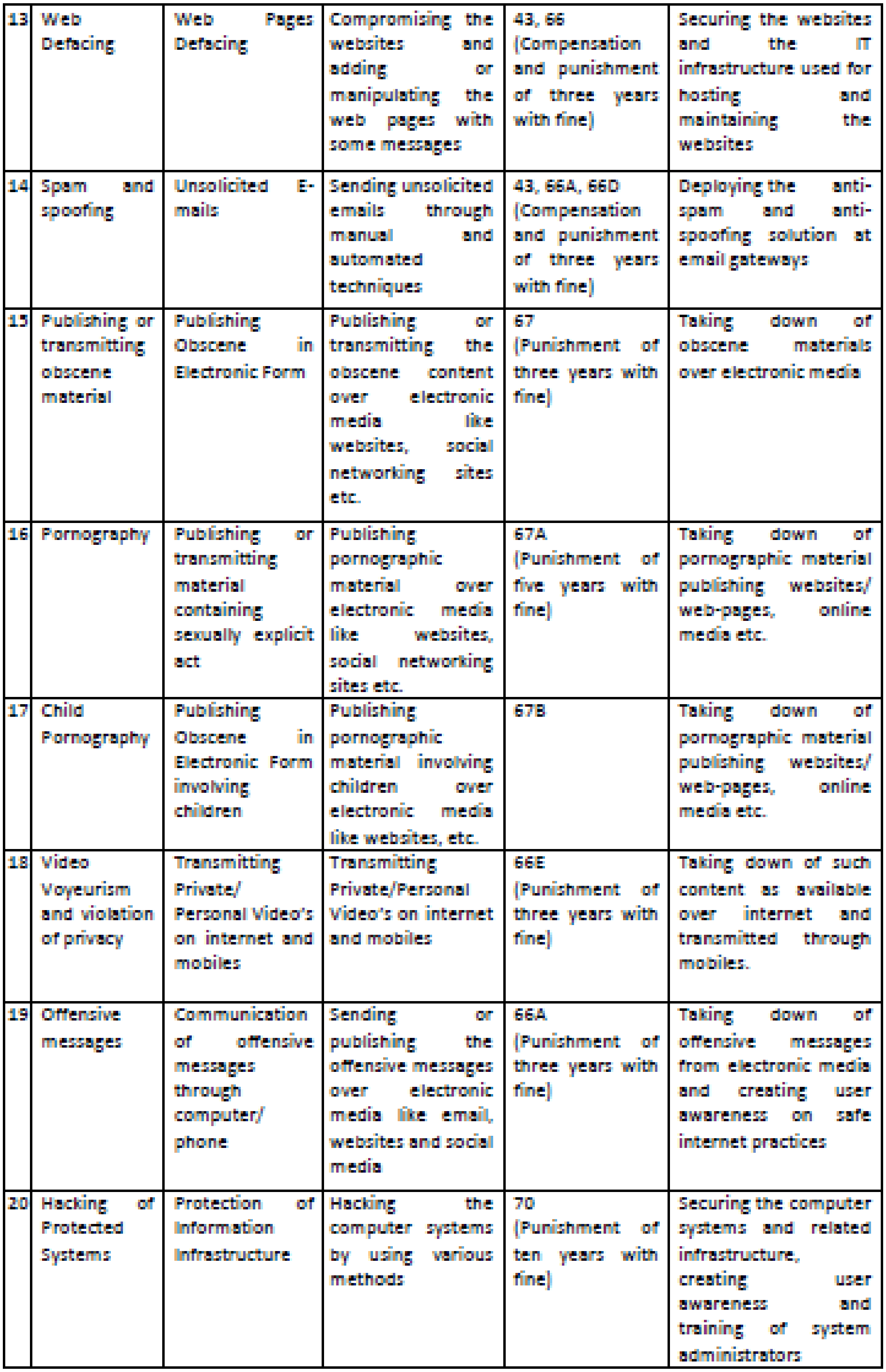
6.0 Provisions In IT ACT 2000



Sl. No	Type of cyber Crime	Definition	Mechanism in which it is carried out	How it can be prevented/tackled	
				Legal Measures as per Sections Relevant in IT Act, 2000 and Amendments	Technical and other Measures
1	Cyber Stalking	Stealthily following a person, tracking his internet chats.	By using electronic communication, such as e-mail instant messaging (IM), messages posted to a Web site or a discussion group.	43, 66 (Compensation and punishment of three years with fine)	Not disclosing personal information on Internet, chat, IM and interacting over electronic media with known people only. Taking up the matter with concerned Service Providers in stopping cyber stalking activities.
2	Intellectual Property Crime	Source Code Tampering etc.	Accessing source code or such type of material and stealing or manipulating the code etc.	43, 65, 66 (Compensation and punishment of three years with fine)	Strong authentication and technical measures for prevention of data leakage
3	Salami Attack (Theft of data or manipulating banking account)	Deducting small amounts from an account without coming in to notice, to make big amount	By means of unauthorized access to source code of software application and databases	43, 66 (Compensation and punishment of three years)	Strong authentication measures for accessing the data and securing the IT infrastructure involved
4	E-Mail Bombing	Flooding an E-mail box with innumerable number of E-mails, to disable to notice important message at times.	Bulk email generation to target specific email account by using automated tools	43, 66 (Compensation and punishment of three years)	Implementing anti-spam filters
5	Phishing	Bank Financial Frauds in Electronic Banking	Using social engineering techniques to commit identity theft	43, 66, 66C (Compensation and punishment of three years with fine)	Immediate take-down of phishing websites. Strong authentication mechanisms for financial and electronic banking. User awareness on phishing attacks Keeping the computer systems secure being used for transacting with the financial



					institutions and banks.
6	Personal Data Theft	Stealing personal data	Compromising online personal data, email accounts and computer systems	43, 43A, 72A (Compensation and punishment of three years with fine)	Safeguarding the online data and personal computer systems
7	Identity Theft	Stealing Cyberspace identity information of individual	Hacking the personal identity information or employing phishing techniques	43 (Compensation and punishment of three years with fine)	Safeguarding of personal identity information, securing the personal computer systems, awareness on preventing identity theft and adopting safe internet practices
8	Spoofing	Stealing Credentials using, friendly and familiar GUI's	Using tools and other manipulative techniques	43, 66 (Compensation and punishment of three years with fine)	Safeguarding the credentials and implementing anti-spoofing measures
9	Data Theft	Stealing Data	Hacking of computer systems and using malicious methods	Provisions under 43, 43A, 65,66 and 72 (Compensation and punishment of three years with fine)	Securing the computer systems, implementing data leak prevention measures and creating user awareness
10	Worms Trojan Horses, Virus etc.	Different Hacking mechanisms	Different methods to install and propagate malicious code	43, 66 (Compensation and punishment of three years with fine)	Securing computer systems, installing anti-malware systems and creating user awareness.
11	Sabotage of Computer	Taking control of computer with the help of malware.	Compromising the computer systems	43, 66 (Compensation and punishment of three years with fine)	Securing computer systems and deploying anti-malware solution
12	DOS, DDOS Demat of Service	Flooding a computer with Denial of Service Attacks, DDOS is Distributed DOS attack	Generating flood traffic from thousands and millions of compromised computers using automated tools and techniques	43, 66, 66F (Compensation (up to life imprisonment under 66F)	Implementing DOS, DDOS prevention systems



