

# Social Networking Websites – A Concatenation of Impersonation, Denigration, Sexual Aggressive Solicitation, Cyber-Bullying or Happy Slapping Videos

---

BRUCE L. MANN\*

## 1 Introduction

Hands-off legislation, toothless policy statements, unknowing parents, uncaring participants, and unwilling social network intermediaries (SNIs), have conspired to invite impersonation, denigration, sexual or aggressive solicitation, cyber-bullying, and happy slapping to the members of most social networking websites (SNWs). The situation is serious - serious because the user-generated content (UGC) that is displayed on-screen is destroying users' lives;<sup>1</sup> serious too, because of the volume of users at risk from posting their content, without intervention by the SNI.<sup>2</sup>

---

\*Ph.D. (Ed.Tech.), LL.M; Professor at Memorial University in Canada. Email: bmann@mun.ca

<sup>1</sup> Bergstrom, I. (2008). Facebook can ruin your life. And so can MySpace, Bebo... The Independent, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html>

<sup>2</sup> Tofalides, M. & Orakwusi, L. (December 2007). User generated content: privacy issues, Data Protection Law & Policy, (4), 12, <http://www.e-comlaw.com>

## 2 Social Networking Websites (SNWs)

In July 2006, Jonathan Abrams submitted an application to the US Patent and Trademark Office for ‘Friendster’, “a system, method and apparatus for connecting users in an online computer system based on their relationships within social networks”.<sup>3</sup> The patent application that had been filed 3 years earlier, explains:

“...a computer system collects descriptive data about various individuals and allows those individuals to indicate other individuals with whom they have a personal relationship. The descriptive data and the relationship data are integrated and processed to reveal the series of social relationships connecting any two individuals within a social network.”<sup>4</sup>

Today there is no shortage of social networking sites in which to share personal information. Whereas some sites are open to anyone, others are restricted by age.<sup>5</sup> In October 2007 Daksh Sharma published a list of online links to 350 social networking websites (SNWs), some generalist, others specialist.<sup>6</sup> Many encourage their users to express themselves by providing features for displaying their pictures, music and video, and for making personal annotations.<sup>7</sup> Most are not exclusively regional. The San Francisco-based ‘Bebo’ for example, recently became the most-visited SNW from within the UK.<sup>8</sup> ‘Faceparty’ is also a generalist SNW, though this one is based in the UK. ‘ProfileHeaven’ is a specialist site for teenagers based in Northeast England with a privacy policy that ‘logs and shares non-personally-identifiable information with third parties to provide more relevant services and advertisements to members. User IP addresses are recorded for security and monitoring purposes.’<sup>9</sup>

‘MyFaveShop’, a specialist UK-based SNW, resembles the California site ‘SecondLife’ without the avatars, where shoppers can design their own web store, choose products to display in their store, and invite their FaveShop friends to shop there. The terms in MyFaveShop are opt-in, stating ‘We will

---

<sup>3</sup> OUT-LAW News (July 2006). Friendster patents social networking, <http://www.out-law.com/default.aspx?page=7092>

<sup>4</sup> United States Patent & Trade Mark Office. June 16, 2003, Application No. 10/462,142, <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HIPTO&p=1&u=%2Fnethtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=7,069,308.PN.&OS=PN/7,069,308&RS=PN/7,069,308>

<sup>5</sup> Wikipedia (March 2008). List of notable social networking websites, [http://en.wikipedia.org/wiki/List\\_of\\_social\\_networking\\_websites](http://en.wikipedia.org/wiki/List_of_social_networking_websites)

<sup>6</sup> Sharma, D. (October 2007) Social networking God: 350+ social networking sites. Mashable: Social Networking News, <http://mashable.com/2007/10/23/social-networking-god/>

<sup>7</sup> comScore Inc. (September 2006). Leading user-generated content sites see exponential growth in UK Visitors During the Past Year, <http://www.comscore.com/press/release.asp?press=993>

<sup>8</sup> comScore Inc. (August 2007). Bebo becomes the most visited social networking site in the UK, <http://www.comscore.com/press/release.asp?press=1571>

<sup>9</sup> ProfileHeaven. (March 2008). Privacy policy, <http://www.profileheaven.com/index.php?do=privacy>

not share or sell your personal information, including your email address, with any third parties for marketing purposes without your permission.’<sup>10</sup>

‘OSOYOU’ is a London-based shopping and socialising SNW intended for women, that seems to behave a little like an eBay auction site, OSOYOU ‘uses personal data collected through their website for editorial and feedback purposes, marketing and promotion, statistical analysis of users’ behaviour, product development, delivering products and services, providing customer support, customizing and improving the content and layout of the Website, completing business transactions, administering individual accounts and meeting government regulatory requirements such as sales tax collection. Monitoring Data may be used for internal or external purposes such as researching and identifying market segments and needs.’<sup>11</sup>

‘iliketotallyloveit’ is a German-based SNW, wherein the members share product ideas. Its Terms and Conditions state that ‘this website uses Google Analytics, a web analytics service. Google Analytics uses “cookies”, to help the website analyze how users use the site.’<sup>12</sup> The PEACD 2002 was the first EC Directive in Europe to address the regulation of privacy-invading technologies such as cookies and spam<sup>13</sup> though they predated their use in SNW’s.

