The purpose and the scheme behind the comparative analysis of major developed legal system is to learn from the experiences and experiments of similarly placed legal systems. At this juncture, the comparison may be insightful because by this alone, we can measure/calculate our legal system and also get a feel of the strength and weaknesses of our own system. The history of social media in the last decade has heavily relied on the contemporary development in Information and Communication Technologies. These technologies have received high focus in those countries where the research and development institutions are highly robust and developed. In this regard U.K. and U.S. are leading countries which have been instrumental in spreading the use of communication technologies by way of internet and telephony etc. Naturally these countries have been feeling the flux of legal challenge arising out of interactions between law, science and technology. It is because of these reasons that corresponding development of laws and regulations facilitating the information dissemination and communication in these countries has been trend setting and therefore our legal system can heavily draw from the problems, issues and challenges of the social media revolution.

The comparison takes into its fold differential parameters like areas in which major issues and challenges are noticed/frequently occurring, areas in which we have some effective legislative mechanism to handle present issues, areas where we require new policies and new regulatory structure.

An attempt has been made in this chapter to look into the differential aspects in these two legal systems, which have provided the stuff for other corresponding developing legal systems as well, so that we can effectively provide legal regulatory mechanism suited to our own native conditions. This chapter will study the social media regulatory framework in these countries. India's legal system is based on the Anglo-American common law model, which means that among the most important emerging markets, India is the one that bears the closest resemblance to the American Legal system. The Indian Constitution
which came about in 1950 was drafted on the basis of English Common law and incorporating important US court decisions. Having regard to its borrowing of constitutional provisions from United States and United Kingdom, this chapter discusses social media regulation in United States and United Kingdom. The chapter attempts to look at the laws, policies, cases and regulatory framework governing social media in both the legal systems to suggest the possible implications for India.

4.1 SOCIAL MEDIA REGULATION IN UNITED STATES

All electronic communications in the US is regulated by the Federal Communications Commission. The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable in US. As an independent US Government agency monitored by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation. In its work facing economic opportunities and challenges associated with rapidly evolving advances in global communications, the agency capitalizes on its competencies in:

- Promoting competition, innovation and investment in broadband services and facilities
- Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution
- Encouraging the highest and best use of spectrum domestically and internationally
- Revising media regulations so that new technologies flourish alongside diversity and localism
- Providing leadership in strengthening the defence of the nation's communications infrastructure

While the strong protections of the US Constitution and the Bill of Rights have resulted in very little government mandated filtering or censorship, the internet became highly regulated as it expanded and developed in the United States. There continues to be debate
over content regulation on the internet concerning a wide range of topics. Many of the issues concern the First and Fourth Amendment of the US Constitution.

The first amendment of the US Constitution prevents the power of congress in certain areas. It says:

“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.”

It does not mean, however, that the US has no regulations for the Internet. Social Media proliferation like other countries has been a matter of concern in United States as well. Its regulation has been widely debated across the country and various laws have been made. In the wake of the London Riots in United Kingdom, problems arose in San Francisco, California, when transit police shot and killed a knife wielding homeless man on a train platform.215 Public anger over the shooting has sparked tensions. Bay Area Rapid Transit ("BART"), the operator of San Francisco's subway, suspended service on its own mobile network for three hours, not allowing passengers to make even emergency calls. It was argued by the critics that government can only enforce reasonable restrictions on demonstrations when there is a present and clear danger. Transit officials maintained that actions were necessary to protect public safety and that the transit passenger’s right to safety outweighed the right to freedom of speech and assembly. An emergency petition was filed asking the FCC to declare BART’s actions a violation of telecom laws, specially the Communications Act of 1934. The FCC responded with a statement commending BART for taking steps to adopt a new policy and stating that the FCC would soon announce an “open, public process to provide guidance on these issues.”216


Many governments mandated attempts to regulate content have been banned on First Amendment grounds. Regulation of the Internet also has raised Fourth Amendment concerns. Fourth Amendment States:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

As technological advancements have created new legal concerns, the Fourth Amendment has become a source of challenges to existing legislation. The Electronic Communications Privacy Act (ECPA) has been challenged being violative of the Fourth Amendment.

The United State Department of Justice (DOJ) which is also known as Justice Department is a federal executive department of the US Govt. The department is responsible for enforcement of law and administration of justice. The department is headed by Attorney General. The Computer Crime and Intellectual Property Section (CCIPS) of United States Department of Justice is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. Section attorneys work to improve the domestic and international infrastructure-legal, technological, and operational-to pursue network criminals most effectively. Apart from it, every state police in the United States has expert personnel to investigate cyber crimes which cover offences committed on social media as well. For example the Cyber Crime Unit (CCU) of New Jersey State Police is composed of State Police enlisted detectives, civilian analysts, and task forces from other police agencies.

217 See; Reno Vs. ACLU; 521 U.S. 844 (1997)

218 U.S. Constitution Amendment IV

219 Alexandra Paslawsky, ‘The growth of social media norms and governments attempts at regulation’ (2011-12) 35 Fordham Int'l L.J. 1485
CCU Investigation squad is to conduct and assist in investigations where computers, networks, telecommunication devices, and other technological instruments are the vehicle or target for the commission of criminal acts against network resources critical to the function of corporate or government entities. These vehicle or target intrusions lead the unit to specialize in the investigations of Computer Intrusions, Data Theft, Cyber Terrorism, Social Networking/Email Account Intrusions & Online ID Theft etc.

In U.S. employer social media policies continue to raise complex legal issues. Public employers are subject to the First Amendment's prohibition against abridging the freedom of speech. However, not everything a public employee says is protected by the First Amendment. The Maine Supreme Court has stated that a public employee's speech is not protected if it is uttered as part of his or her official job duties. The rationale behind the judgment is that when a public employee's job requires a person to speak, the speech is not made in the person's capacity as a "citizen." Rather, the person is working, and just like a private employer, the public employer has a right to control what is said on behalf of the employer. However, a public employee's speech is protected if made in the person's capacity as a citizen and the speech involves a matter of public concern. In short, a public employee's speech is only protected if it is not uttered in the course of official work duties and it involves a matter of public concern.

The legislative efforts to combat computerized forms of pornography and internet based transmission of material judged harmful to minors for commercial purposes constitute more clearly contents based regulations. The efforts of the Congress have run into choppy constitutional waters.