13	Web Defacing	Web Pages Defacing	Compromising the websites and adding or manipulating the web pages with some messages	43, 66 (Compensation and punishment of three years with fine)	Securing the websites and the IT infrastructure used for hosting and maintaining the websites
14	Spam and spoofing	Unsolicited E-mails	Sending unsolicited emails through manual and automated techniques	43, 66A, 66D (Compensation and punishment of three years with fine)	Deploying the anti-spam and anti-spoofing solution at email gateways
15	Publishing or transmitting obscene material	Publishing Obscene in Electronic Form	Publishing or transmitting the obscene content over electronic media like websites, social networking sites etc.	67 (Punishment of three years with fine)	Taking down of obscene materials over electronic media
16	Pornography	Publishing or transmitting material containing sexually explicit act	Publishing pornographic material over electronic media like websites, social networking sites etc.	67A (Punishment of five years with fine)	Taking down of pornographic material publishing websites/ web-pages, online media etc.
17	Child Pornography	Publishing Obscene in Electronic Form involving children	Publishing pornographic material involving children over electronic media like websites, etc.	67B	Taking down of pornographic material publishing websites/ web-pages, online media etc.
18	Video Voyeurism and violation of privacy	Transmitting Private/ Personal Video's on internet and mobiles	Transmitting Private/Personal Video's on internet and mobiles	66E (Punishment of three years with fine)	Taking down of such content as available over internet and transmitted through mobiles.
19	Offensive messages	Communication of offensive messages through computer/ phone	Sending or publishing the offensive messages over electronic media like email, websites and social media	66A (Punishment of three years with fine)	Taking down of offensive messages from electronic media and creating user awareness on safe internet practices
20	Hacking of Protected Systems	Protection of Information Infrastructure	Hacking the computer systems by using various methods	70 (Punishment of ten years with fine)	Securing the computer systems and related infrastructure, creating user awareness and training of system administrators

7.0CASE STUDIES FOR SOCIAL MEDIA CRIME

CREATION OF FAKE FACEBOOK ID TO DEFAME A FACEBOOK FRIEND

On 1st may 2016 Commissioner of Police Gurugram (Haryana) received a complaint from Mr. Ramesh resident of Palm Vihar, Gurugram about an unknown person who has created a fake Facebook id of his daughter aged 14 years. In that, he mentioned about some unknown person who has created a fake Facebook id in the name of his daughter Meenashi. In this, he used her photo in the account and also attached the photograph from adult websites with comments from her side like to pose her as a online call girl and these photographs were uploaded to his Facebook group which were accessible to the all group friends. This unwanted activity was disturbing the whole family and especially the girl who was being defamed for no reasons. The girl was feeling very depressed and confused with the issue and unable to concentrate on her day-to-day life.

CASE FOLLOWUP

On the basis of complaint given by Ramesh, the case was referred to Haryana State Cyber-Crime Branch, Gurugram by Commissioner of Police. A complaint no. 296 dated 01 May 2016 was made. In the process of investigation Cyber Crime Branch asked the father and daughter were asked to give the user details of the Facebook id as there was no clue available with the police based on their verbal investigation with the family. The family could not give any suspicious name behind the act. After receiving the user details, the Cyber Crime Branch under section 91 of CrPC act took up the case on 2nd May 2016 with Facebook asking the following details about the fake Facebook id.

a. Creation of IP
b. Login and logout details of IP from creation date
c. Alternate mail id and contact numbers.
d. Password change of IP if any
e. Request for blocking the account

The above mentioned details were made available to Cyber Crime Branch, Gurugram in around one month time. After receiving the log details the police started finding the most suspected person based on the mobile nos. The police based on the mobile no, approached the service provider for individual details of the person. This mobile no. was in the name of Mr. Mohan. Then Mohan was contacted on his other mobile no. to maintain the secrecy of matter. It came to notice that his son was using Mr. Mohan's first no. which was found in the victim's mail. Thereafter, the police asked Mr. Mohan to come along with his son to the police station for further investigation. The police also asked Mr. Ramesh and his daughter to be present during the investigation process at the Cyber Crime Branch. During the investigation, Mr. Mohan's son Ajay accepted his fault. Further effort were made to find motive behind the Crime. The girl and boy are studying in the same school and they were Facebook friends. Ajay mentioned that there was no specific motive behind the act but he was experimenting with the social media and for that he was feeling ashamed and apologetic.

CASE DISPOSAL

Since Mr. Ramesh didn't want to pursue the case further after knowing the source person. A Maafinama was rendered by Mr. Ajay on behave of his son which was acceptable to Mr. Ramesh. All the account and the details were deleted from the fake Facebook account by the Facebook. The boy also ,promised that he will not do such activity in future. The families were satisfied with the investigation and its outcome. For that, a mutual agreement was signed by both parties for closing the case. The Cyber Crime Branch, Gurugram made the final report on 17 May 2016 and sent it to Commissioner of Police, Gurugram for final disposal.