In the United States, the home of Facebook, the CAN-SPAM Act of 2003 has provided little protection against the use of cookies and SPAM, though here again the Act predated these imposters within a SNW. Facebook’s ‘Pulse Feature’ for example, is inadequately represented as ‘that friend who always knows the latest band, movie or book. Someone who knows what you like and only recommends the good stuff.’<sup>14</sup> What is unsaid here and should be clearly stated, is that these data may be used by companies to spam users with advertising. Used together in a SNW, cookies and spam technologies collect the preferences of a SNW user, and then send them advertisements of products and services that reflect their preferences - ideal for marketers perhaps, but a genuine nuisance for users who had joined-up just to ‘vent’.

Then in September 2007 Facebook Engineer Phil Fung announced that Facebook had expanded their ‘Search’ engine to make limited public search listings available to people who were not logged in to Facebook, ‘so that people could more easily find their friends on Facebook. Fung

<sup>10</sup> MyFaveShop. (March 2008). <http://www.myfaveshop.com/page/terms.html?sessionid=FC127E598AC98CE6963F40366AB7FEB7>

<sup>11</sup> Ohmigod Limited (March 2008). OSOYOU privacy policy, <http://www.osoyou.com/info/privacy-policy.publisha>

<sup>12</sup> iliketotallyloveit (March 2008). Terms and conditions, <http://www.iliketotallyloveit.com/about/en>

<sup>13</sup> Edwards, L. (2005). Articles 6-7 ECD; Privacy and Electronic Communications Directive 2002 – Cancelling the spam and cutting the cookies: Consumer privacy online and EU regulation, In Lilian Edwards (ed). The new legal framework for e-commerce in Europe. Chapter 2. UK: Hart Publishing.

<sup>14</sup> Facebook Pulse, <http://www.facebook.com/s.php?q=Pulse&init=q>

assured readers that Facebook was not exposing any new information, and you have complete control over your public search listing'.<sup>15</sup> His assurances were cold comfort in the light of the 'Facebook Principles' page:

Facebook may collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.<sup>16</sup>

It seems to be only a matter of limiting your profile to specific users,<sup>17</sup> consistent with the opt-out minimum (not an opt-in) in the CAN-SPAM Act – indeed, if in fact, users would read a lengthy document in a separate area of the SNW, which documented evidence shows they do not. The question is, – why don't the owners do it for them?

As of 28 March 2008, Facebook had logged 98 million registered users, and was open to people 13 years of age. Facebook's has what might be called a *carte blanche* version of Facebook's Terms of Use, which states

By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing.<sup>18</sup>

When the feature in Facebook called 'News Feeds' is on, every action a user takes on their site is displayed to 'their friends' the next time those friends login. So what's the problem? If these people are in fact, real friends, then news feeds and mini-feeds shouldn't be a worry. However these people are not real friends of the user. Some of the reasons why a user would associate with someone in a SNW<sup>19</sup>:

1. To be nice to people that they hardly know (like the folks in their classes)

---

<sup>15</sup> Fung, P. (2008). The Facebook Blog, <http://blog.facebook.com/blog.php?post=2963412130>

<sup>16</sup> Facebook Principles, retrieved 6 December 2007, <http://www.facebook.com/policy.php>

<sup>17</sup> Bierdorfer (January 2008). Staying private on Facebook, New York Times, <http://www.nytimes.com/2008/01/17/technology/personaltech/17askk-001.html?ei=5070&en=9b745acf32897efb&ex=1201237200&adxnml=1&emc=eta1&adxnmlx=1206288143-11dZ9eoG2siQ8rYFONN32Q&pagewanted=print>

<sup>18</sup> Facebook Terms of Use, retrieved 15 November 2007, <http://www.facebook.com/terms.php>

<sup>19</sup> Boyd, D. (September 2006). Facebook's privacy trainwreck: Exposure, invasion, and drama, *Apophenia* Blog. <http://www.danah.org/papers/FacebookAndPrivacy.html>

2. To keep face with people that they know but don't care for
3. As a way of acknowledging someone they think is interesting
4. To look cool because that link has status
5. To keep up with someone's posts, bulletins or other such bits
6. To circumnavigate the privacy problem that they were forced to use by their parents
7. As a substitute for bookmarking or 'favoriting'
8. It's easier to say yes than no when they're not sure

Facebook's privacy officer Chris Kelly admitted that "after deletion there may still be a record in Facebook's archives that a user made a particular wall post in a group on a particular date, but Facebook's servers no longer contain the information needed to connect that user ID (e.g., name, e-mail address, networks, etc.) to the person associated with that account.' Privacy may have been achieved as of mid- February 2008.<sup>20</sup>

Beacon, Facebook's advertising program uses its "News Feed" feature to share members' activities on third-party sites—went from an opt-out to an opt-in program within a matter of days due to a user uprising over privacy.