4.1.1 Laws Governing Social Media

In US, laws concerning computer crimes have been enacted at the state and federal levels. In 1986, Congress passed the Computer Fraud and Abuse Act (CFAA). This law has been

---

220 Quintal v. City of Hallowell, 2008 ME 155


222 Thomas Gibbons, ‘Free Speech in the New Media’ (1st edn., Ashgate 2009) 448
amended and expanded as internet technology has advanced, and it continues to form the basis for federal prosecutions of computer-related criminal activities. Other relevant federal statutes include the Electronic Communications Privacy Act (ECPA), the Identity Theft Enforcement and Restitution Act of 2008 (ITERA), Digital Millenium Copyright Act and Communications Decency Act etc. These laws are discussed as follows:

A. First Amendment and Social Media

Freedom of speech in the United States is protected by the First Amendment to the United States Constitution and by many state constitutions and state and federal laws. Freedom of speech as guaranteed by first amendment and rise of social media in particular shares a unique nexus. However, every form of speech is not protected by the first amendment and social media is used to publish any form of speech. This has been felt necessary by the courts that a speech which is punishable offline shall also be punishable online. The courts have extended the first amendment and its exception into the domain of social media. The Court has also recognized several categories of speech that are excluded from the freedom for example libel, incitement, obscenity and fighting words.

In Reno v. ACLU\textsuperscript{223}, for example, is the most important case on the point. In 1997, a group of organizations, including the American Civil Liberties Union (ACLU), challenged the “indecent transmission” and “patently offensive display” provisions of the 1996 Communications Decency Act. These provisions made it a crime to send offensive Internet material to persons under age eighteen. The Supreme Court found Internet communication similar to newspaper publishing, which historically enjoyed broad First Amendment protection. This case was the Supreme Court's first case involving cyberspace. An attempt has been made by Justice Stevens to place the Internet in the same structure the Court has devised to decide other media-related First Amendment cases. The Court gave Internet communications the highest level of First Amendment protection.

\textsuperscript{223} 521 U.S. 844 (1997)
protection, which traditionally has been available only to print media like newspapers and magazines.

Internet freedoms have been generally extended to social media sites, yet schools and employers have been given a free hand to filter content and limit individual use. The schools and employers have been given this freedom because of the potential threat to educational and work distraction because of Facebook; Twitter etc. There is variety of reasons for allowing them freedom which is discussed later in this chapter.

B. Computer Fraud and Abuse Act (CFAA)

CFAA\textsuperscript{224}, is an amendment made in 1986 to the Counterfeit Access Device and Abuse Act that was passed in 1984. The Act says that, “whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication shall be punished under the Act.” In 1996 the CFAA was, again, broadened by an amendment that replaced the term “federal interest computer” with the term “protected computer.” While the CFAA is primarily a criminal law intended to reduce the instances of malicious interferences with computer systems and to address federal computer offenses, an amendment in 1994 allows civil actions to brought under the statute, as well.

The CFAA has been invoked for creation of fake user accounts on social network sites, email spam, email phishing, robotic data mining, and unauthorized hard-drive wiping. However courts in various decisions have ruled that creation of fake accounts over social media pages are not bad enough to be computer fraud therefore CFAA cannot be applied in these cases. In \textit{United States v. Lori Drew}\textsuperscript{225} the court refused to invoke CFAA criminal penalties against a mother who created a fake MySpace profile for the purpose of bullying a teenage friend of her daughter. The court while noting the wide existence of

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{224}] Computer Fraud And Abuse Act, 18 U.S.C. § 1030
\item[\textsuperscript{225}] (2009) 259 F.R.D. 449
\end{itemize}
\end{footnotesize}
fake social media accounts agreed that a broad interpretation of the CFAA could turn “millions of unsuspecting individuals” into perpetrators of computer crime.

In the case of *Matot v. C.H.*\(^{226}\) the U.S. District Court of Oregon dismissed a suit brought by a middle school assistant principal claiming that, by creating fake social media accounts using his name and likeness, some students had violated the Computer Fraud and Abuse Act (CFAA). The CFAA claims were based on alleged use “without authorization” of social media services (e.g., Facebook and Twitter) in that the defendants violated terms of use of the social media services by creating fake accounts using the plaintiff’s name and likeness. The court dismissed the CFAA claims. In doing so, it relied upon previous decisions rendered by the Ninth Circuit regarding the scope of the CFAA in *U.S. v. Nosal* case.

*U.S. v. Nosal*\(^{227}\)

In this case, an executive firm brought a case against its ex-employee on the charges that he induced present company employees to use their legitimate credentials to access the company's proprietary database and provide him with information in violation of corporate computer-use policy. It was claimed that the violation of firm’s private policy was a violation of the Computer Fraud and Abuse Act (CFAA). Following a decision issued in 2009 by the Ninth Circuit, the district court ruled that violations of corporate policy are not equivalent to violations of federal computer crime law.

**C. United States Copyright Law**

The U.S. Constitution provides the federal government the authority to protect an author's original work.\(^{228}\) It states that the

> “Congress shall have Power… To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.”


\(^{227}\) 676 F.3d 854 (9th Cir. 2012)

\(^{228}\) Article 1, Section 8, Clause 8 of the U.S. Constitution
Federal law defines what type of content may be protected under U.S. copyright law. According to 17 U.S.C. Section 102(a), "copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." Federal law enables content creators to monetize their original work and protects copyright holders against the unauthorized commercialization of their material.

To address the issues of rapidly changing technology, The Digital Millennium Copyright Act (DMCA) was enacted. Title II of the DMCA adds a new section to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

- Transitory communications;
- System caching;
- Storage of information on systems or networks at direction of users; and
- Information location tools.

New section 512 also includes special rules concerning the application of these limitations to non-profit educational institutions.

Under the DMCA, social media websites like YouTube or Facebook that allow users to post content can obtain protection from liability if they meet certain technical requirements. The requirement also includes promptly removal of user-generated content after receiving the notice. The safe harbor provisions in § 512(c) of the Digital Millennium Copyright Act (DMCA) provide a mechanism that insulates online service providers from liability.

---

229 See 17 U.S.C.A. § 512 (a) - (d) (West 2010).

230 Under Section 512(c)’s safe harbor provision, a service provider will not be liable so long as it:

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent;

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
providers from monetary damages for infringing materials posted or stored by their users. However, in order to receive this protection, service providers must designate an agent to receive notice of claims of infringement with the Copyright Office and publicly post the agent’s contact information on the website.

The validity of this provision was considered in the case of *Viacom vs. YouTube*. In March 2007, YouTube and Google were sued by Viacom on the ground of copyright infringements committed by YouTube users. Huge amount of money was demanded as compensation in this case by Viacom. The plaintiff has made more than 100,000 takedown notices targeting videos allegedly owned by it. The YouTube website had a designated agent to receive notices by copyright owners as required by the DMCA, and upon receipt of plaintiffs’ notice, YouTube responded immediately and removed the allegedly infringing materials from its website.