LEGAL OPTIONS

The case was handled promptly by Gurugram Police & well responded by Facebook. In case the complainant would have not been satisfied with the outcome then, the case could have been processed under IT Act 2000 Section 66C (Identity Theft) and Section 66D (Personation). The Section 499 & 500 (Defamation & 2 Year punishment with & without fine) of IPC. Under these Act the boy could have been given a punishment of 3 Years of imprisonment/fine of 1 Lac or both.
*all characters are fictional

Avnish Bajaj vs State (DPS MMS SCANDAL CASE)

Key Words

Internet Service Providers (ISPs), Cyber Space, Criminal Liability, Director's Liability, Listing

FACTS

The case involved an IIT Kharagpur student Ravi Raj, who placed on the baazee.com a listing offering an obscene MMS video clip for sale with the username alice-elec. Despite the fact that baazee.com have a filter for posting of objectionable content, the listing nevertheless took place with the description, “Item 27877408 – DPS Girls having fun!!! full video + Baazee points.” The item was listed online around 8.30 pm in the evening of November 27th 2004 and was deactivated, around 10 am on 29th November 2004. The Crime Branch of Delhi police took cognizance of the matter and registered an FIR. Upon investigation, a charge sheet was filed showing Ravi Raj, Avnish Bajaj, the owner of the website and Sharat Digumarti, the person responsible for handling the content, as accused. Since, Ravi Raj absconded; the petition was filed by Avnish Bajaj, seeking the quashing of the criminal proceedings.

Petitioner

1. Since the MMS was transferred directly between the seller and buyer without the intervention of the website, they can at most be responsible for the listing placed on the website which by itself was not obscene and did not attract the offence under Section 292/294 IPC or Section 67 of the Information Technology (IT) Act.

2. Due diligence was taken by the website to immediately remove the video clip once it was brought to its knowledge that it was objectionable.

3. The scope of Section 67 of the IT Act is only restricted to publication of obscene material and does not cover transmission of such material.

State

1 Offence under Section 292 of Indian Penal Code (IPC) includes not only overt acts but illegal omissions within the meaning of Sections 32, 35 and 36 IPC.

2 The failure to have adequate filter in a system which is entirely automated entails serious consequences and a website cannot escape such legal consequences.

3 The fact that payment was made to the seller even as on 27th December 2004 shows that no attempt was made to prevent or stop the commission of the illegality by the website.

HELD (Delhi High Court)

The court observed that a prima facie case for the offence under Section 292 (2) (a) and 292 (2) (d) IPC is made out against the website both in respect of the listing and the video clip respectively. The court observed that “[b]y not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene”, and thus it held that as per the strict liability imposed by Section 292, knowledge of the listing can be imputed to the company.

However, as far as Avnish Bajaj is concerned, the court held that since the Indian Penal Code does not recognize the concept of an automatic criminal liability attaching to the director where the company is an accused, the petitioner can be discharged under Sections 292 and 294 of IPC, but not the other accused.

As regards S. 67, read with Section 85 of the IT Act, the Court however, observed that a prima facie case was made out against the petitioner Avnish Bajaj, since the law recognizes the deemed criminal Liability of the directors even where the company is not arraigned as an accused. The judgement however did not declare Avnish Bajaj guilty.

Remark

I respectfully submit that there is no sound reason to absolve the director, Avnish Bajaj, even under the said provision of section 292 and 294 of IPC. The concept of corporate criminal liability must be applied here to impose appropriate penalty on the director. Support for such argument can also be drawn from Article 12 of the European Convention on Cyber Crime which provides for imposition of criminal liability on the legal person having a power of representation, authority to take decisions and exercise control. Clause 2 of Article 12 provides that a legal person can be held liable where the lack of supervision or control by a natural person acting under his authority has made possible the commission of a criminal offence.

Though India has not ratified the convention as yet but the said provision can be taken as a guiding principle to impose liability on the director of the company. If the director is absolved of any liability, it will set a wrong precedent. The approach taken by the court in this case does not contribute to the determination of the extent of liability of Internet service providers and their directors, as the court did not specifically delve into these issues and settle the law on this subject.

8.0 Social Media Monitor: Solution to Social Media Crimes by Our Team

8.1Website Design

Task Analysis:

The tasks and subtasks that the users perform when interacting with the website, such as searching or uploading a file, also have a profound influence on the design decisions. The following characteristics need to be considered:

Task objectives:

What are the goals of users as they perform their tasks?

Basic actions:

What actions do users need to perform to achieve this objective?

Frequency of use:

Are there tasks that are performed very often? Do we need shortcuts for them?

Primary training:

Will users get trained to perform those tasks? Do we need to provide help messages?

Task importance:

How important is each task? What if an error happens? What can we design to prevent errors?

Alternative solutions:

Are there other ways to achieve the same goals?

Relationship between tasks:

Are tasks related to each other? Do we need links?

8.1.1 Four Level Model

A web design model is based on identified needs of users and established requirements of the system. Via a conceptual simulation of users navigating through the website, a designer formulates a model to outline the structure of the website in detail and illuminate how it will be implemented.

a. Conceptual level –

Thorough understanding of goals and intended model, such as the overall structure and functionality of the website.

b. **Semantic level –**

Identify users’ input and what the system will output.

c. **Syntactic level –**

Placement of components on the webpage, arrangement of content.

d. **Lexical level –**

Primitive ingredients such as icons, links, messages, and search boxes.

8.1.2 Principles

In addition to the analysis and fulfilment of the websites’ pre-requirements, applying appropriate design principles and guidelines are also necessary to ensure a user-centred website.

1) Functionality

Identify who the functions are designed to serve and what their special needs are. Operations should be accessible and easy to perform without assumed knowledge, catering to both experienced and inexperienced users.

2) Content

All of the content should be logically organized and expressed in natural phrases and concepts familiar to the users. Instructions should be provided when necessary. A good design should also include correct grammar and spelling.