However, the monitoring of social networking sites for content that may interest employers in America, is now so routine that software is being put on the market that will automate the process.<sup>21</sup>

### 3 The Membership: *non compus mentus*

Users of social networking websites invariably ignore or forget to read important instructions and feedback presented in text and other visual displays regardless of their intended function, unless they are explicitly told to do so.<sup>22</sup> The consequence amounts to a clickwrap license that constitutes permission to release personal data to third parties;<sup>23</sup> a contract that effectively absolves those parties and the ISP (should they have had knowledge of the content) of any liability. This is all due to an act of omission on the user's part, *actus reus*. Barring medical or psychological reasons,

<sup>20</sup> Aspan, M. (March 2008). After stumbling Facebook finds a working eraser. NY: New York Times.

<sup>21</sup> Bergstrom, I. (2008). Facebook can ruin your life. And so can MySpace, Bebo... The Independent.

<sup>22</sup> In a recent example, see: Edwards, L. (2005). Articles 12-15 ECD: ISP liability – The problem of intermediary service provider liability, In Lilian Edwards (ed). The new legal framework for e-commerce in Europe. Hart Publishing, p.57. From the 1980's and 90's, see: Reinking, D. (1987). (Ed.), Reading and computers: Issues for theory and practice. NY: Columbia University. See also: Huff, C., & Finholt, T. (1994). Social issues in computing: Putting computing in its place. NY: McGraw Hill. For unintended effects, see: Wah, B.W. (Ed.). (2008). Wiley Encyclopedia of Computer Science and Engineering. Hoboken, NJ: John Wiley & Sons, Inc.

<sup>23</sup> Rambam, S. (2006). Privacy is dead - Get over it. The eighth ToorCon information security conference, Sept 30 - Aug 1, San Diego, Google video clip, <http://video.google.ca/videoplay?docid=383709537384528624&q=Steven+Rambam+Privacy+Is+Dead&total=1&start=0&num=10&so=0&type=search&plindex=0>

‘not thinking’, *non compus mentus*, can be no argument for breach of confidence. This begs the question – why do they do it? The answer seems to be, to provide their personal data with ‘context, context context’.<sup>24</sup> But at what expense? Clearly the time has come for the liability, or partial liability, to rest with the user and the intervening SNI. The position taken here therefore, is that any person who is intent on joining an SNW should be under a duty to take reasonable steps to protect their own personal data from being viewed, re-used, or sold, article 10 ECHR notwithstanding.

## 4 Privacies

Article 8 in the Charter of Fundamental Rights of the European Union recognises that (1) Everyone has the right to the protection of personal data, and that (2) everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.<sup>25</sup> Children are big users of SNWs. Article 24 of the Charter states that (2) a child’s best interests must be a primary consideration, and that (1) children shall have the right to such protection, and may express their views freely.<sup>26</sup>

## 5 Social Network Intermediary (SNI)

From the casual observer’s perspective, it should be the Social Network Intermediary (SNI) who is best placed to assist new members in managing their privacy. Unfortunately (for new members), the legislation absolves the SNI of any responsibility. ‘The law actually gives intermediaries an incentive to be as little involved as possible in what goes on their web servers.’<sup>27</sup> For example, Directive 2000/31/EC<sup>28</sup>

- (42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information

---

<sup>24</sup> Boyd, D. (September 2006). Facebook’s privacy trainwreck: Exposure, invasion, and drama, Apophenia Blog. <http://www.danah.org/papers/FacebookAndPrivacy.html>

<sup>25</sup> Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 2000/C 364/01, Article 8.

<sup>26</sup> Charter, Article 24.

<sup>27</sup> George, C. & Scerri, J. (2008). Web 2.0 and User-Generated Content: legal challenges in the new frontier, Journal of Information, Law and Technology, [http://go.warwick.ac.uk/jilt/2007\\_2/george\\_scerri](http://go.warwick.ac.uk/jilt/2007_2/george_scerri)

<sup>28</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services.