Facts of the case establish that the DMCA actually worked to prevent continued infringement of copyrighted work but potential harm was already done to the plaintiff till he find the infringement and company stopped its unauthorized use. In YouTube, copyrighted videos are easy to upload by anyone and accessible by everyone until it is identified by the copyright owner and removal notice is received by YouTube. However, removal notice by genuine user is not enough because only specific copy of the infringing work identified by the copyright owner will be removed, despite the fact that additional copies may exist on the site at the time of notification or may be uploaded thereafter.

In the case of Northern District of California, *Oppenheimer v. Allvoices, Inc.* an interesting issue came before the court. The court was asked to examine whether service providers can avail the § 512(c) safe harbor for infringing acts that precede designation of

(iv) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity;
(v) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity; and
(vi) has designated an agent to receive notifications of claimed infringement.

231 718 F. Supp. 2d 514 (S.D.N.Y. 2010)

such an agent. It was held by the court that an online service provider may invoke the § 512(c) safe harbor only if it has registered a DMCA agent with the Copyright Office. According to the court, designation of an agent is a “predicate, express condition” for application of the safe harbors, so Allvoices could not avail itself of the safe harbors with respect to infringement that occurred prior to designation.

In the case of *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*\(^{233}\), the moot question before the U.S. district court was whether the operator of a computer bulletin board service ("BBS") and Internet access provider (Netcom-the defendant) that allows that BBS to reach the Internet should be liable for copyright infringement committed by a subscriber of the BBS. It was argued by the plaintiff that defendant Netcom was directly, contributory, and vicariously liable for copyright infringement. The defendant moved for summary judgment and urged the court to make a judgment without a full trial, disputing plaintiff’s claims and raising a First Amendment argument and a fair use defense. The district court of the Northern District of California held that plaintiff’s claims of direct and vicarious infringement failed, but genuine issues of fact precluded summary judgment on contributory liability and fair use.

In the case of *CoStar Group, Inc. v. LoopNet, Inc.*\(^{234}\), also the main question before the court was whether LoopNet should be held directly liable for CoStar’s copyrighted photographs posted by LoopNet’s subscribers on LoopNet’s website. The majority of the court ruled that since LoopNet was an ISP that automatically and passively stored material at the direction of users, it did not copy the material in violation of the Copyright Act. The majority of the court also held that the screening process by a LoopNet employee before the images were stored and displayed did not alter the passivity of LoopNet.

\(^{233}\) 907 F. Supp. 1361 (N.D. Cal. 1995)

\(^{234}\) 373 F.3d 544 (4th Cir. 2004)
D. Communications Decency Act

Section 230 of the Communications Decency Act of 1996\(^{235}\) (it is a common name for Title V of the Telecommunications Act of 1996) is a landmark piece of Internet legislation in the United States. Originally, it attempted to regulate the internet in two ways. First, it attempted to regulate both indecency and obscenity in cyberspace. Secondly, it was interpreted to the mean that ISPs should not to be construed as publishers & thereby not liable for the contents of third parties who use their services. In 1997, in the landmark cyber law case of *Reno v. ACLU*\(^{236}\), the United States Supreme Court has struck down the anti-indecency provisions of the Act.

Section 230 of the Communications Decency Act (“CDA”) provides broad immunity to any “interactive computer service” for third party content that is posted onto its service, as long as the service did not provide substantive or editorial contributions. “Interactive computer service” is defined broadly in the statute to include websites, message boards, instant messenger services, blog hosting services, and other internet based services including Facebook, MySpace, YouTube, Google, Yahoo, Flickr, Twitter. Given CDA 230, victims of online harassment or hateful speech most often cannot hold the ISP liable, whether the ISP is a blog hosting service, a web forum, a social media site like Facebook or Twitter, or an email provider such as Hotmail or Gmail. Service providers do not have a legal responsibility to moderate or take down content that is harassing or offensive, even if such content violates the site’s terms of service. For example, Facebook encountered protests from feminist groups who objected to a number of user-created Facebook pages in which rape and domestic violence were treated humorously.\(^{237}\)

Section 230 is very ambiguous and debatable because several courts have interpreted it as providing complete immunity for ISPs with regard to the torts committed by their users

\(^{235}\) 47 U.S.C. §230

\(^{236}\) *Reno v. ACLU* (1997) 521 U.S. 844

\(^{237}\) Meredith Bennett-Smith, ‘Facebook Vows To Crack Down On Rape Joke Pages After Successful Protest, Boycott’ (Huffington Post, 21 Aug 2013) <http://www.huffingtonpost.com/2013/05/29/facebook-rapejokes-protest_n_3349319.html>
over their systems. Various cases have held that social media companies cannot be held liable for content added by its members. The exemption provided by section 230 has been criticized for being silent over the inflammatory contents. In Klayman v. Zuckerberg, the plaintiff sued Facebook over a "Third Palestinian Intifada" page that had more than 360,000 members and called upon "the Muslims to rise up and kill the Jewish people." But the court has provided the exemption benefit of CDA to Facebook.

E. The Electronic Communications Privacy Act (“ECPA”)

The Electronic Communications Privacy Act (“ECPA”), enacted in 1986, is comprised of two statutes:

a. Stored Communications Act &
b. Federal Wiretap Act

a. Stored Communications Act\textsuperscript{240}, 1986

Historically, most litigation arising under the ECPA has involved the Wiretap Act, that is, where there are “interceptions” of wire, audio or aural communications. However, with the social media revolution, the Stored Communications Act (“SCA”) has come into picture. Generally speaking, in the employment context, the SCA makes it unlawful for an employer to have unauthorized access to an employee’s private social media accounts.

More than a dozen states prohibit employers from asking applicants or employees for their passwords to their private social media sites. However, the SCA, which applies to employers in all fifty states and which comes with civil and criminal penalties, may go even further.

The SCA provides that whoever “intentionally accesses without authorization a facility through which an electronic communication service is provided . . . shall be liable for

\textsuperscript{238} Zeran v. AOL, 129 (1997) F.3d 327, 330; Immunity was upheld against claims that AOL unreasonably delayed in removing defamatory messages posted by third party, failed to post retractions, and failed to screen for similar postings.


