RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF JURIDICAL SCIENCES

COURSE:BA.LL.B

Semester : VIII th

SUBJECT: Cyber Law

SUBJECT CODE:BAL-805

NAME OF FACULTY: Dr.Puja Paul Srivastava

RAMA UNIVERSITY

Lecture-28

LECTURE 28: Legal implications of social networking,

The Legal Implications of Social Networking: The Basics

We are in the midst of a communications revolution. Use of social media for communication purposes continues to grow, while "old school" messaging media like email is on the decline. Facebook reportedly has reached 700 million users worldwide and is putatively valued at $50 billion dollars. Advertising revenue expected to be generated from social media is estimated to reach $8.3 billion dollars annually by 2015. Significantly, according to one survey, 81% of companies have implemented (or plan to implement) social networking in order to enhance their exposure. Seventy-three percent of small and medium businesses reportedly employ social media for marketing purposes.

Much like the "Cloud computing revolution" there is an almost frenzied excitement around social media, and many companies are stampeding to exploit social networking. The promise of increased intimate customer interactions, input and loyalty, and enhanced sales and expanded market share can result in some organizations overlooking the thorny issues arising out of social networking. Many of these issues are legal in nature and could increase the legal risk and liability potential of an organization employing a social media strategy.

Coming on the heels of a white paper we wrote with ACE USA, in this multi-part series the InfoLawGroup will identify and explore the legal implications of social media. This series will help organizations begin to identify some of the legal risks associated with social media so that they may start addressing and mitigating these risks while maximizing their social media strategy.

In Part One of the series, we will provide a high level overview of the legal risks and issues associated with an organization's use of social media. In subsequent parts members of the InfoLawGroup team will take a deeper dive into these matters, and provide some practical insight and strategic direction for addressing these issues. As always, we view our series as the beginning of a broader conversation between ourselves and the larger community, and we welcome and strongly encourage comments, concerns, corrections and criticisms.

What is Social Media?

For a phenomenon that is taking over the world, one would think that the meaning of social media would be clear. While that may not be the case, we are not going to belabor the issue in this post. Instead we will simply use the definition generated by Wikipedia (itself a form of social media that relies on the collective efforts of its users to come up with the "right" answer):

Social media are media for social interaction, using highly accessible and scalable publishing techniques. Social media use web-based technologies to turn communication into interactive dialogue.

Examples of websites and internet activities that fall into this definition include: LinkedIn, Facebook, Twitter, Digg, Delicious, StumbleUpon,Foursquare, blogging platforms (e.g. WordPress, Drupal, etc.), Wikipedia, bulletin boards (e.g. phpbb.com), Quora and YouTube.

The InfoLawGroup is a heavy user of social media, and the best way that I have been able to explain our social media is by analogy: social media is like a wide-ranging conversation that can be with the entire world, or on a very intimate level with a single individual, and often both. Social media provides a mechanism for finding communities of like-minded (or not) individuals interested in particular topics (and sub-topics). InfoLawGroup uses social media to engage in conversation concerning issues that are important and interesting to us (and others), and by engaging in that conversation in a meaningful way, others begin to recognize and value our input (and we in turn discover experts, influencers, and valuable information resources). Based on our experience, the key attributes of a successful social networking include clear communication, multi-party interaction, trust and intimacy.

How is Social Media Used?

So your organization wants to "use" social networking. Why? For many organizations considering the use of social media a vague idea may exist that they "should" be doing that. However, clear organizational goals may not exist concerning the use of social media. As a threshold issue, before even considering specific legal issues, organizations must have a clear idea of why they want to use social media. Companies should identify the business process or organizational strategy they are seeking to advance by the use of social networking. They should be able to establish goals and metrics in order to measure success and allow for the adjustment of their strategy if it is not proving successful. Of course, when the question of why is answered, then the question of "how" must be addressed (and often the two questions must be considered together).

The process of developing a social media strategy tied to specific business processes and goals will enlighten companies as to the legal implications of their use of social networking. While there may be certain legal

concerns baked into “social media” in general, many of the legal risks will arise based on the specific business process and goals surrounding the use of social media. In addition, the characteristics of the social media platform(s) an organization chooses to leverage may also impact the legal risks faced by the organization. While there are as many social media strategies as there are organizations seeking to employ them (in fact, there are certainly many more), we have laid out some “use cases” that will help us explore the legal implications of social media:

Direct Interaction. Direct interaction (with customer, "influencers," media, colleagues, etc.) is really the most basic use of social media, it involves an organization using social media to communicate and interact with the general social media population (or subsets of that population). This would happen on various social media platforms such as Facebook, LinkedIn and Twitter, or through a weblog. However, the approach organizations employ to interact may vary, and as discussed later, the differences in approach could impact the legal risks associated with social media. Some approaches for direct interaction include the following: (a) allowing an organization’s general employee population to go out and interact on behalf of the company with little instruction or supervision; (b) allowing an organization’s general employee population to go out and interact on behalf of the company with strict instructions and supervision; (c) identifying a small dedicated group to interact on social media on behalf of the company, including potentially the use of “corporate profiles” not tied to any individual person; and (d) hiring a third party marketing company to interact on social media pursuant to a specific marketing strategy.