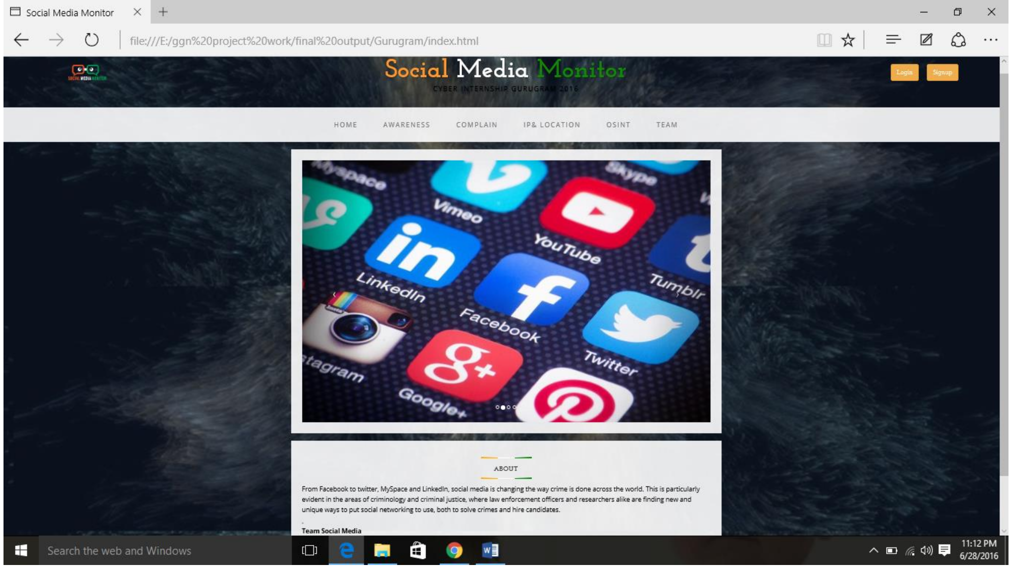
3) Consistency

To design a consistent and predicable website, the designer can use a template. The “look and feel” of every page should be similar, so that a user does not need to wonder whether different situations mean the same.

4) Aesthetics

A disorganized layout can lead to error, and a bad-looking homepage can turn users away. Designers should focus their efforts on fonts, colours and images. The overall design should not be too fancy. White space is necessary for good page layout.

8.1.2 Screen Shots

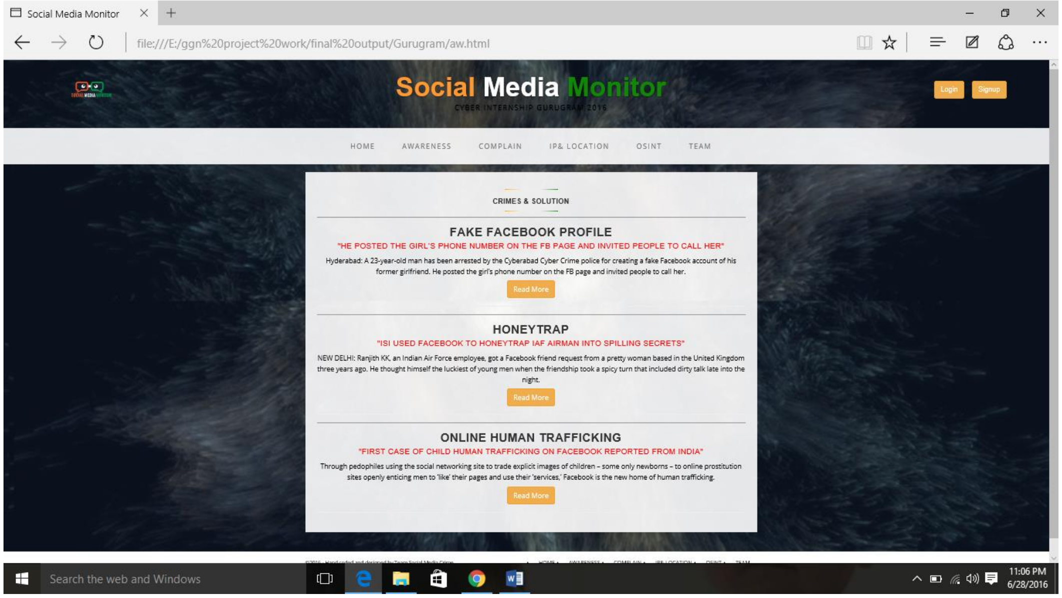


ABOUT

From Facebook to twitter, MySpace and LinkedIn, social media is changing the way crime is done across the world. This is particularly evident in the areas of criminology and criminal justice, where law enforcement officers and researchers alike are finding new and unique ways to put social networking to use, both to solve crimes and hire candidates.

Team Social Media

Fig: Front Page


Social Media Monitor
file:///E:/ggn%20project%20work/final%20output/Gurugram/aw.html
Social Media Monitor
CYBER INTERNSHIP GURUGRAM 2016
Login
Signup
HOME
AWARENESS
COMPLAIN
IP& LOCATION
OSINT
TEAM
Read More
Search the web and Windows
11:06 PM
6/28/2016

CRIMES & SOLUTION

FAKE FACEBOOK PROFILE

"HE POSTED THE GIRL'S PHONE NUMBER ON THE FB PAGE AND INVITED PEOPLE TO CALL HER"

Hyderabad: A 23-year-old man has been arrested by the Cyberabad Cyber Crime police for creating a fake Facebook account of his former girlfriend. He posted the girl's phone number on the FB page and invited people to call her.

HONEYTRAP

"ISI USED FACEBOOK TO HONEYTRAP IAF AIRMAN INTO SPILLING SECRETS"

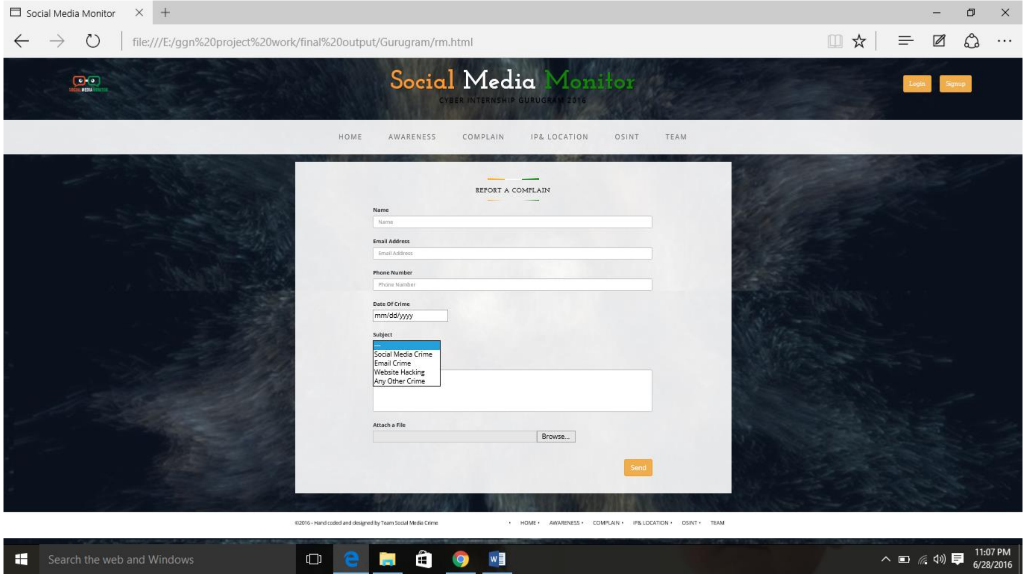
NEW DELHI: Ranjith KK, an Indian Air Force employee, got a Facebook friend request from a pretty woman based in the United Kingdom three years ago. He thought himself the luckiest of young men when the friendship took a spicy turn that included dirty talk late into the night.

