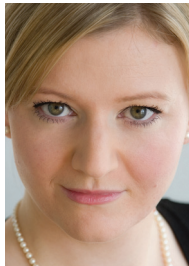


UK government's guidelines for social networking sites



BY CATE HAYWOOD
solicitor,
Harbottle &
Lewis LLP

IN APRIL 2008 THE HOME OFFICE TASK FORCE ON child protection on the internet published a guidance note offering good practice recommendations for the providers of social networking sites. The aim of the guidance is to enhance the online safety of children and young people and was drawn up in consultation with websites, mobile phone operators, children's charities and academics. As well as providing an educational resource for parents, the guidance seeks to provide service providers with practical advice on how they should operate social networking sites to adequately protect young people.

STATUS OF THE GUIDANCE

The guidance note is not legally binding but is offered to online service providers with a strong recommendation for its use. The incentive for businesses to follow this guidance is largely reputational; to attract users and reassure parents, social networking sites need to prove themselves to be morally responsible.

WHY IS CHANGE REQUIRED?

The world wide web is currently evolving to become a newer, more dynamic and more interactive medium. The enhanced creativity and collaboration that social networking sites promote represents part of a movement in internet culture that is known as 'Web 2.0'. While Web 1.0 was made up of static websites, the download of content and the use of search engines; Web 2.0 has grown into a more dynamic environment, where content is often generated by users and shared with others.

Social networking sites, such as Facebook, MySpace and Bebo are playing a big part in this movement and are hugely popular at present, particularly with younger users. According to a recent study by the media regulator, the Ofcom, millions of children are using social networking websites intended for older users. The Ofcom research shows that just over one-fifth (22%) of internet users aged 16-plus, and almost half (49%) of those aged 8-17 who use the internet, have set up their own profile on a social networking site. Perhaps most alarmingly, more than a quarter (27%) of children aged 8-11 claimed to have a profile page on a social networking website, despite restrictions on such sites aimed at preventing under-13s from using them. As an aside, it should be noted that there is no legal reason in the UK why 13 years is the minimum age. The reason many service providers operating in the UK and other jurisdictions choose this as their minimum age is due to the fact that many sites are owned by companies based in the US and must comply with US law, which designates 13 as the age that distinguishes children from young adults.

The research also found that users are not especially concerned with privacy and that while two-thirds of parents claim to set rules on their child's use of social networking sites, only just over half of children said that their parents set such rules. Further areas of risk were identified, such as the fact that 41% of 8 to 17 year olds with profile pages left their privacy settings 'open' so that anyone could see them. The research also found that younger users were more likely to give out sensitive personal information via their profiles, including details of their phone number, home address or e-mail address.

As the Home Office guidance note points out:

'Social networking and user interactive services offer many positive opportunities for children and young people to communicate, interact, and share content and interests. However, children and young people (under the age of 18) may also be vulnerable to inappropriate or harmful contact through these services. As in the real world, there is no environment that is completely safe.'

In publishing this guidance, the government recognises that co-operative efforts between business, government, law enforcement and users are necessary to create a safer, more secure online environment for children and young people. A significant part of this task involves the improved education of children and parents to help them appreciate the benefits and risks associated with social networking sites. However, a good proportion of responsibility lies with the providers of social networking sites to protect and enhance the safety of children and young people using their services.

RECOMMENDATIONS

The Home Office guidance note offers a number of recommendations to social networking site providers. A selection of the most important recommendations are as follows:

- Social networking sites should change the default privacy settings of under-18s to private. The Ofcom research estimates that millions of children who use social networking sites are exposing themselves to potential danger by leaving their privacy settings open. This is largely due to a lack of understanding of the implications of the privacy settings and a lack of knowledge of how to change them.
- Social networking sites should ensure that the private profiles of under-18s are not searchable unless consent is given.