\textsuperscript{240} Stored Communications Act; 1986, 18 U.S.C. § 2701
“damages” under the SCA. However this provision does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user;241

The SCA also prohibits unauthorized access of stored wire and electronic communications and records that are intended to be private. Specifically, it prohibits anyone (including employers) from accessing electronic communications in electronic storage without authorization. The SCA provides for monetary damages, injunctions and attorney’s fees for violations of its provisions. The question arises is whether the messages stored in private Facebook wall of a user is covered by SCA?

_Ehling vs Monmouth Ocean Hospital Service_242, is an important case on this point. In this case the court ruled that the SCA covers “private” Facebook wall posts. The plaintiff, a registered nurse and paramedic, sued her former employer in federal court asserting a number of claims including violations of the SCA. The court found that the employer had not violated the SCA by viewing the employee’s wall, however, because a co-worker, who was one of her Facebook friends, showed the post to their employer without any prior prompting by the employer. Although the wall posts were covered by the SCA, the Court held that the hospital did not violate the SCA because the “authorized user” exception under the SCA applied to the posts.

b. Federal Wiretap Act

The "Wiretap Act" is a federal law that is aimed at protecting communication privacy with other persons. The Act makes it illegal to

- Intentionally or purposefully.

241 ibid

- Intercept, disclose or use the contents of
  Any wire, oral or electronic communication through the use of a device.

The Act provides criminal and civil penalties for its violations, and provides for various exceptions, when interceptions and disclosures are not illegal. The act has great implications for social media privacy issues in USA.

In the case of Crispin vs. Christian Audigier, Inc\textsuperscript{243} defendants subpoenaed the social networking sites for wall postings and private messages from plaintiff accounts. Plaintiff filed a motion to quash the subpoenas, asserting that the Stored Communications Act prohibited the disclosure. After a lengthy hearing, the court held that Facebook and MySpace were both either an Electronic Communication Service (ECS) or Remote Computing Service (RCS) and thus potentially covered by the SCA. The court then referred to Wiretap Act\textsuperscript{244} and quashed the subpoena insofar as it sought messages that plaintiff sent through the websites’ private messaging services. The court found that those communications are “inherently private” such that the stored messages are not “readily accessible to the general public.”

**F. Children Online Privacy Protection Act (COPPA)**

When Supreme Court has struck down part of the CDA as discussed above, Congress has made two attempts to regulate children's exposure to Internet indecency. However, the enforcement of Child Online Protection Act (COPA) which was the first attempt was blocked by a court injunction almost immediately after its passage in 1998. Legal challenges were also made against COPA’s successor, the Children's Internet Protection Act (CIPA) of 2000 but the Supreme Court upheld it as constitutional in 2004. COPPA, which was enacted in 1998, works to control the collection of personal information from children. Children's Online Privacy Protection Act of 1998 is enacted at 15 U.S.C. § 6501 through § 6506. It prohibits-

\textsuperscript{243}717 F.Supp.2d 965 (C.D. Cal. 2010)
\textsuperscript{244}Wiretap Act 1968, (18 U.S. Code§ 2511)
“an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section.”

Federal Trade Commission administers the COPPA regulations. The regulations are directed at operators of websites directed to children, or any website operator that has actual knowledge that it is collecting or maintaining personal information from a child without consent. The FTC has taken law enforcement actions against companies that failed to comply with the provisions of the law and has issued a report to Congress assessing how companies have complied with it. The Federal Trade Commission’s revised Children’s Online Privacy Protection Act Rule provides parents greater control over the online collection of their children’s personal information.245

G. National Labour Relations Act

A large of companies is now using social media to promote their products and to enhance their customer list. As more companies recognize the brand value created and sustained through social media, there is greater interest in preserving social media accounts for company use. Simultaneously, an increasing number of employees believe that the social media accounts are not company property but their personal property. However, the companies hold contrary view. This situation has led to social media account ownership issues.

The case of PhoneDog LLC v. Noah Kravitz246 illustrate the importance of a social media use policy and the need for a clear distinction at the company level as to who owns the

245 The revised COPPA rule addresses changes in the way children use and access the Internet, including the increased use of mobile devices and social networking. See; FTC, ‘Revised Children’s Online Privacy Protection Rule Goes Into Effect Today’ (FTC, 01 July 2013) <http://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect> accessed 14 December 2014

social media used by the company. In this case a former employee argued that the Twitter account he used to promote his former employer belonged to him personally, and not to the former company.\textsuperscript{247}

The National Labor Relations Act protects the rights of employees to act together to address conditions at work, with or without a union. This protection extends to certain work-related conversations conducted on social media, such as Facebook and Twitter. The National Labour Relations Board (NLRB), which enforces the National Labour Relations Act (NLRA), became the first federal agency to decide how employees' social media use fits in existing labour and employment laws.

The NLRB's Office of the General Counsel (OGC) has issued several memoranda discussing the validity of employer social media policies in light of existing principles under the National Labour Relations Act. The NLRB made national headlines in late 2010 when OGC instructed an NLRB regional office to prosecute an unfair labour practice complaint against an employer that disciplined an employee for posting comments critical of her supervisor on Facebook allegedly in violation of the company's internet and blog posting rule.\textsuperscript{248} In another advice memorandum OGC provided enforcement guidance on social media policies. The OGC has reviewed the social media policies of a company which required its employees to post a specific disclaimer that they were sharing their own views and not the views of their company if they have identified themselves as company employee on any website or social media network.

\textsuperscript{247} Jay Greathouse and Heather Sherrod, ‘Owning your social media: Drafting a social media use policy’(Social Media Law Bulletin, 4 March 2013) <http://www.socialmedialawbulletin.com/2013/03/owning-your-social-media-drafting-a-social-media-use-policy/> accessed on 05 July 2014

The relevant portion of the policy stated:

“If you identify yourself anywhere on a web site, blog, or text as an employee of USA ...... we require that you put the following notice in a reasonably prominent place on your site: ‘The views expressed on this web site/blog are mine alone and do not necessarily reflect the views of my employer, US Security Associates, Inc’.”

The OGC found this provision to be lawful. It explained that posting this disclaimer would not be burdensome for employees to implement or infringe on their Section 7 right of National Labour Relations Act to discuss working conditions. Section 7 of this Act provides that employees have a right to “engage in concerted activity for the purpose of collective bargaining or for other mutual aid and protection”

In an effort to provide additional guidance, the OGC reviewed the remainder of the social media policy. It determined that:

- a provision encouraging employees to express themselves on social media in a “respectful manner” is not unlawful;
- provisions preventing employees from publishing on websites or blogs “confidential information” and “material that violates the privacy of another” are unlawfully overbroad and could be construed to inhibit Section 7 rights;
- a provision preventing employees from disclosing “sensitive information” on websites or blogs is unlawfully overbroad because the meaning of sensitive information was ambiguous; and
- a provision prohibiting employees from referring to their employer’s website without prior written approval from the employer is unlawful. The OGC explained that employees could be hindered in exercising their

---

Section 7 rights if they cannot refer third parties to the website to garner support for their position.