ONLINE HUMAN TRAFFICKING

"FIRST CASE OF CHILD HUMAN TRAFFICKING ON FACEBOOK REPORTED FROM INDIA"

Through pedophiles using the social networking site to trade explicit images of children – some only newborns – to online prostitution sites openly enticing men to 'like' their pages and use their 'services,' Facebook is the new home of human trafficking.

Fig: Awareness page



REPORT A COMPLAIN

Name

Name

Email Address

Email Address

Phone Number

Phone Number

Date Of Crime

mm/dd/yyyy

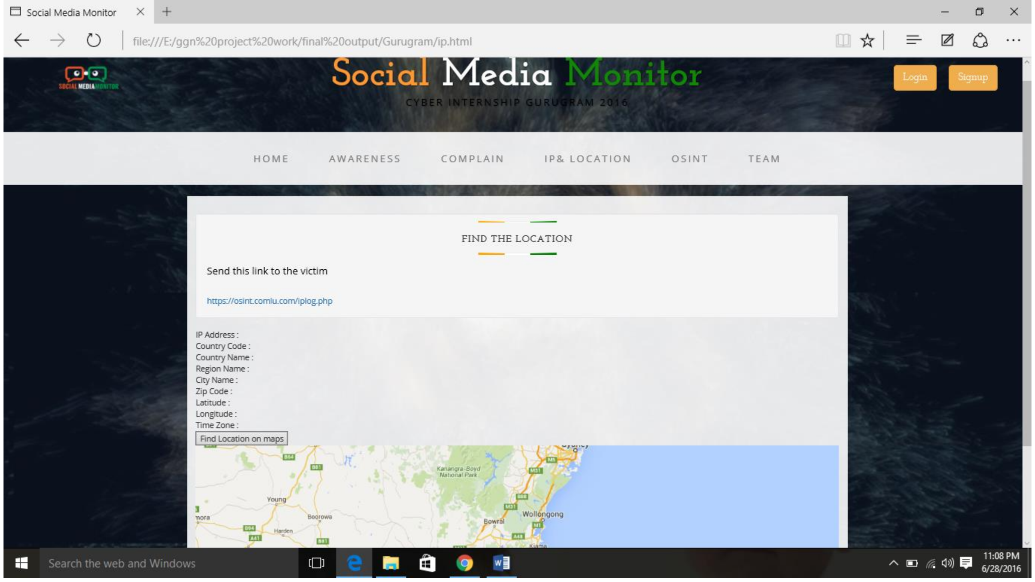
Subject

Social Media Crime
Email Crime
Website Hacking
Any Other Crime

Attach a File

©2016 - Hand coded and designed by Team Social Media Crime • HOME • AWARENESS • COMPLAIN • IP& LOCATION • OSINT • TEAM

Fig: Register Complaints



FIND THE LOCATION

Send this link to the victim

https://osint.comlu.com/iplog.php

IP Address :
Country Code :
Country Name :
Region Name :
City Name :
Zip Code :
Latitude :
Longitude :
Time Zone :

