2011 International Conference on Social Science and Humanity
IPEDR vol.5 (2011) © (2011) IACSIT Press, Singapore

Information Gathered on Social Networking Sites and the Law of Confidence

Manique Cooray
Faculty of Business and Law
Multimedia University
Malacca, Malaysia
Email: manique.cooray@mmu.edu.my

Abstract—the acquisition and transaction of personal information in electronic form through digital technology such as data collection, recording, storage, processing, use, exchange or trade may be performed by persons, group of persons or other entities from both the public and the private sector. They may include government departments, agencies and other public or quasi-public bodies as well as sole proprietors, businesses and other forms of corporate entities.

Similarly, the want or the need to reach out to a wide audience using communications technology, including through unsolicited means, is common to non-profit and profit organizations alike. The biggest benefactor of these is social networking sites. This paper examines the legal basis for protecting such information gathered on social networking sites with reference to principles under the law of confidence.

Keywords-confidence,information,privacy,social-networking sites.

I. INTRODUCTION

The acquisition and transaction of personal information in electronic form such as data collection, recording, storage, processing, use, exchange or trade may be performed by persons, group of persons or other entities from both the public and the private sector [1]. They may include government departments, agencies, public or quasi-public bodies as well as sole proprietors, businesses and other forms of corporate entities. The want or need to reach out to a wide audience using communications technology, including through unsolicited means, is common to non-profit and profit organizations alike [2].

Similarly, commercial entities may post information online that can lead to great personal embarrassment and, at times individuals themselves may voluntarily post information leading to severe consequences relating to violations of their rights to privacy.

Drawing a line between information that can be disclosed to the public and information that is private as to violate all levels of decency has not proven simple, especially so, as much of the power of the Internet derives from companies' ability to disseminate widely private information that had only a limited audience previously [3].

Fred Cate, in his book *Privacy in the Information Age* illustrates the power of digital informational management and retrieval [4]. He offers four generic reasons for the growth of digital information. According to him firstly, it is easier to generate, manipulate, transmit and store information digitally. Individuals with simple database programs such as Microsoft can manage and manipulate more data on a simple home computer. Secondly, the cost of collecting, manipulating, storing and transmitting data is lower. Cheap storage media such as CDs, DVDs, and the advent of cheap Internet access devices and the development of file sharing systems such as *KaZaa* means that, for a lesser payment, thousands of pages of data may be uploaded, downloaded or stored. Thirdly, due to its very nature, electronic information has developed an intrinsic value not found previously. This is due to the fact that digital information is cheaply processed and stored and it attracts a premium in the marketplace. This market encourages gatherers' of information to favour the collection of digital information over analogue information, leading to vast increase in the volume of digital information available. Finally, Cate notes that the operating parameters of computer systems and networks generate additional digital information through back-up copies and cache copies.

Due to these four factors, Cate records that "we are witnessing an explosion in digital data." Therefore, digitisation of information has caused a shift in the management, sharing and processing of data which has brought about important social and societal changes.

Social networking sites have been the biggest benefactor of all with the reference to the above factors identified. For example, for the vast majority of the existence of Facebook its primary differentiator was that the user's data was only visible to other's that are approved by the user. Text, photographs and video updates shared on the site have always been by default private. As of mid December 2009, Facebook users were no longer allowed to hide from the web-at-large information including their profiles, photographs, list of friends and interests in the form of "fan pages" they followed. If the user had not changed the privacy settings before December 2009, Facebook suggested that the user switch them to make those updates publicly visible to everyone. That became the new default.

As a way of calming anger about the social network's privacy policy Facebook unveiled a new set of user controls policies. The new controls, allows the user to receive login notifications anytime someone accesses the users Facebook account from an unknown device. Another provides supplemental security questions during "suspicious logins." Neither however, addresses the issue of how Facebook is handling the personal information of the user.