H. Social Networking Online Protection Act

Social Networking Online Protection Act (SNOPA) was originally introduced in May 2012, but it could not see the light of the day and had to be reintroduced since Congress adjourned at the end of 2012. It prohibits employers from:

“(1) requiring or requesting that an employee or applicant for employment provide a user name, password, or any other means for accessing a private email account or personal account on a social networking website; or

(2) discharging, disciplining, discriminating against, denying employment or promotion to, or threatening to take any such action against any employee or applicant who refuses to provide such information, files a complaint or institutes a proceeding under this Act, or testifies in any such proceeding.”

The enactment of SNOPA is of critical importance. The existing framework of the law affords limited protection to one’s security and privacy. The decision of the court in *Maremont v. Susan Fredman Design Grp* provide a glimpse into the court’s apprehension to limit potential employer’s actions and their snooping around the public’s social media pages. In this case, the defendant used the plaintiff’s social networking credentials without permission to access her Facebook and Twitter accounts. The court held that the information on those social networking sites were not private because the plaintiff had over 1,250 followers, and thus, subsequently dismissed the claim. Though the judgement of court in the present case can be criticized on many grounds but since the role of the judiciary is merely to apply the enacted laws, it is the legislature’s

---

250 Social Networking Online protection Act 2012, Preamble of the Act says “To prohibit employers and certain other entities from requiring or requesting that employees and certain other individuals provide a user name, password, or other means for accessing a personal account on any social networking website.”

251 2011 WL 6101949
responsibility to take actions necessary to clearly establish that an individual’s rights will not be compromised simply due to technological advancements.252

I. Fair Credit Reporting Act253

The Fair Credit Reporting Act (FCRA) regulates the dissemination, collection, and use of consumer information, including consumer credit information. The Act is enforced by FTC. The Act was basically designed to ensure that the information provided by third parties to employers or creditors is accurate, and that consumers are informed of any adverse decisions that are made about them, based on such information.

An interesting question arises is whether companies that compile social-media data are subject to the FCRA? The question has been answered by Federal Trade Commission when it leveled charges against Spokeo Inc., a data broker that compiles and sells detailed information profiles on millions of consumer for violating FCRA norms. The FTC imposed $800,000 fine for failure to adhere to the FCRA when collecting social-media data and passing it on to prospective employers. The FTC alleges that Spokeo failed to adhere to three key requirements of the FCRA: to maintain reasonable procedures to verify who its users are and that the consumer report information would be used for a permissible purpose; to ensure accuracy of consumer reports; and to provide a user notice to any person that purchased its consumer reports.254


Social media regulation in United Kingdom is also a matter of great concern. During Tottenham Riots in London, the police and regulatory authorities have found themselves helpless. It was believed that the rioter have arranged their meetings, plans through twitter, Facebook and Blackberry ‘BBM’ service. It was hard on the part of authorities to crack down the coded messages and therefore they have called for the help of Blackberry itself.\textsuperscript{255} The regulatory concern has forced the Prime Minister to take heavy measures for social media regulation.\textsuperscript{256}

A range of UK laws is currently being used to regulate the content of tweets and other online messages. At the moment, there is no particular consistency as to which laws will be used to regulate which messages. It appears to depend on what evidence is available. The House of Lords Select Committee on Communications has said that legislations currently in existence, including the Communications Act 2003, the Malicious Communications Act 1988 and the Protection from Harassment Act 1997, are enough to ensure that criminal offences committed using social media can be adequately prosecuted.\textsuperscript{257} The committee also established that guidance for prosecutions in the case of social media offences accounts appropriately for freedom of expression. However, the law commission of United Kingdom adopts a different view on the sufficiency of laws to contain social media mischief. In its proposed reform on “Social media (criminal law, evidence and procedure)” for reforming the law it said

\begin{quote}
\textit{“While there have been a number of initiatives that have considered aspects of social media in the criminal process, such as the DPP’s guidance on social media prosecutions and the Lord Chief Justice’s}\end{quote}


\textsuperscript{257} Lords Select Committee, Current laws sufficient to cover social media offences (HL, 2013-14, 37-I)
Another report by the Science and Technology Committee (a UK parliamentary select committee) on the ‘Responsible Use of Data’ concludes that online terms and conditions for the use of social media platforms are unnecessarily complex and may not serve their intended purpose of obtaining informed consent from a user for the right to process personal data.\(^ {259} \) The Committee recommends that the UK government should work towards the development of an internationally recognised “kitemark” system to grade the contents of social media platform terms and conditions. According to the Committee, such a system would provide users with an easy and immediate identification of those terms and conditions that have achieved a high kitemark rating, as well as incentivize businesses to review their terms and conditions to obtain a good kitemark rating.\(^ {260} \) While the Report focuses on the UK, the Committee’s observations have relevance globally because the requirement for informed consent to process personal data features in the privacy regimes of many jurisdictions.

In the UK, the Data Protection Act 1998 provides that businesses may process personal data if they have obtained the informed consent of the user.\(^ {261} \) “Consent” is not defined in the Act, so the term is interpreted by reference to the EU Data Protection Directive (95/46/EC) to which the Data Protection Act 1998 gives effect.

The EU Data Protection Directive defines consent as “ . . . any freely given specific and informed indication of [the data subject’s] wishes by which the data subject signifies his agreement to personal data relating to him being processed”.\(^ {262} \) Typically, a social media

---

\(^ {258} \) Law Commission in its 12\(^ {th} \) programme of law reform has sought suggestions on whether social media in a criminal law context is worthy of its attention. See, <http://lawcommission.justice.gov.uk/docs/social-media.pdf> accessed 17 December 2014

\(^ {259} \) Science and Technology Committee, Responsible Use of Data (HL, 2014-15, 245-IV)

\(^ {260} \) Jane Berry, ‘UK MPs consider social media terms & conditions too complex’ (Social Media Law Bulletin, 04 February 2015) <http://www.socialmedialawbulletin.com/> accessed on 10 Feb. 2015

\(^ {261} \) Data Protection Act 1998, Schedule 2

\(^ {262} \) EU Data Protection Directive (95/46/EC), Article 2
platform business will seek to obtain this consent by requiring the user to accept a set of terms and conditions in order to access and use the platform. The Report questions the efficacy of this practice. It notes that making acceptance of the terms of conditions the basis for permission to use a social media platform does not necessarily correlate to having obtained informed consent, as such terms and conditions are rarely read in detail or understood by the user. They are often far too long, contain jargon and use complex language.