- society service provider has neither knowledge of nor control over the information which is transmitted or stored.
- (43) A service provider can benefit from the exemptions for “mere conduit” and for “caching” when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.
  - (44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of “mere conduit” or “caching” and as a result cannot benefit from the liability exemptions established for these activities.
  - (45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.
  - (46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States’ possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

This chain of thought lead to a “safe harbor” or total immunity for ISPs, and other on line intermediaries provided for in the US by the Communications Decency Act 1996,<sup>29</sup> which imposed broadcast-style content regulations on an open, and decentralized Internet.<sup>30</sup>

---

<sup>29</sup> Edwards, L. (2005). Article 12-15 ECD: ISP liability - The problem of Intermediate Service Provider liability. In Lilian Edwards (eds.). *The New Legal Framework for E-Commerce in Europe* (pp. 93-136) UK: Hart Publishing. Also published in: Waelde, C. & Edwards, L. (April 2005). *Online intermediaries and liability for copyright infringement*, A report to the WIPO Seminar on Copyright and Internet Intermediaries.

<sup>30</sup> Staff (March 2008). *Communications Decency Act*, Center for Democracy and Technology, <http://www.cdt.org/speech/cda/>

“One Internet service provider’s representative explained his concerns as follows: We provide free anonymous access to the net to sexual abuse survivors. We don’t even know who they are, *nor do we care*—a lot of them are hiding out...and to try and identify them would be an enormous breach of their trust, as they are depending on us for their anonymity... some of them are under the age of 18.... Sure, we could trace each and every one of them back to their providers, and find out who they are, but I’m not going to do it, and I’m perfectly willing to go to jail to protect their identities. My integrity is worth a whole hell of a lot more than any government law.”<sup>31</sup>

The Act was struck down in 1997 by the US Supreme Court as ‘unconstitutional’, and replaced by the Child Online Protection Act 1998 (COPA) which narrowed the range of material covered. COPA only limits commercial speech and only affects providers based within the United States. COPA requires all commercial distributors of “material harmful to minors” to restrict their sites from access by minors. “Material harmful to minors” was defined as material that by “contemporary community standards” was judged to appeal to the “prurient interest” and that showed sexual acts or nudity, a much broader standard than obscenity.

The European Union Council adopted the new Privacy and Electronic Communications Directive in 2002 that added new definitions and protections for “communications,” “calls,” “traffic data” and “location data”, to enhance the consumer’s right to privacy and control all kinds of data processing.<sup>32</sup>

Who should be liable for the risks of user-generated content in SNWs destroying users’ lives? It’s not likely to be the users themselves since most seem oblivious to the risks, or choose to ignore them. It’s not likely to be the ISPs because there is too much data to censor. It’s not likely to be the third parties who unabashedly use the data to send product information back the users, and worse. That leaves the program itself – the social networking website, which could be treated with more contextualised form of technical protection measure (TPM), that would, eventually, be circumvented by the users.

## 6 Privacy Policies in SNWs

An indication of recent media attention is evident in some SNWs and not others. Consider the differences between the Privacy Policies of ‘Friendster’, Bebo, and ‘gURL’ in Table 1.

---

<sup>31</sup> Bernstein, B. (November 1996) Beyond The Communications Decency Act: Constitutional Lessons Of The Internet, Cato Policy Analysis No. 262, <http://www.cato.org/pubs/pas/pa-262.html>

<sup>32</sup> Electronic Privacy Information Center and Privacy International (2003). Privacy and Human Rights: Overview, <http://www.privacyinternational.org/survey/phr2003/overview.htm#ftnref1>

**Table 1. Comparison of selected privacy factors in the Privacy Policies of three SNWs.**

	<b>gURL</b>	<b>Bebo</b>	<b>Friendster</b>
Policy updated -	December 2004.	November 2007	October 2007
Child warning -	Yes. 'gURL may be unsuitable under 13'.	Yes. 'Under 13 cannot register in Bebo'. Also they recommend 13-17 yrs not to make visible any personal info w/o their parents permission.	No statement in Friendster.
Private data Opt-In / Opt-Out -	Must opt-out to get privacy in Profile. No data visible to non-members, visitors.	Neither, however there is a clear recommendation from Bebo not to share personal contact info. Opt-in to make invisible to non-members.	Two profiles – one 'public', one Friendster. Must opt-out to get privacy. Must opt-out to make invisible to non-members, visitors. Some data visible during discussions.
3 <sup>rd</sup> -Party ads Opt-In / Opt-Out -	Must opt-out of special offers, affiliate emails. But can opt-in for 3 <sup>rd</sup> -Party Ads.	Default is to receive affiliate emails and 3 <sup>rd</sup> -Party Ads. Widget creation will also redirect web browser to 3 <sup>rd</sup> -Party sites.	Must opt-out of weekly emails. Default is to receive affiliate emails and 3 <sup>rd</sup> -Party Ads.
Internet awareness warning statement -	Yes	Yes	Yes.
No-SPAM notice	No.	Yes	Yes.