Company Page/Fan Site. Some social media platforms allow organizations to create “fan pages” (e.g. Facebook) or company pages (LinkedIn). In essence these types of pages/site allow an organization to set up a centralized presence or "destination" within a social media platform. Interested individuals can then join or follow postings that occur on the organization’s fan page/site, and those visitors can themselves post and interact on the fan page or site. This allows for interaction in a more centralized fashion.

Social Media Applications. Some social media platforms may allow organizations to create applications that can be plugged into the social media platform. For example, a mortgage broker with a presence on Facebook could hire an application developer to develop a mortgage interest rate calculator application that Facebook users could operate. This would essentially provide an advertisement for the mortgage company and create goodwill amongst potential customers. In addition, when the application is downloaded by a user, the mortgage company would then get access to certain personal information that is part of the user’s profile. This information can be valuable for targeting prospective customers and data mining purposes.

Blogging. While it may not be obvious to everybody, most blogs constitute social media. Blogs that allow for comments and interaction between the blogger and his readers (and interaction between the readers themselves) are social media. This interaction typically occurs in the “comments” section of a blog. In addition, many organizations use their blog as the kernel for interaction in other social media platforms. So, an organization with a blog might do a post and tweet it on Twitter, cross-post it on their Facebook fan page and post it in a LinkedIn Group, in order to drive traffic to the company’s blogpost (and ultimately website, product or service).

Social Plug-ins. Many social media platforms provide “widgets” or “plug-ins” that can be put into a website to allow the content of the website to be commented upon and shared within the social media platform. The plug-in may be in the form of a “button” that allows a website visitor to “like” particular content and have their preference posted in Twitter, Facebook or Digg. Some social medial platforms may be seamlessly integrated into a website in such a manner that makes it virtually invisible. Using these plug-ins can help` spread an organization’s message to a much wider audience and drive traffic to the organization’s website.

Log-In Credentials. Another interesting way social media platforms are being utilized is to allow website visitors to login to an organization’s website employing the log-in credentials they use to gain access to a social media platform. Under this scenario an organization with a website could allow visitors to access the company's website by logging into their Facebook or Twitter account using the same username and password (this is achieved by utilizing the social media platform’s API). The organization benefits in several ways by employing this practice. First, the visitor gets to avoid setting up a new username and password specific to the website, which can be viewed as time-consuming by some visitors. Second, the user is less likely to forget a username/password from a frequently-used social media platform, and this makes logging in very easy. Last, by linking to the social media platform’s authentication credentials, the organization is able to obtain certain personal information about that visitor that is available on the social media platform.

The forgoing use case scenarios are surely the tip of the iceberg, and new social media platforms and strategies are being developed every day. It is in this dynamic environment that organizations must analyze and understand the legal risks associated with the use of social media.

Social Media Legal Issues

As we work through the various legal implications of social media it hopefully will become increasingly clear

that context is very important. While we can (and will) talk about broad categories of legal risks that apply to most (or all) social media, a basic formula can be used to identify and analyze the specific legal risks of a particular social media use. The social media legal risk "formula" can be summarized as follows:
the inherent characteristics/capabilities/limitations of the social media platform to be leveraged, PLUS
the organization's specific intended social media strategy and uses, REVEALS
the relevant legal issues and level of legal risk present.
With this formula in mind we turn to a short summary of the social medial legal issues that InfoLawGroup will be exploring in detail as part of its multi-part blog series.

Information Security Legal Risk

Organizations that employ social media face several information security legal issues. These legal risks can be broken down into three broad categories: (1) potential liability due to a breach of the organization's security as the result of an attack originating through the use of social media; (2) potential legal risk associated with social engineering and spoofing attacks against users or "fans" of an organization's social media presence, persona or application; and (3) legal consequences of leakage of third party confidential information as a result of social media use.

As might be expected organized crime views social networks as fertile ground for committing fraud. One of the biggest risks is in the name of the medium itself. Social media yields social engineering. Fraudsters leverage the central component of social media that makes it so attractive: trust between "friends." As such social media users are tricked into downloading applications infected with malware because it was "recommended" by a friend, or they click on the link of the "real" Osama Bin Laden dead body photo that looks like it was posted on a friend's wall (and a computer attack occurs), or they visit a site that looks like a brand name company's fan page and are enticed to provide some of their personal information to criminals.

The direct risk to an organization allowing its employees to use social media on company computers is obvious: if malware from social media infects a company computer and steals personal information, credit card numbers or trade secrets, the company may have to provide notice of a security breach and could face lawsuits and regulatory actions arising out of the breach.

