

## Social networking sites and identity theft

By Priti Suri  
and Dhruv Suri,  
PSA,  
Legal Counsellors



PSA

PSA  
Legal Counsellors  
14A & 14B Hansalaya, 15 Barakhamba Road  
New Delhi - 110001, India  
Tel: +91 11 4350 0500  
Fax: +91 11 4350 0502  
www.psalegal.com  
Email: p.suri@psalegal.com

The chief justice of India, KG Balakrishnan, has noted that democratic values such as “freedom of speech and expression”, “freedom of association” and the “freedom to pursue an occupation, business, profession or trade” need to be protected in the online domain as well.

Social networking sites have become extremely popular over the years, so much so that some workplaces have banned employee access to them. Facebook, Twitter, Orkut, LinkedIn, etc., instantly connect their members with each other and allow them to share information, photographs, contact details, status updates and a lot more almost free of charge. This raises a plethora of legal issues with respect to the uploaded content, such as copyright infringement, compliance with local legislation, identity theft, defamation, etc.

India has fewer legal precedents on defamation or abuse through websites than the US or Europe. Most cases in India relate to creating and posting fake profiles of women, describing them with lewd comments, or posting content online that infringes someone’s copyright.

In the context of identity theft, it is crucial to understand what recourses are available. The first step is to ask the website owner to remove the fake profile. Requests should be accompanied by sufficient evidence in the form of the URL of the impugned profile page, URL of the aggrieved person’s profile page (if any) and the relevant webpage snapshots. The time taken by the website to remove the forged profile is of essence; any delay may defeat the purpose of reporting the offence. In most cases though, the website owner will take timely and adequate action.

If the fake profile is not withdrawn, the aggrieved person has legal recourse under the Information Technology (IT) Act, 2000, in addition to the provisions

of the Indian Penal Code pertaining to cheating by personation, defamation, etc. If the accused has accessed the complainant’s computer system without permission and extracted data, he or she can be prosecuted for damaging a computer by downloading information from it and punished for identity theft under section 43(b) read with section 66C of the IT Act respectively.

Further, if the fake profile consists of obscene images of the complainant or of any third party, the accused can be prosecuted under section 66E (punishment for violation of privacy) read with section 67 (punishment for publishing or transmitting obscene material in electronic format) of the IT Act. Such offences provide for a maximum imprisonment of three years along with a fine of up to Rs500,000, (US\$11,000) except for violations to sections 66C and 66E which incur maximum fines of Rs100,000 and Rs200,000 respectively.

Interestingly, section 77B of the IT Act states that all offences punishable with imprisonment of three years and more are cognizable, i.e. arrests can be made without a warrant, and those up to three years are bailable. This implies that the accused, in most cases of identity theft on a social networking site, will be able to procure bail. Therefore, it is crucial that the complainant registers a first information report with the cyber cell of the state police under the Criminal Procedure Code, 1973 (CrPC). Alternately, a written complaint may be filed with the superintendent of police under section 154(3) of the CrPC or a court may be directly approached under section 200 to direct the police to investigate the offence.

While resorting to provisions of the IT Act and the CrPC, it is important to understand some practical concerns. A cyber crime causes damage almost instantaneously, however, the investigation and

prosecution process is time-consuming and often frustrates the complainant. Previously, not too many cases were reported to the cyber cell due to lack of awareness among the general public and lack of sufficient technical expertise among cyber cell officers. However, the situation looks more positive now with more cyber cells being set up in different cities across India.

Extradition concerns are also quite prevalent when the accused is residing outside India. With the world becoming “flatter”, it is crucial that such apprehensions are adequately addressed. The Indian government must execute extradition treaties, at least with those countries which account for a large percentage of cyber offences in India, and also enforce and implement such extradition when the need arises. Most importantly, for the effective enforcement of such cyber regulations, India still needs cyber-savvy judges, who can understand, interpret and enforce the law comprehensively.

Social networking sites have, in a lot of ways, bridged geographical and generational barriers. Nevertheless, they come with troubles of their own, which one must be aware of before posting information online. One thing is certain, no data in the virtual world is 100% secure. Data back-up and records are created and stored at every stage and remain on servers even when individuals have removed their profiles from a site. Therefore, as long as data is stored somewhere in the world, there is always a possibility of breach of privacy. Sharing content through social networking sites is not a bad thing as long as sensible personal boundaries are drawn. After all, self regulation is the best regulation!

*Priti Suri is the proprietor of PSA where Dhruv Suri is an associate.*