The question is whether the information which is retained by making data public by requirement and some data public by default is protected as confidential information as reliance

on legal or equitable rights to protect confidential information is one of the ways in which the use and disclosure of personal information may be controlled on the Internet

II. THE TYPES OF INFORMATION

Research on privacy indicates the several dimensions on the types of information in existence [5]. Informational privacy is highlighted as the focus of this paper is on information privacy. Informational privacy emerged as an issue during the late 1960s and early 1970s, when seminal works by Westin and Miller laid down the issues and offered definitions that remain influential to this day [7].Westin states that informational privacy lets individuals determine for themselves when, how and to what extent information about them is communicated to others, where as Miller framed the concept as giving individuals the ability to control the circulation of information relating to them.

III. GATHERING OF INFORMATION ON SOCIAL NETWORKING SITES

Facebook, one of the most popular social networks in the world, has more that 400 million registered people on its Website. According to reports, half of these users log into the service every day, and users spend 500 billion minutes on the site each month. Facebook's Privacy Policy is 5830 words long. It is said that the United State's Constitution, without any of its amendments, is a concise 4543 words [6]. However, in recent months, Facebook has revised its privacy policy to require users to opt out if they wish to keep information private, making most of that information public by default. Some personal data is now being shared with third-party websites.

As a result, the company has come under scrutiny from privacy groups, government officials and its own users, who complain that the new policy is bewildering and the new opt-out settings too time consuming to understand and use. The new opt-out settings certainly are complex. To opt out of full disclosure of most information, it is necessary to click though more than 50 privacy buttons, which then require choosing among a total of more than 170 options. Users must decide if they want only friends, friends of friends, everyone on Facebook, or a customized list of people to view information such as birthdays or their most recent photographs uploaded. To keep information as private as possible users must select "only friends" or "only me" from the pull-down options for all the choice in the privacy settings, and must uncheck boxes that say information will be shared across the Web.

Even if a user changes all the settings on the privacy section of the site, certain pieces of information will still be shared across the site unless a user takes further action. For example, under the Account Settings Option, in the Facebook Ads tab, two options are automatically turned on to share some information with advertising networks and friends. Anyone who wants to keep this information private must uncheck the boxes in that tab. And still some information will no longer remain private as Facebook has also added a feature known as community pages, which automatically links personal data, like hometown or university to other links for that town or university.

Facebook finally unveiled a new, simpler privacy policy in April 2010. This includes aggregating all privacy settings into one simple control; blocking unwanted visitors to the user's profile and others; and preventing third-party applications from sneaking into the user's personal information. Furthermore, the new features require outside applications and websites to inform users exactly what parts of their profiles have to be shared for the applications to work.

Under the new policy, the services will inform which aspects of a profile will be made public. The user however, will not be able to pick out which piece of information they want to grant access to. The users either grant permission or disallow the application from working at all.

According to Facebook's founder Mark Zuckerberg "the world has changed. It is now more public and less private and that the controversial new default and permanent settings reflect how the site would work if he were to create it today."

Most recently, privacy advocates and lawmakers have complained about Facebook's instant personalization feature which draws information from user's profiles to customize a handful of other sites, including review site, and the music service Pandora.

IV. RISKS AND THREATS OF GATHERING INFORMATION ON LINE

The loss of control over private information can result in serious adverse consequences. First, and of growing concern is identity theft. Identity theft occurs when criminals use information about third parties to assume their identity and leave the third party with unpaid loans or credit charges. With personal information about an individual such as a name, birthday, address, job history, they can accumulate additional information to apply for credit as an imposter. Second, many individuals are concerned instead about the more intangible loss of privacy on the Internet. Much of the harm arises because direct marketers sell information about users to companies on and off the Web and as such companies then may send us unwanted e-mail messages, or promotions. Information mined by one website can be combined with information from others to present a remarkably accurate portrayal of our spending habits.