Fig: IP & Location

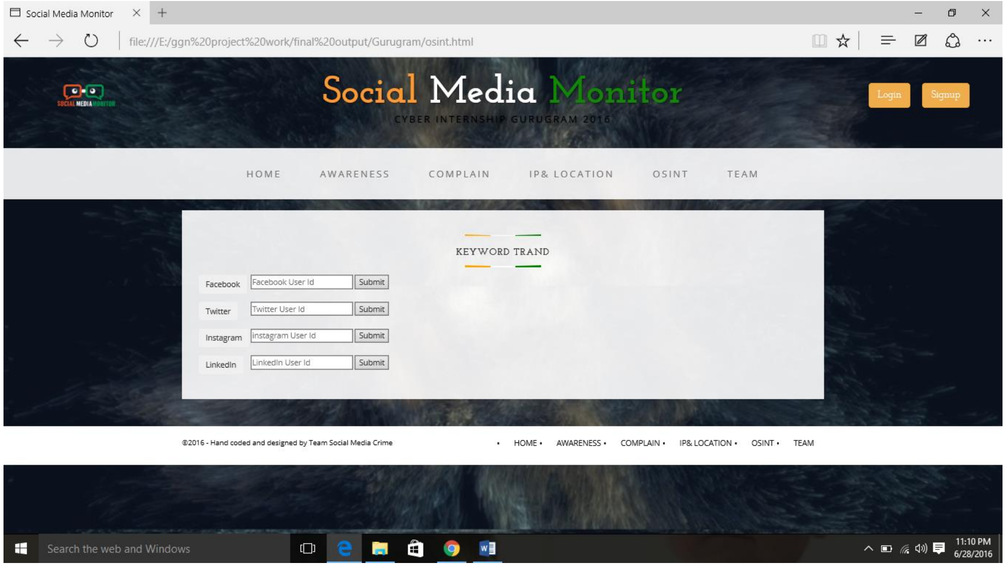


Fig: OSINT

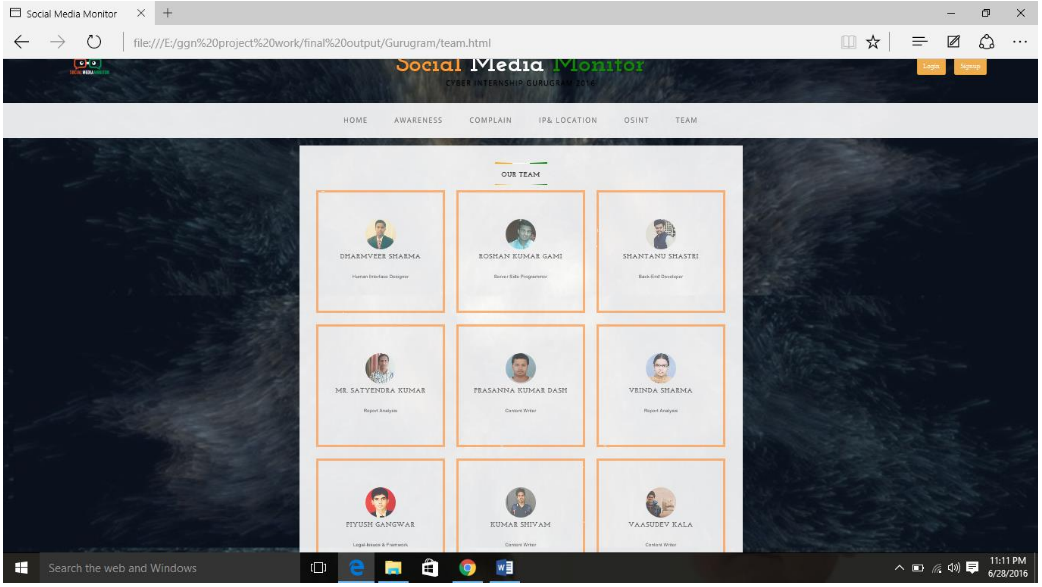


Fig: Our Team

8.2 IP and Location Grabbing

We have used PHP to retrieve and transmit data. PHP is a Hypertext Pre-processor (earlier called, **Personal Home Page**) **PHP** is an HTML-embedded, server-side scripting language designed for web development. It is also used as a general purpose programming language. It was created by Rasmus Lerdorf in 1994 and appeared in the market in 1995.

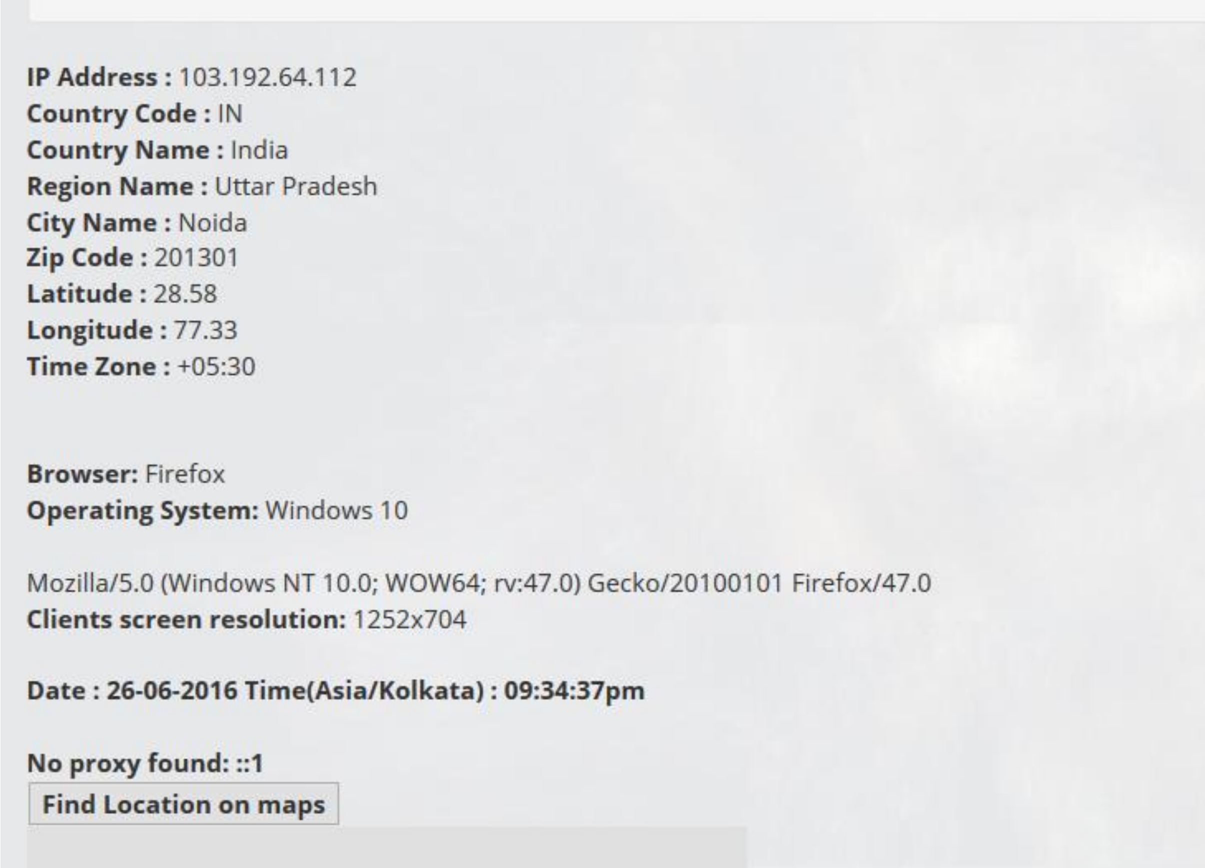
We have embedded API of ipindb.com is to our server side script which fetches us the following data:- IP Address : "103.192.65.2", Country Code : "IN", Country Name : "India", "Region Name" : "Delhi", City Name : "Delhi", Zip Code : "110008", Latitude : "28.6667", longitude : "77.2167", Time Zone : "+05:30".

Application program interface (**API**) is a set of routines, protocols and tools for building software applications. An **API** specifies how software components should interact and **APIs** are **used** when programming graphical user interface (GUI) components.

Interface of API:

An interface is a common boundary shared by two applications or programs that allow both to communicate with one another.

So an API is essentially a way for programmers to communicate with a certain application. So here we have used json API to communicate with the other application.



IP Address : 103.192.64.112
Country Code : IN
Country Name : India
Region Name : Uttar Pradesh
City Name : Noida
Zip Code : 201301
Latitude : 28.58
Longitude : 77.33
Time Zone : +05:30

Browser: Firefox
Operating System: Windows 10

Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Clients screen resolution: 1252x704

Date : 26-06-2016 Time(Asia/Kolkata) : 09:34:37pm

No proxy found: ::1

API Used:- http://api.ipinfodb.com/v3/ip-city/?key=<your_api_key>&ip=74.125.45.100&format=json

Here Key is registered with the name Roshan Kumar Gami at ipinfodb.com and required IP address is of the victim.