The Crown Prosecution Service has given detailed guidelines on prosecuting cases involving communications sent via social media. These guidelines set out the approach that prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media. The guidelines are designed to give clear advice to prosecutors who have been asked either for a charging decision or for early advice to the police, as well as in reviewing those cases which have been charged by the police.  

Content Regulation in UK

In UK freedom of expression is guaranteed through Human Rights Act. The law provides for freedom of press and it also allows people freedom of speech. The law prohibits any undue interference with the privacy, family, correspondence etc. But there has been a gradual decline in this right by the increasing surveillance and police measures in UK. National security concerns have resulted in the state introducing heavy surveillance measures over online communications as well as filtering and tracking practices. The country was listed as the “Enemies of the Internet” in 2014 by ‘Reporters without Borders’. The country was put in the category of highest level of internet censorship and surveillance.

The Internet Service Providers Association (ISPA) was formed in 1995, and established a Code of Practice after a meeting with the Home Office in January 1996. ISPA was given

---

<http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/> accessed on 17 December 2014
a free hand in dealing with the internet contents but increasing crime concerns have forced the govt. and authorities to interfere with their independent functioning. To curb the problem of child pornography, the all the ISPs were asked by the govt. to introduce default filtering mechanism. However, the default filtering mechanism was rejected in September 2013 in the conference of liberal democrats and no govt. legislation to this effect has taken place until now.

4.2.1 Levesson Inquiry Report and Social Media

In the wake of revelations concerning phone hacking conducted by the News of the World tabloid into the phones of celebrities, politicians, and other members of the public, including the missing schoolgirl Milly Dowler and her family, an Inquiry committee headed by Lord Justice Leveson was constituted in the United Kingdom to look into the ethical and legal practice of the press. The report investigated: the press’ relationship with the public, police and politicians and identified a number of key issues and made a series of recommendations; addressed the extent to which the current policy and regulatory framework failed in relation to data protection and various other issues.

The report says that that the relative lack of Internet-specific regulation is unlikely to change and provided a general overview of the Internet, including blogs and social networking sites. Here, the report used a very broad brush to paint a situation that is difficult to control. The relatively few pages dedicated to this sphere shows that the Internet was not foremost in the focus of the report.  

Negligent approach of report towards social media is very curious because at a time when more and more people are going online to obtain news and as a result circulation of

---

newspapers is in steady decline, it seems strange to respond by designing a system which does very little to address new media.

Defending its stance over the putting the social media out of regulation the report says that newspapers should still face more regulation than the internet because parents can 'to some extent' control what their children see online, while they could not control what they see on a newsagent or supermarket shelf.  

4.2.2 Laws Governing Social Media in UK

The laws which are governing social media in UK are as follows:

A. Communications Act 2003

The Communications Act 2003 is an Act of the Parliament of the United Kingdom. The act superseded the Telecommunications Act 1984. Section 127 of the act makes it an offence to send a message that is grossly offensive or of an indecent, obscene or menacing character over a public electronic communications network. In DPP v Collins, proceedings were brought under section 127(1) (a) against the accused for


266 The Communication Act 2003, “ Sec127- Improper use of public electronic communications network
(1) A person is guilty of an offence if he—
(a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
(b) causes any such message or matter to be so sent.
(2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—
(a) sends by means of a public electronic communications network, a message that he knows to be false,
(b) causes such a message to be sent; or
(c) persistently makes use of a public electronic communications network.
(3) A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.”

267 (2006) UKHL 40
offensive and racist phone calls made to the office of his local Member of Parliament. The House of Lords held that whether a message was grossly offensive was to be determined as a question of fact applying the standards of an open and just multiracial society, and taking into account the context of the words and all relevant circumstances. The test was whether a message was couched in terms that were liable to cause gross offense to those to whom it related. The court made clear that an individual is entitled to express his views and to do so strongly; however, the question was whether he had used language that went beyond the pale of what was tolerable in society. The court considered that at least some of the language used by the defendant could only have been chosen because it was highly abusive, insulting and pejorative.

Unlike section 66-A of Information Technology Act in India, Sec. 127 (1) (a) has also been abused by the authorities to prosecute general public. The section was used to prosecute people in cases such as the Twitter Joke Trial (R vs. Paul Chambers) and Facebook comments concerning the murder of April Jones.

In the case of R v Paul Chambers (appealed to the High Court as Chambers v Director of Public Prosecutions) Paul chambers was prosecuted under section 127 because of his frustrating tweet about a delayed flight. He was convicted by the crown court of using Twitter to send a "public electronic message that was grossly offensive or of an indecent, obscene or menacing character contrary to the Communications Act 2003". However the High Court has allowed the appeal against conviction. The lord chief justice, Lord Judge, sitting with Mr. Justice Owen and Mr. Justice Griffith Williams, said:

"We have concluded that, on an objective assessment, the decision of the crown court that this 'tweet' constituted or included a message of a menacing character was not open to it. On this basis, the appeal against conviction must be allowed."

268 (2012) EWHC 2157

The case of offensive messages was further elaborated in the case of Facebook comments concerning murder of April Jones. On 8 October 2012, a 19-year-old male from Chorley in Lancashire pled guilty to sending a grossly offensive message and for posting comments about Jones and Madeleine McCann on his Facebook page, an offence under section 127 (1) (a) of the Communications Act 2003. He was sentenced to 12 weeks' imprisonment in a Young Offender Institution.\(^\text{270}\) In a separate case, an 18-year-old male from Worcester, who posted his opinions about the case on his Facebook page, was given a six-week suspended prison sentence on 7 November, and ordered to do 200 hours of community service.\(^\text{271}\)

**B. Defamation Act, 2013**

The Defamation Act 2013 is an Act of the Parliament of the United Kingdom. Prior to the Act, the law on defamation was made up of common law supported by the 1952 and 1996 Defamation Acts. The 2013 Act is not designed to codify libel law into a single statute; it sits alongside the Defamation Acts of 1952 and 1996.

The Defamation Act, 2013 treats online defamatory material differently. The Act’s effect is largely limited to England and Wales, though certain parts of the Act affect Scotland also. The Act provides welcome reform to an area of law which has become increasingly outdated in light of recent technological and societal changes, particularly as the amount of defamatory material published online has increased with the rise of user-generated content.