Social networking sites such as Facebook share personal individual information with affiliates. Therefore, such personal information should have some protection as it falls within the parameters of informational privacy.

V. APPLICATION OF THE PRINCIPLES OF THE LAW OF CONFIDENCE

Breach of confidence has traditionally been concerned with protecting four main classes of information: trade secrets, personal confidence, government information and artistic and literary confidence. For information to acquire the quality of confidence however there must be some

application of human skill and some selection. As stated by Megarry J., in *Coco* v. *AN Clark (Engineers) Ltd* [1969] RPC 41:

"Something that has been constructed solely from materials in the public domain may possess the necessary quality of confidentially; for something new and confidential may have been brought into being by the application of the skill and ingenuity of the human brain. Novelty depends on the thing itself, and not upon the quality of its constituent parts."

Therefore three requirements must be met for information to be protected as confidential information. The information must have a quality of confidence; it should have been communicated in circumstances importing an obligation of confidence; and there must be an unauthorised disclosure of that information.

Development of the principle over the years indicate that the information protected is not limited to trade/business, but also personal information *(Prince Albert* v. *Strange*, 1849), including sexual information (*Argyll* v. *Argyll*, 1967) and the obligation of confidence is not confined to original confidante but third parties as well. In *A-G* v. *Guardian Newspapers Ltd (No. 2)*, 1990 and in *Venables* v. *Times Group Newspapers*, (2001) the relaxation of the need for an initial confidential relationship between the parties was highlighted. This rule was modified in *Campbell* v. *MGN Ltd*., (2004) to extend to information to be "confidential" to cover "private" information as well.

VI. CLASSES OF INFORMATION WHICH MAY BE PROTECTED AS CONFIDENTIAL INFORMATION

It has been said that equity will intervene whenever a person's private affairs are liable to be exposed, regardless of whether that exposure would cast a doubt on the credibility of the person. The classes of information which may be protected as confidential information are:

(a) Information about health and medical treatment;
(b) Information about sexual life;
(c) Information about appearance;
(d) Other information about identity;
(e) Information about private acts;
(f) Information about knowledge of or involvement in Crime;
(g) Financial and business information;
(h) The contents of personal communications and Conversations.

Where parties have agreed by an express contract to characterise a particular class of personal information as confidential that will in general suffice to identity it as such. If as in many of the networking sites that there is no contract then a clamant will need to establish by other means that the information in issue has the "necessary quality of confidence about it." Therefore, some kinds of personal information are now authoritatively classified as confidentail in character. The criteria by which that classification is arrived at have however, receive relatively little analyis.

If a case is concerned with information outside the established classes it is necessary to determine that the information has the necessary quality of confidence. Therefore, for information gathered on social networking sites to have the level of confidentail information the above criteria must be established.

REFERENCES

[1] Raul, A, Privacy and the Digital State (Norwell: Kluwer International, 2002) pg.1.According to the writer informational privacy i.e., the ability to control information about oneself, is one of the defining concerns of the American public at the beginning of the 21st century.

[2] D. Murray Andrew, "Should States Have a Right to Informational Privacy?", Human Rights in the Digital Age, Ed., Mathias Klang & Andrew Murray, (Great Britain: The GlassHouse Press, 2005) pp.191-202.

[3] Edwards, Lillian, "Consumer Privacy, Online Business And the Internet: Looking for Privacy in All the Wrong Places," (2003) 11 IJL & IT at 226.

[4] Cate, F, Privacy in the Information Age (Washington, DC: Brookings Institution Press, 1997) pp.14 -15.

[5] Cho, H. and Larose, R., "Privacy Issues in Internet Surveys" (1999) 17(4) Soc.Sci Comp. Rev., 421-434.

[6] Bilton Nick, "Price of Facebook Privacy? Start Clicking" (New York Times May 12, 2010). Available at: http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html .

[7] Westin, A Privacy and Freedom (New York: Athenaeum, Prologue, 1967) pg.45