Bebo appears to be the safest to use. Children under 13 are not allowed to register, most options are opt-in, and the policy has been recently updated. Bebo and gURL recommend that members using their SNW can contact them in writing should they wish to refuse to receive direct marketing, in accordance with the Data Protection Act.<sup>33</sup> It is worth noting too, that Bebo representatives have been helping to draft a Good Practice Guide for Providers of Social Networking and User Interactive Services, at the Home Office in the UK. That said, some researchers have found that they had no difficulty setting-up profiles as 14 year olds in Bebo, and were subsequently exposed to pornographic material.<sup>34</sup> The Privacy Policies in Bebo may soon change

<sup>33</sup> Data Protection Act section 11.

toward a more commercialized service anyway, now that AOL has purchased Bebo.<sup>35</sup> This news coincides with that from Commission of European Committees on promoting data protection by Privacy Enhancing Technologies (PETS).<sup>36</sup> PET appears to be a technical protection measure that protects privacy, instead of preventing copyright infringement through downloading. Ostensibly privacy is protected through the reduction of personal data – a system of redacting private data. Some balance may be achievable.

## 7 Privacies Unmanaged

The general wording in Article 8 ECHR describes the right to respect private and family life, home and correspondence. However in the context of SNWs, section 2 in Article 8 cuts both ways. On the one hand public authorities cannot interfere unless there is a matter of national security, public safety, etc. On the other, non-interference leaves the innocent, albeit verbose user, at the mercy of those who would use the digital evidence against the user. Add to this, article 10 ECHR such that any curtailment of a user's right to say whatever is on their mind, including disclosure of their own private information, is to deny their right to freedom of expression.<sup>37</sup> Barbara Lacey's (2007) dissertation research of Internet harassment, accounted for several potential consequences of unmanaged privacy:<sup>38</sup>

- 'Denigration' is "dissing" someone online. Sending or posting cruel gossip or rumors about a person to damage his or her reputation of friendships.
- 'Cyber-stalking' is repeatedly sending messages that include threats of harm or are highly intimidating or engaging in other online activities that make a person afraid for his or her safety.
- 'Outing and Trickery' is sharing someone's secrets or embarrassing information online or tricking someone into revealing secrets or embarrassing information, which is then shared online.
- 'Flaming' is online "fighting" sending electronic messages using angry and vulgar language.
- 'Harassment' is repeatedly sending offensive, rude, and insulting messages.

---

<sup>34</sup> OUT-LAW News. (October 2006). Code of conduct proposed for social networking sites, <http://www.out-law.com/default.aspx?page=7298>

<sup>35</sup> OUT-LAW News. (March 2008). AOL buys Bebo in \$850m cash deal. <http://www.out-law.com/default.aspx?page=8936>

<sup>36</sup> Commission of European Committees. (March 2007). Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETS), 228. final.

<sup>37</sup> European Court of Human Rights (2003). Convention for the Protection of Human Rights and Fundamental Freedoms, Articles 8 and 10.

<sup>38</sup> Lacey, B. (May 2007). Social aggression: A study of Internet harassment. A dissertation for the Ed.D. in Educational and Policy Leadership, Hofstra University. 242 pages.

- ‘Impersonation’ is breaking into someone’s account, posing as that person and sending messages to make the person look bad, get that person in trouble or danger, or damage that person’s reputation or friendships.
- ‘Exclusion’ (Cyberostracism) is intentionally excluding someone from an online group, like a “buddy list” or a game.

## 8 Privacies Unmanaged: Sexual Solicitation

Despite the rise of social networking sites such as MySpace, fewer young people are being sexually solicited online than five years ago.<sup>39</sup> In two US telephone surveys of a random sample of 1501 youth aged 10 through 17 years who were regular Internet users, Wolak and associates compared the results of interviews in 2000 with those 5 years later in 2005. Table 2 shows a comparison of online victimization of youth in the United States over five years.

## 9 Privacy Unmanaged: Cyber-Bullying and Happy Slapping

‘Cyber-bullying’ in a SNW is often a harassing or humiliating text message directed from one member in a SNW to another. The object of the attack is often a child, preteen or teenager, who is being bullied, harassed, humiliated,

**Table 2. Comparison of online victimization of US youth over five years.**<sup>40</sup>

	2005	2000
Unwanted exposures to sexual material and online harassment	more	less
Receiving unwanted sexual solicitations.	less	more
Saw sexual material online they did not want to see	34%	25%
Exposure to unwanted sexual material occurred despite increased use of filtering, blocking, and monitoring software in households of youth Internet users.	55%	33%
Online harassment	9%	6%
Received unwanted sexual solicitations	13%	19%
Aggressive solicitations	4%	3%

<sup>39</sup> Kornblum, J. (October 2006). Children less likely to encounter online predators, USA TODAY, [http://www.usatoday.com/tech/news/internetprivacy/2006-08-08-kids-online-survey\\_x.htm](http://www.usatoday.com/tech/news/internetprivacy/2006-08-08-kids-online-survey_x.htm)