The main provisions of the act, which are related to Social Media, are as follows:

“Section 1: Serious harm- This section introduces a requirement that publication causes (or is likely to cause) serious harm, thereby raising the threshold for defamation cases.”


\(^{271}\) Fiveash Kelly, ‘Lancashire man jailed over April Jones Facebook posts’ (The Register, 8 October 2012) <http://www.theregister.co.uk/2012/10/08/man_jailed_for_12_weeks_over_april_jones_facebook_posts/> accessed on 18 December 2014
“Section 5: Operators of websites- Operators of websites that host user-generated content now have more protection by virtue of Sec. 5. It provides new defence for the operators of websites, who did not publish the materials themselves (i.e. it is a defence where user-generated content has been defamatory). The defence will not be available where: (a) the claimant could not hold the website user responsible; (b) the defendant was notified of the publication; and (c) the defendant failed to respond to that notice in the manner prescribed by applicable regulations.”

In December 2013 the Government published The Defamation (Operators of Websites) Regulations 2013 setting out the notice and take-down procedures which website operators must comply with in order to avail themselves of a defence under the Act. Under the Regulations, website operators will have 48 hours following a notice of complaint to act. The first step will be to notify the poster (if the poster cannot be contacted the content should be removed). The poster then has five days to respond and, unless the poster provides an adequate objection to removal, the operator will have a further 48 hours in which to remove the content.272

C. Malicious Communications Act 1998

Preamble of the Act says that this Act is “An Act to make provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety”. According to Section 1 of the Act, it is an offense to send an electronic communication that conveys a message that is grossly offensive/ threatening to another person, where the message is sent with the purpose of causing distress or anxiety to that person.

The Act was drafted in a pre-internet stage but it has been updated in 2001 to enable it to target ‘electronic communication’ ‘oral or otherwise’. The speciality of the 1998 Act is that it is intended to apply to only one- to-one exchanges and not to one- to- many

broadcasting. The act clearly prescribes under section 1 that communication must be ‘sent to another person’.

**D. Protection from Harassment Act 1997**

The aim of this act is to protect the victims of harassment. It protects all victims of the harassment whether stalking behaviour, racial harassment, or anti-social behaviour by neighbours or harassment over social media pages.

Claims for harassment in the UK are generally brought under the Protection from Harassment Act 1996 or the Public Order Act 1994. The Protection from Harassment Act 1997 makes it a civil and criminal offence to harass two or more persons. Section 1 of the Act says that “the person whose course of conduct is in question ought to know that it amounts to or involves harassment of another if a reasonable person in possession of the same information would think the course of conduct amounted to or involved harassment of the other.” Section 2 of the Act says that “a person guilty of an offence under the Act is liable on summary conviction to imprisonment for a term not exceeding six months, or a fine not exceeding level 5 on the standard scale.” However, the imprisonment can be increased to up to 5 years and an unlimited fine if harassment causes the victim to fear violence. In order to show harassment a victim will have to demonstrate the alleged individual is causing harassment, alarm or distress by using threatening, abusive or insulting words or behaviour.

The act further says that the provisions of the act will not apply to a course of conduct if the person who pursued it shows-

- That it was pursued for the purpose of preventing or detecting crime,
- That it was pursued under any enactment or rule of law to comply with any condition imposed by any person under any enactment, or
- That in the particular circumstances the pursuit of the course of conduct was reasonable.
Various guidelines of the UK govt. encourage the use of the Protection from Harassment Act 1997 legislation where a particular individual is being targeted on social media, either by being put in fear of violence (the more serious offences under ss.4 and 4A), or by conduct that amounts to harassment, particularly through "stalking". Examples of "stalking" given in Sec.2A (3) (b) include contacting or attempted to contact a person by any means, and publishing any statement relating to a person or purporting to originate from them. Although a "course of conduct" must be proved, this may be shown by conduct "on at least two occasions" (in reality, a subjective assessment will be made of all the circumstances, and it is usual for conduct to be more extensive before it can be said that a reasonable person would be caused the requisite fear or distress).\textsuperscript{273}

\textbf{E. Obscene Publications Act, 1964}

In England and Wales, the main pieces of general obscenity legislation are the Obscene Publications Act 1959 and 1964, which make it an offence to publish an obscene article. The preamble of the act provides for “An act to strengthen the law for preventing the publication for gain of obscene matter and the publication of things intended for the production of obscene matter.”

It is an offence under this Act to publish an obscene article. Publishing under this act includes

- Distribution, circulation, sell, let on hire, giving, lending or
- In the case of an article containing or embodying matter to be looked at or a record, shows, plays or where the matter is data stored electronically, transmits that data.

An obscene article is one whose effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it.

Obscene Publications Act, 1964 has amended the Obscene Publications Act, 1959. The Act says that any person who publishes an obscene article shall be liable-

\textsuperscript{273} Jennifer Agate, ‘Social media: how the net is closing in on cyber bullies’ (2013) 8 Ent. L.R. 263, 268
- On summary conviction to a fine not exceeding one hundred pounds or imprisonment for a term not exceeding six months;
- On conviction on indictment to a fine or to imprisonment for a term not exceeding five years or both.

Section 2 of the 1959 Act which has not been amended by the 1964 Act further says that a prosecution for an offence under section 2 shall not be commenced more than two years after the commission of the offence.

F. Public Order Act, 1986

The Preamble of the Act says

“An Act to abolish the common law offences of riot, rout, unlawful assembly and affray and certain statutory offences relating to public order; to create new offences relating to public order; to control public processions and assemblies; to control the stirring up of racial hatred……………… obsolete or unnecessary enactments; and for connected purposes.”

Under this Act, it is an offence to, with the intent to cause harassment, alarm and distress, use threatening, abusive or insulting words, behaviour, writing, signs or other visual representation within the sight or hearing of a person likely to be caused harassment, alarm or distress. This offence may apply where a mobile phone is used as a camera or video rather than where speech writing or images are transmitted.