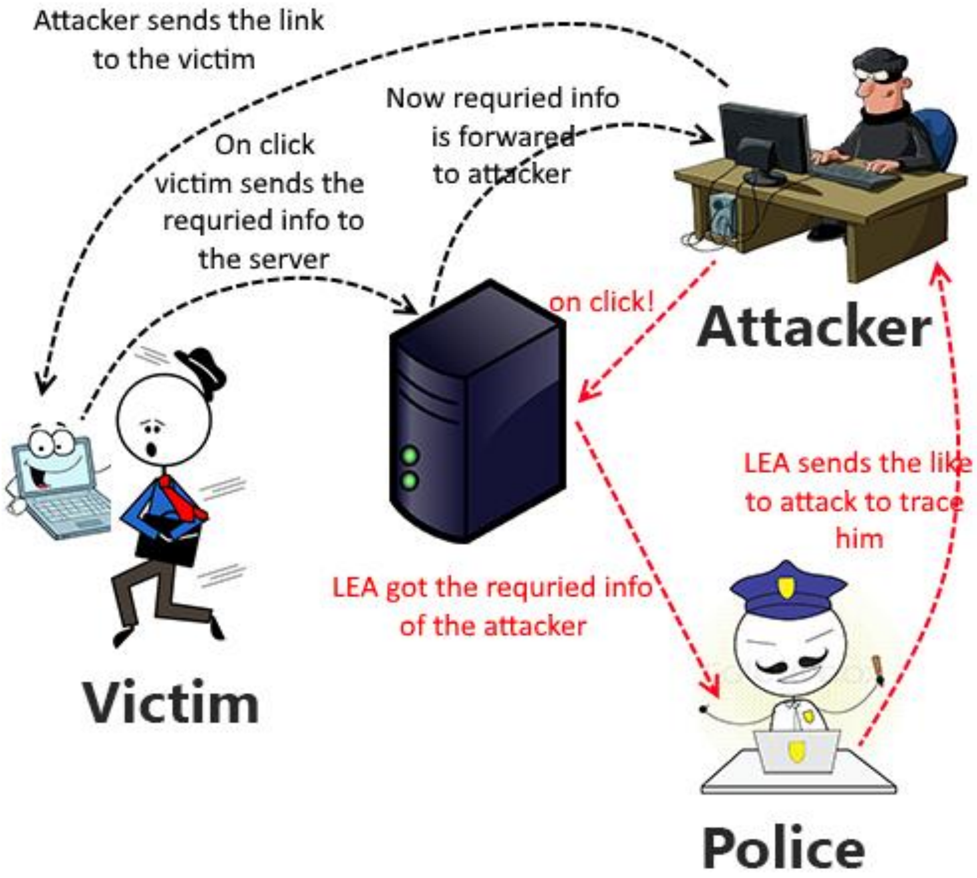
Now this API is further connected to google maps passing latitude and longitude as a variable, which gives the graphical location of attacker/victim.

This API is embedded with our PHP code. So, when victim opens this link, the above mentioned information gets locked in a variable that sends back to the server. Now the investigating team will have every required information about the attacker/victim.

Working of API’s

These days, APIs are especially important because they dictate how developers can create new apps that tap into big Web services—social networks like Facebook or Pinterest, for instance, or utilities like Google Maps or Dropbox. In one sense, then, APIs are great time savers. They also offer user convenience in many cases.

In our case we have used API of ipinfodb.com which fetches us the required information in JSON. Therefore, through json_decode() procedure in php to parse and decoded it to the viewable form.


Attacker sends the link to the victim
Now requried info is forwared to attacker
On click victim sends the requried info to the server
on click!
Attacker
LEA sends the like to attack to trace him
LEA got the requried info of the attacker
Victim
Police

The above mentioned figure demonstrate "how the attack works?", when victim clicks on the link send by attacker, the API captures the required information and send it to the attacker. Now attacker has the every information needed to fulfil his/her aim. Similarly this technique is LEA to track down the attacker.

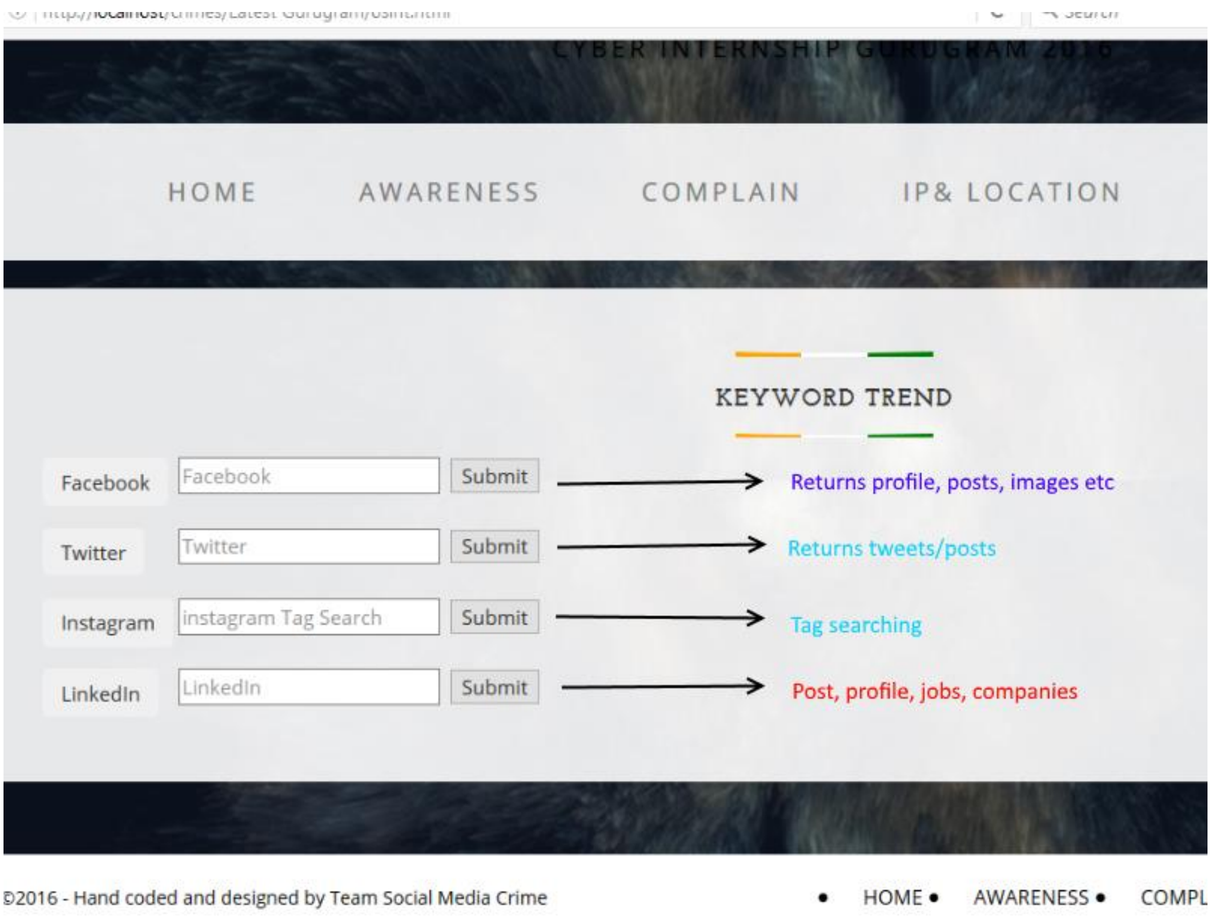
8.3 OSINT (Open Source Intelligence)

OSINT stands for “Open-Source **INT**elligence”, which refers to any unclassified information and includes anything freely available on the web. OSINT is the opposite of close-source intelligence or classified information. Common OSINT sources include social networks, forums, business websites, blogs, videos, and news sources.