<sup>40</sup> Wolak, J., Mitchell, K., & Finkelhor, D. (2006). Online victimization of youth: Five years later. National Center for Missing & Exploited Children. Alexandria, VA, <http://www.unh.edu/ccrc/pdf/CV138.pdf>

threatened, embarrassed, or targeted in some way by another person (often another young person) through the use of Internet or mobile phone.<sup>41</sup> An extended form of cyber-bullying is a video clip in a SNW showing a person undressing in front of their web cam. The cyber-bully has enticed or threatened a peer to strip-off their clothes in front of a web cam, which later appears as video footage in a social networking website.<sup>42</sup>

'Happy slapping', is a video clip on a social networking website depicting one individual being swarmed by one or more others. Happy slapping videos depict several youths 'hitting a random person (on the bus, walking down the street) whilst recording the act with a video camera phone. The attackers are usually aggressive, poorly educated youths known in England as 'chavs' ('neds' in Scotland). Victims are usually boys around the same age as the attackers, but it's not unknown for victims to be older, or even women.'<sup>43</sup> In one clip a 27-year-old man can be seen shouting into the camera of his mobile phone, "this is YouTube material" as he urinates on a disabled 50-year-old woman who lay dying in the street. The woman later died in hospital.<sup>44</sup>

## 10 Second Life

Young adults are big users of Second Life as well. 'Second Life' is an interactive virtual reality playground that also fits the definition of a social networking website. Reporter Jason Farrell recently investigated child pornography in Second Life and discovered an area called 'Wonderland' that was used by child abusers where 'child-like' avatars were offering sex.<sup>45</sup> Since Second Life is a user-created virtual environment, player interactions are not saved on the client computer. Home Secretary Jacqui Smith, in an interview with Farrell, said that she would be publishing a consultation paper to outlaw virtual imagery of child abuse used in virtual on-line worlds. Since then, Second Life owner-managers Linden Lab, Inc. has installed a verification system in place, and is experimenting with tracking players' interactions.<sup>46</sup> Nevertheless British police are going undercover in Second Life to investigate depictions of adult-child sex to track down pedophiles.<sup>47</sup>

---

<sup>41</sup> Wikipedia (April 2008). Cyber-bullying, <http://en.wikipedia.org/wiki/Cyber-bullying>

<sup>42</sup> Stromdale, C. (2007). Regulating online content: A global view. *Computer and Telecommunications Law Review*, 13(6), pg. 7

<sup>43</sup> Urban Dictionary (April 2008). Happy Slapping, <http://www.urbandictionary.com/define.php?term=happy+slap>

<sup>44</sup> Staff. (September 2007). Man admits urinating on ill woman, BBC News, [http://news.bbc.co.uk/2/hi/uk\\_news/england/tees/7002627.stm](http://news.bbc.co.uk/2/hi/uk_news/england/tees/7002627.stm)

<sup>45</sup> Farrell, J. (October 2007). Perverts use virtual world for fantasies, SkyNews, <http://news.sky.com/skynews/article/0,,30100-1290719,00.html>

<sup>46</sup> Virtual World News (October 2007). Age Play Report Prompts UK Investigation of Second Life Pedophilia., <http://www.virtualworldsnews.com/2007/10/age-play-report.html>

<sup>47</sup> Reuters, E (October 2007). UK to investigate pedophilia in virtual worlds, Reuters/Second Life > Blog, <http://secondlife.reuters.com/stories/2007/10/30/uk-to-investigate-pedophilia-in-virtual-worlds/>

## 11 Conclusions

Two conclusions are evident from this critical assessment of the relationship between privacy and the growing popularity of SNWs. First, there must be someone assigned to interpret the risks of disclosing information about one's most private thoughts, interests opinions, work and health status on a SNW, particularly in times of psychological distress or personal tragedy. This 'someone' could be and should be, the SNI, a logical choice under the circumstances. Some SNWs serve a critical need, for those in psychological distress or medical tragedy. Consider the recently opened SNW in the UK that enables cancer sufferers to share their experiences and knowledge about dealing with cancer.<sup>48</sup> But even here, especially here, user-generated medical content is grist for anyone with an account and a buyer for these details. Worried advocates of SNWs emphasize the need for individual responsibility when using social networking sites. Developing responsible citizens occurs at the family level. Parents also need to be educated about how to teach their children to be responsible Internet citizens. The children in Lacey's study were asked for *their* advice on how to prevent or stop cyberspace aggression, which could include the importance of a parental role and control, confronting the bully, security online, raising awareness and education and password protection. A couple of responses were:<sup>49</sup>

"i think that teasing online could be stopped by parents having more control over their children and watching what their children do on the computer. Also i think that there should be some kind of block on websites like myspace and chat rooms for households with children or even teenagers." (5<sup>th</sup> grade girl).

"Restrict cell phone and internet access to all unless agreement is signed to not tease. Punishment is banning from internet." (8<sup>th</sup> grade boy).