Where the abuse involves an element of race, religion or anything founded on disability, sexual orientation or transgender identity, the police and CPS are prepared to take the abuse particularly seriously. Part III of the Public Order Act 1986 may also be invoked (acts likely or intended to stir up racial or religious hatred, or hatred on the grounds of sexual orientation). In March 2012 university student Liam Stacey received a 56-day jail term for racially aggravated public disorder contrary to Sec. 31(1)(b) of the Public Order Act 1986 after tweeting "LOL" (laugh out loud) in response to the mid-match collapse of the footballer Fabrice Muamba and posting racist and offensive comments when other
users criticised him for the original tweet. A subsequent appeal against the sentence was dismissed.274

Users of social media should also be aware that whilst the Guidelines do not encourage the indiscriminate use of public order legislation (such as Part I of the Public Order Act 1986), as with many other statutes, they will be used in appropriate circumstances regardless of the fact that behaviour takes place online, and the user will not always be protected by the fact that he is acting from a private dwelling, rather than a public place. In 2012, Terry Balson was convicted of inciting others to riot after setting up Facebook group For the Riot "Fuck the Feds" which encouraged others to take part in the London riots in August 2011, although there was no evidence he had been present or physically participated in the riots.275


Regulation of Investigatory Powers Act confers power of intelligence agencies to intercept any communication. However, intelligence agencies must obtain specific legal permission to intercept “internal” communications – where both sender and recipient are based in Britain. Section 8.1 of the Act requires an individual warrant for the purpose of interception of internal communication but according to Section 8.4 no such warrant is required to intercept external communications.

Govt. of United Kingdom has defended its action to monitor the social media communication citing it as ‘external communications’. Speaking on behalf of the UK’s three intelligence agencies – GCHQ, MI5 and MI6 – Charles Farr, director-general of the Office for Security and Counter Terrorism, has accepted in a press brief that The British


275 Jennifer Agate, ‘Social media: how the net is closing in on cyber bullies’ (2013) 8 Ent. L.R. 263, 268
government has the legal power to monitor citizens’ activities on Facebook, Google and Twitter without specific warrants because they are based outside the UK.\(^\text{276}\)

Demos, a research institute based in UK has prepared a report on social media intelligence monitoring.\(^\text{277}\) The report proposes a regulatory framework that applies the Regulation of Investigatory Powers Act 2000 (RIPA) to social media, which would give the police clear guidance on using online data for criminal intelligence. Under this system, infiltrating a closed chat room to monitor conversations would require authorisation by a superintendent, while viewing private messages sent between individuals on Facebook could only be accessed with a warrant from the Secretary of State. The researchers go on to recommend the creation of a central national hub for collating and utilising social media intelligence – known as SOCMINT – that would encourage greater co-operation between forces and provide specialist training for analysts and those working closely with the Crown Prosecution Service.

H. Wireless Telegraphy Act 2006

The transmission of content wirelessly through the national radio spectrum network is regulated through the Wireless Telegraphy Act 2006 and has regulatory impacts for access to the Internet through wireless devices other than computers such as mobile phones & tablets etc. These devices which come with push technologies play a significant role in communicating a message instantly to other devices. These devices play most dominant role in creating social media mischief by instantly sending offensive/inflammatory/hate contents. This Act is helpful in preventing the access to these devices in sensitive situations.

\(^{276}\) Sam Jones and Robert Cookson, ‘UK has power to monitor citizens on social media, says counter-terrorism chief’ (FT, 17 June 2014) <http://www.ft.com/cms/s/0/ee25c112-f628-11e3-a038-00144feabdc0.html#axzz3dYI8j6zv> accessed on 25 June 2014

The regulation which affects the new communications services in UK has mainly developed around traditional and separate telecommunications and broadcasting markets. It is clear from the abovementioned discussion that UK regulation was not drafted with convergence in mind, and as a result the way in which existing rules apply to new communication services is something of an anachronism.\textsuperscript{278}

4.3 IMPLICATIONS FOR INDIA

From the above mentioned discussion it is clear that there is no single statute/authority for regulation of social media in UK and USA. If we compare the regulation of social media in India with United States, we see a lot of differences. The ground realities of India vary from USA and UK in terms of implementing the laws, policies and rules relating to social media. Though none of both legal systems offer a dedicated law to regulate the social media yet there are various lessons for India. Major deviations and similarities between India, USA and UK relating to social media regulation can be summarized under the following heads:

4.3.1 Major Deviations:

- To protect the privacy of employees, laws has been enacted in United States to prevent the employer from asking passwords of employee’s social media accounts. The laws in this field in India are still unsettled and only Ministry of Communications and Information Technology has issued a guideline for the use of social media in government organization. These guidelines cater strictly to government organizations and other employers are not to follow them.

- In United States, Computer Crime and IP Section of US Dept of Justice is responsible for implementing the department’s national strategies in combating computer and IP crimes worldwide. Whereas in India Computer Emergency

\textsuperscript{278} David Goldberg, Tony Prosser et al, \textit{Regulating the Changing Media: A Comparative Study}, (First edn., Cleardon Press, 1998) 118
Response Team works only for computer related crimes. For the matters connected with IPR violations, it possesses no powers.

- Cyber Crime Unit of every U.S. State Police inducts personnel having expertise in detecting cyber crime. However, in India Cyber Cells are limited to specific regions and their power and functions are more investigatory in nature. Cyber cells in India do not have much prohibitory powers to control the social media mischief.
- The safe harbour provisions coupled with complete protection of free speech in USA has given ISPs a free hand to work independently and without any substantial interference from the government. However, in India as we have already seen in Chapter 2, ISPs immunity provision is ill drafted.

4.3.2 Similarities

- For a variety of reasons all these legal systems have not responded to social media regulation with a single statute. There are different sets of laws for different kind of offences committed over social media pages in India, United States and United Kingdom.
- Almost all of them provide for safe harbour provision to intermediaries.
- All of these legal systems are more favourable for ‘regulation’ rather than ‘monitoring’ of social media behaviour.

4.4 CONCLUSIONS

The social media regulation in UK and US is relatively far better than ours because of a relatively better legislative framework touching on the issues which arise in social media. There are numerous corresponding legislations and regulations which effectively control the mischief which arises primarily at social media for example, Computer Fraud and Abuse Act, ECPA, DMCA, DCA, SCA, FWA, COPPA etc. These legislations are not primarily media legislation and much less social media legislation but these are corresponding legislations which effectively trap and regulate the mischief arises at social
If we locate our own position, forget about media and social media legislations, we have not devised the corresponding legislations as are there in UK and US. It is because of these reasons that whenever a mischief is noticed at social media fora we suffer greater injury, heat and flux as compared to the position in these two leading legal systems. In a sense, we are lagging far behind in terms of devising a core of regulatory mechanism and a supportive preferential legislative mechanism. There is a pressing need for continuously revising the legislative measures to keep the social media behaviour in accordance with law. Perhaps it would be best suited to find a common agreement at the international level to adopt universal guidelines for regulation of social media. Attempts of state laws to regulate social media webs, which are transnational in character, is a futile exercise.