- Social networking sites should clearly state during registration what information will appear on a user's profile and what will be private. Users should then be given the opportunity to hide, limit access to or edit this information.
- Social networking sites should offer clear and straightforward ways for children and young people to report suspected abuse, including the emergency 999 telephone number and the telephone numbers of child welfare organisations, such as the National Society for the Prevention of Cruelty to Children and Childline.
- Social networking sites should encourage children not to provide excessive information about themselves.
- Arrangements should be made for industry and law enforcement to share reports of potentially illegal activity and suspicious behaviour.

OTHER LEGAL CONSIDERATIONS

While the Home Office guidance represents a new set of requirements for service providers to consider, it is worth remembering that there are already laws that affect social networking sites:

Criminal Justice and Immigration Act (CJIA) 2008

Although not yet in force, a new law was recently passed, the CJIA 2008, which contains provisions to allow the Secretary of State to increase the notification requirements of sex offenders. At present, sex offenders can be required to notify details such as their name and address to the police. However, the new notification requirements could include the registration of any e-mail addresses. The government has suggested that this blacklist of e-mail addresses would be made available to social networking sites, which would be required to check it against the e-mail addresses of their user base and deactivate any accounts that are matched.

Data Protection Act (DPA) 1998

In the UK, organisations that process information relating to living, identifiable individuals are required to comply with the provisions of the DPA 1998. There is a strong argument that service providers need to take extra care when processing information about children to ensure compliance with the Act. This will include social networking service providers who collect personal data from users to enable registration.

In 2007 the Information Commissioner's Office (ICO) published a good practice note for website operators that included a section for sites directed at children, which stated:

'Websites that collect information from children must have stronger safeguards in place to make sure any processing is fair. You should recognise that children generally have a lower level of understanding than adults, and so notices explaining the way you will use their information should be appropriate to their level, and should not exploit any lack of understanding. The language of the explanation should be clear and appropriate to the age group the website is aimed at. If you ask a child to provide personal information you need consent from a parent or guardian, unless it is reasonable to believe the child clearly understands what is involved and they are capable of making an informed decision.'

The DPA 1998 does not state a precise age at which a child can act in their own right. It depends on the capacity of the child and how complicated the proposition being put to them is. As a general rule, the ICO considers the standard adopted by TrustUK (the UK body set up by the government to approve online codes of practice) to be reasonable. Although TrustUK is now defunct, the ICO still considers the following principles and age brackets to be reasonable:

'TrustUK approved web traders recognise children need to be treated differently from adults. They will not market their products in any way that exploits children, nor will they collect information from children under 12 without first obtaining the permission of a parent or guardian. They will not collect personal data about adults from children.'

The above standard is based on a definition of a child as a person aged 16 or under.

If a service provider (or indeed the ICO when investigating a reported breach) is not satisfied that a child is capable of making an informed decision in relation to the data they are giving, then the site will need to obtain parental consent. This parental consent will need to be verifiable, it will not usually be enough to ask children to confirm their parents have agreed by, for example, using a mouse-click.

The ICO also recommends that any site for children should display prominent links to a privacy policy and terms and conditions of use (preferably on every page), which should be in language that is easily understandable by a child. It is also recommended that service providers should provide links to online safety guides, available either on the operator's site or on third-party sites.

CONCLUSION

The Home Secretary, Jacqui Smith, has stated that while the recommendations contained in the Home

Office guidance are voluntary, the success of the initiative depends on a wide take-up within the industry. The government has continued to support a self-regulatory model for the internet industry. However, this can only be effective if and when service providers take appropriate steps to help address concerns about child protection arising from the development of new media.

The issue of children's privacy is an area of growing concern and one that UK law does not sufficiently protect at present. Indeed, this is an important agenda item for each of the UK's political parties and also for the European Commission, which currently has the Article 29 Working Party (on data protection) reviewing and reporting on this topic.

NOTES

The full Home Office guidance can be found at: <http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance>

The full Ofcom research report can be found at: www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/

While the Home Office guidance provides welcome guidance on the issue of child protection on the internet, it is not a panacea and a more comprehensive review is overdue.