The second conclusion is that, given the growing risk of identity theft and marketing CAN-SPAM to users of SNWs who appear to be oblivious to the risk of generating UGC, something must be done to alert users of the risks. Documented evidence of computer users ignoring privacy policies and terms of use, in a SNW is no excuse for acts of omission by the user. Scare tactics that work for habitual drunk drivers may be needed for habitual SNW users acting *actus reus*, such as television commercials showing users in jail and others who have lost their job as a result of the UGC they generated in a SNW.

---

<sup>48</sup> Staff (March 2008). Social networking site launches for cancer sufferers, Easier Media, [http://www.easier.com/view/Lifestyle/Health\\_and\\_Fitness/Health/article-169879.html](http://www.easier.com/view/Lifestyle/Health_and_Fitness/Health/article-169879.html) The 'What Now' SNW is located at <http://www.whatnow.org.uk/> and was launched by Cancerbackup, an information and support charity in the UK.

<sup>49</sup> Lacey, B. (May 2007). Social aggression: A study of Internet harassment. A dissertation for the Ed.D. in Educational and Policy Leadership, Hofstra University. 242 pages. Listed at [http://www.hofstra.edu/academics/Colleges/SOEAHS/FLPS/flps\\_dissertations.html](http://www.hofstra.edu/academics/Colleges/SOEAHS/FLPS/flps_dissertations.html)

## Bibliography

Aspan, M. (March 2008). After stumbling Facebook finds a working eraser. NY: New York Times.

Bergstrom, I. (2008). Facebook can ruin your life. And so can MySpace, Bebo... The Independent, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html>.

Bernstein, B. (November 1996). Beyond The Communications Decency Act: Constitutional Lessons Of The Internet, Cato Policy Analysis No. 262, <http://www.cato.org/pubs/pas/pa-262.html>.

Bierdorfer, (January 2008). Staying private on Facebook, New York Times, <http://www.nytimes.com/2008/01/17/technology/personaltech/17askk-001.html?ei=5070&en=9b745acf32897efb&ex=1201237200&adxnnl=1&emc=etal&adxnnlx=1206288143-1ldZ9eoG2siQ8rYFONN32Q&pagewanted=print>.

Boyd, D. (September 2006). Facebook's privacy trainwreck: Exposure, invasion, and drama, Apophenia Blog. <http://www.danah.org/papers/FacebookAndPrivacy.html>.

Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 2000/C 364/01, Article 8.

Commission of European Committees (March 2007). Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETS), 228. final.

comScore Inc (September 2006). Leading user-generated content sites see exponential growth in UK Visitors During the Past Year, <http://www.comscore.com/press/release.asp?press=993>.

comScore Inc (August 2007). Bebo becomes the most visited social networking site in the UK, <http://www.comscore.com/press/release.asp?press=1571>.

Data Protection Act section 11.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services.

Edwards, L. (2005). Articles 6–7 ECD; Privacy and Electronic Communications Directive 2002 – Canning the spam and cutting the cookies: Consumer privacy online and EU regulation, In Lilian Edwards (ed). The new legal framework for e-commerce in Europe. Chapter 2. UK: Hart Publishing.

Edwards, L. (2005). Articles 12–15 ECD: ISP liability – The problem of intermediary service provider liability, In Lilian Edwards (ed). The new legal framework for e-commerce in Europe. Hart Publishing, p.57.

Electronic Privacy Information Center and Privacy International (2003). Privacy and Human Rights: Overview, <http://www.privacyinternational.org/survey/phr2003/overview.htm#ftnref1>.

European Court of Human Rights (2003). Convention for the Protection of Human Rights and Fundamental Freedoms, Articles 8 and 10.

Facebook Pulse, <http://www.facebook.com/s.php?q=Pulse&init=q>.

Facebook Principles, retrieved 6 December 2007, <http://www.facebook.com/policy.php>.

Facebook Terms of Use, retrieved 15 November 2007, <http://www.facebook.com/terms.php>.

Farrell, J. (October 2007). Perverts use virtual world for fantasies, SkyNews, <http://news.sky.com/skynews/article/0,,30100-1290719,00.html>.

Fung, P. (2008). The Facebook Blog, <http://blog.facebook.com/blog.php?post=2963412130>.

George, C. & Scerri, J. (2008). Web 2.0 and User-Generated Content: legal challenges in the new frontier, *Journal of Information, Law and Technology*, [http://go.warwick.ac.uk/jilt/2007\\_2/george\\_scerri](http://go.warwick.ac.uk/jilt/2007_2/george_scerri).

Huff, C., & Finholt, T. (1994). *Social issues in computing: Putting computing in its place*. NY: McGraw Hill. For unintended effects, see: Wah, B.W. (Ed.). (2008). *Wiley Encyclopedia of Computer Science and Engineering*. Hoboken, NJ: John Wiley & Sons, Inc.