Companies may also face liability for failing to detect and notify social media users of scams associated with the company's name or site. If an organization becomes aware of a spoofed fan page that looks like its own, or a criminal disseminating a malware-infested social application that looks like it is sponsored by the organization, legal repercussions could arise. In the email context we are already aware of lawsuits involving phishing that allege that the defendant should have been aware of scam emails sent to their customers, and should have warned those customers of the scam.

Finally, social media sites and the activities of multiple users for or on behalf of an organization could result in information leakage. If that leakage involves confidential information or trade secrets of an organization's customer, or perhaps certain financial disclosures in violation of securities laws, liability could arise. The risk of confidential information leakage was recently on display involving the use of LinkedIn. This risk can also be indirect in its nature, and there are several social media corporate intelligence companies that will data mine and aggregate information about competitors in order to discover leaked secrets, plans and trends.

Privacy

For many companies the Holy Grail of social media is in depth and detailed personal information about their current and would-be customers. Social media provides a platform for much more interactive and intimate communications between companies and their customers. In turn companies seek to use this knowledge to sell their products and services back to these customers (in a way that does not erode the trust relationship that is often gained in the social media context). Social media platforms enable the gathering of information, including personal information, in ways that were unimaginable only a few years back. Companies leveraging social media, depending on the platform, can gain access to this personal information. This raises a host of privacy concerns that could increase legal risk. Most social media sites have terms and conditions that may result in legal liability if an organization's collection or use of personal information violates those terms. Laws such as COPPA may have applicability with respect to an organization's "fan" page. Finally, to what extent do an organization's privacy policies apply, if at all, to its social media activities? All of these issues will become increasingly important as use of social media becomes the norm.

IP Infringement

Social media sites allow users and companies to post content, including content that may be copyrighted or trademarked. Posting can be performed not only by employees of organizations using social media, but also fans and visitors to a company's social media site. Organizations may face infringement claims (direct or based on vicarious liability) due to copyrighted or trademarked materials being posted by them or by third parties.

Disparagement and Defamation

Social media environments provide a forum for defamatory statements to be made about individuals, and disparaging remarks to be made about companies' products and services. Organizations with overzealous employees attempting to get a leg up on competitors may post comments or remarks that may not be fully accurate or true about an individual or a competitor's products or services. This could lead to a potential lawsuit and liability. Social media sites and blogs that allow comments may also involve such statements made by third parties over which the organization has little to no control. While defenses may exist, including potentially Section 230 of the Communications Decency Act, this area of law is notoriously fact specific and varies by jurisdiction, and it could pose problems for companies.

Employment Law Issues

The use of social media in the employment context raises a lot of tricky legal issues. First, many organizations use social media to vet candidates for employment and as part of background checks. The information obtained from a social media site may constitute a "consumer report" under the Fair Credit Reporting Act and similar state laws, and employers may have to obtain an individual's consent before accessing such information (or may be prohibited from using that information to make employment decisions). During employment, the issue is to what extent an employee may have privacy rights concerning its use of social media while at work, and to what extent the employer may monitor such activities. Overzealous employers that create fake social media accounts to monitor social media activities of their employees could also raise legal issues, including issues under the Stored Communications Act, which is part of the larger Electronic Communications Privacy Act. Finally, using social media activities as the basis for firing or taking disciplinary action against employees may run afoul of the law. Recently, there have been a series of "Facebook Firings" where the National Labor Relations Board has alleged that and employer's action violated the National Labor Relations Act.

Advertising Law

Organizations that use social media to promote their products and services should also be concerned about advertising laws. For example, some social media activities may amount to a contest or sweepstakes and may need to have appropriate disclaimers and notices. In addition, for social media sites that allow users to rate products or services, an employee that "rates up" the products or services of his or her company may violate advertising laws concerning testimonials and endorsements.

Electronic Discovery and Evidence

Social networks are brimming with social interactions and information generated by and about those interactions. That information may be highly relevant in a litigation context, and the parties in a litigation may seek to obtain this information via discovery or subpoena. Questions arise as to whether obtaining this information for use in court is permissible in light of potential privacy concerns. On the flipside, when litigation begins, how should lawyers advise their clients concerning the preservation of information on social media sites, and what kind of problems may arise if a litigant fails to preserve social media information.

Drafting a Social Media Policy

In the final part of this series, we will take a closer look at one of the key controls to address the legal risk associated with the use of social media: the social media policy. We will look at the key elements and issues that should be addressed in a social media policy, and identify strategies for dealing with this risk. In addition, we will discuss some new technological controls that companies are developing to help organizations understand, monitor and manage social media use and legal risks. Overall, there is much more to come on this topic. Stay tuned!

SELF-TEST QUESTIONS

S.NO	Question	Option (a)	Option (b)

1.			
2.			
3.			
4.			
5.			

Answers: 1-(),2-(), 3-(),4-(),5-()