Now the above figure shows the mechanism of open source information gathering tool, here the respective search box returns result of your searched elements.

Here we have used different API provided by Facebook, Twitter, and LinkedIn etc.

For Facebook it returns profiles, status, posts on the images etc. Similarly for twitter, Instagram and LinkedIn it results in target tweets, tag lines, profiles etc.



©2016 - Hand coded and designed by Team Social Media Crime

8.4 Report A Complaint

This section of website gathers all the complaint on various crimes that are carried out and reports it to the cybercrime cell so that a course of action is carried out as early as possible. This section of website has the following:

- Name
- Email Address
- Contact no.
- Date of crime
- Subject
- Message
- Attach a file

Finally this will help the investing officer in charge of the cybercrime cell to reach the victim as early as possible by determining the location and the reach the place so that culprit can easily be determined and will be punished as soon as possible.

8.5 Team Contribution

- Roshan Kumar Gami pursuing B.Tech 3rd year from Maharaja Agrasen College, University of Delhi. He programmed server side end in PHP & MY SQL & implemented IP Grabbing, location Grabbing & OSINT web application.
- Shantanu Shastri pursuing B.Tech 3rd year (2013-17) from ITM University, Gwalior. He handles backend development & give his contribution in content writing in OSINT.
- Dharmveer Sharma pursuing B.Tech 2nd year (2014-18) from Shri Mata Vaishno Devi University, J& K. He works on Human Interface Design & Front Hand Development.
- Prasanna Dash pursuing B.Tech 4th year from SRM University, Chennai. He has given his contribution as report editing.
- Vrinda Sharma pursuing M.Tech 1st year from DCSA, KUK, Kurukshetra. She worked on content collection, writing & report analysis.
- Vaasudev Kala pursuing Vivekananda Instt. Of Professional studies, Delhi. He works on content collection & supported in report writing.
- Piyush Gangwar pursing MS in Cyber Law & Info. Tech. 4th trimester NLIU, Bhopal. He handles Legal aspects & Case Studies.
- Kumar Shivam pursuing B.Tech from University of Petroleum & Energy Studies. He worked on content collection & content writing.
- Satyendra Kumar worked as Project Analyser & guidance.

9.0 FUTURE SCOPE

Our team as a whole contributed in development of website which works on IP Grabbing, Location Grabbing, OSINT, spread awareness among society, a person can file report also & have many more features. In OSINT application, we can connected to other social networking sites like Facebook, twitter, LinkedIn & so on. From these social site we can get current updated data & analyse that information accordingly. But now in our application, we can only see the data Live but in future, our team is concentrating on connecting it to Hadoop & APACHE SPARK (machine learning) for data storage purpose. Hadoop is a software platform that lets one easily write and run applications that process vast amounts of data i.e. Big Data & Apache Spark provide support to Hadoop for fast access & executes query in parallel.

10.0 CONCLUSION

Social media sites overwhelmingly provide a positive means of social interaction and communication. Many government entities, including law enforcement agencies are using social media sites in order to interact with and provide information to the public. On the other hand, participants are also using social media sites for criminal purposes. They may be used to organize and coordinate a civil disorder, plan a robbery, or recruit new members for terrorist groups. Law enforcement personnel must be trained in the concept and function of social media sites and how they can be used by law enforcement to prevent, mitigate, respond to, and investigate criminal activity. In conducting law enforcement activities in social media sites, agencies must ensure that information obtained from these sites for investigative and criminal intelligence-related activity is used lawfully. Law enforcement agencies must develop and disseminate a social media policy that states how information from social media sites can be used by law enforcement, as well as the differing levels of engagement with subjects when social media sites are accessed. A policy statement should also specify the authorization requirements, if any, associated with each level of engagement. Other issues that should be addressed in the policy include the documentation, storage, and retention for information obtained; a statement of the reasons, if any, for off-duty personnel to use social media information related to their law enforcement responsibilities; and the identification of dissemination procedures for criminal intelligence and investigative products obtained from social media sites.

The webpage created by us will help the police/security agencies in monitoring the opinions of various peoples being floated on social media. The opinion and comments offered by people make a huge impact on other people accessing this information in positive or negative way. Therefore, in today's time social media has become a powerful tool to influence the mass on a larger scale. Since police needs to monitor these social media opinions in order to maintain peace, law and order. But on the other hand they have lack of time and insufficient number personnel to monitor these activities on such a huge IT platform. Hence this web page will help them to monitor the concerned subject in least possible time with limited man power to plan legal course of action against any criminal, anti-social and anti-national elements.

REFRENCES

Websites-

-http://www.business-standard.com/article/opinion/social-media-misuse-and-indian-cyber-law-115100700139_1.html

-http://www.iacpsocialmedia.org/Portals/1/documents/External/ NW3CArticle.pdf

-https://indiancaselaws.wordpress.com/2013/10/20/avnish-bajaj-vs-state-dps-mms-scandal-case/

-http://www.business-standard.com/article/opinion/social-media-misuse-and-indian-cyber-law-115100700139_1.html

-http://www.business-standard.com/article/technology/india-ranked-2nd-in-cyber-attacks-through-social-media-in-2014-115042200643_1.html

-http://securityaffairs.co/wordpress/4891/cyber-crime/7-most-common-facebook-crimes.html

-http://www.iacpsocialmedia.org/Portals/1/documents/External/ NW3CArticle.pdf

-http://criminal.lawyers.com/criminal-law-basics/social-networking-web-sites-and-crimes.html

-http://blogs.lse.ac.uk/usappblog/2016/01/28/how-social-media-is-changing-the-way-people-commit-crimes-and-police-fight-them/