Kornblum, J. (October 2006). Children less likely to encounter online predators, USA TODAY, [http://www.usatoday.com/tech/news/internetprivacy/2006-08-08-kids-online-survey\\_x.htm](http://www.usatoday.com/tech/news/internetprivacy/2006-08-08-kids-online-survey_x.htm).

Lacey, B. (May 2007). *Social aggression: A study of Internet harassment*. A dissertation for the Ed.D. in Educational and Policy Leadership, Hofstra University. 242 pages. Listed at [http://www.hofstra.edu/academics/Colleges/SOEAHHS/FLPS/flps\\_dissertations.html](http://www.hofstra.edu/academics/Colleges/SOEAHHS/FLPS/flps_dissertations.html).

Ohmigod Limited (March 2008). OSOYOU privacy policy, <http://www.osoyou.com/info/privacy-policy.publisha>.

OUT-LAW News. (March 2008). AOL buys Bebo in \$850m cash deal. <http://www.out-law.com/default.aspx?page=8936>.

OUT-LAW News (July 2006). Friendster patents social networking, <http://www.out-law.com/default.aspx?page=7092>.

OUT-LAW News. (October 2006). Code of conduct proposed for social networking sites, <http://www.out-law.com/default.aspx?page=7298>.

iliketotallyloveit (March 2008). Terms and conditions, <http://www.iliketotallyloveit.com/about/en>.

MyFaveShop. (March 2008). <http://www.myfaveshop.com/page/terms.html?sessionid=FC127E598AC98CE6963F40366AB7FEB7>.

ProfileHeaven. (March 2008). Privacy policy, <http://www.profileheaven.com/index.php?do=privacy>.

Rambam, S. (2006). Privacy is dead - Get over it. The eighth ToorCon information security conference, Sept 30-Aug 1, San Diego, Google video clip, <http://video.google.ca/videoplay?docid=-383709537384528624&q=Steven+Rambam+Privacy+Is+Dead&total=1&start=0&num=10&so=0&type=search&plindex=0>.

- Reinking, D. (1987). (ED.), Reading and computers: Issues for theory and practice. NY: Columbia University.
- Reuters, E. (October 2007). UK to investigate pedophilia in virtual worlds, Reuters/SecondLife>Blog, <http://secondlife.reuters.com/stories/2007/10/30/uk-to-investigate-pedophilia-in-virtual-worlds/>.
- Sharma, D. (October 2007). Social networking God: 350+ social networking sites. Mashable: Social Networking News, <http://mashable.com/2007/10/23/social-networking-god/>.
- Staff, (March 2008). Communications Decency Act, Center for Democracy and Technology, <http://www.cdt.org/speech/cda/>.
- Staff (September 2007). Man admits urinating on ill woman, BBC News, [http://news.bbc.co.uk/2/hi/uk\\_news/england/tees/7002627.stm](http://news.bbc.co.uk/2/hi/uk_news/england/tees/7002627.stm).
- Staff (March 2008). Social networking site launches for cancer sufferers, Easier Media, [http://www.easier.com/view/Lifestyle/Health\\_and\\_Fitness/Health/article-169879.html](http://www.easier.com/view/Lifestyle/Health_and_Fitness/Health/article-169879.html) The 'What Now' SNW is located at <http://www.whatnow.org.uk/> and was launched by Cancerbackup, an information and support charity in the UK.
- Stromdale, C. (2007). Regulating online content: A global view. Computer and Telecommunications Law Review 13(6), pg. 7.
- Tofalides, M. & Orakwusi, L. (December 2007). User generated content: privacy issues, Data Protection Law & Policy, (4), 12, <http://www.e-comlaw.com>.
- Urban Dictionary (April 2008). Happy Slapping, <http://www.urbandictionary.com/define.php?term=happy+slap>.
- United States Patent & Trade Mark Office. June 16, 2003, Application No. 10/462,142, <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=7,069,308.PN.&OS=PN/7,069,308&RS=PN/7,069,308>.
- Virtual World News (October 2007). Age Play Report Prompts UK Investigation of Second Life Pedophilia,, <http://www.virtualworldsnews.com/2007/10/age-play-report.html>.
- Waelde, C. & Edwards, L. (April 2005). Online intermediaries and liability for copyright infringement, A report to the WIPO Seminar on Copyright and Internet Intermediaries.
- Wikipedia (March 2008). List of notable social networking websites, [http://en.wikipedia.org/wiki/List\\_of\\_social\\_networking\\_websites](http://en.wikipedia.org/wiki/List_of_social_networking_websites).
- Wikipedia (April 2008). Cyber-bullying, <http://en.wikipedia.org/wiki/Cyber-bullying>.
- Wolak, J., Mitchell, K., & Finkelhor, D. (2006). Online victimization of youth: Five years later. National Center for Missing & Exploited Children. Alexandria, VA, <http://www.unh.edu/ccrc/pdf/CV138.pdf>