Safe and effective SNS applications for young people.

Considerations in building social networking applications for under 19s.

A working paper prepared for

as part of the
Information & Signposting Project (ISP)

Find out more about ISP at:
http://isp.substance.coop

or from the Plings blog at:
http://blogs.plings.net

Written by Tim Davies, Practical Participation
http://www.timdavies.org.uk / tim@practicalparticipation.co.uk

Version 0.3
November 2008.

Introduction: designing ethics and safety in

Online social networks offer exciting opportunities for promoting information about positive activities to young people, deepening young people's engagement with positive activities, and getting young people involved in shaping positive activity provision and wider public services. Activity and information providers can use the pre-existing tools of Social Network Sites (SNS), as well as developing their own applications, to engage with and provide information and participation opportunities to young people.

However, it is crucial to recognise that opportunity and risk online (as in most contexts) go hand in hand[1] - and creating new ways of communicating with young people through social media and SNS can expose young people to new risks. This paper sets out to explore the particular considerations that those developing SNS applications and engagement approaches targeted at under 19s need to take into account in order to maximise opportunity and minimise risk[2]. It will address the tensions between ethics and efficacy of applications and interventions through Social Network Sites.

This paper will address:

1. **Understandings of young people -** identifying the key contexts of youth that mean specific attention must be paid to developing SNS applications targeted at young people;

2. **Understandings of social network sites** - identifying the features of SNS which give rise to both opportunities and risks;

3. **Identifying risks** - setting out a framework for thinking about the potential risks to young people from social network site applications;

4. **Identifying responses** - setting out a framework for responding to risks and designing ethical, pro-social SNS applications.
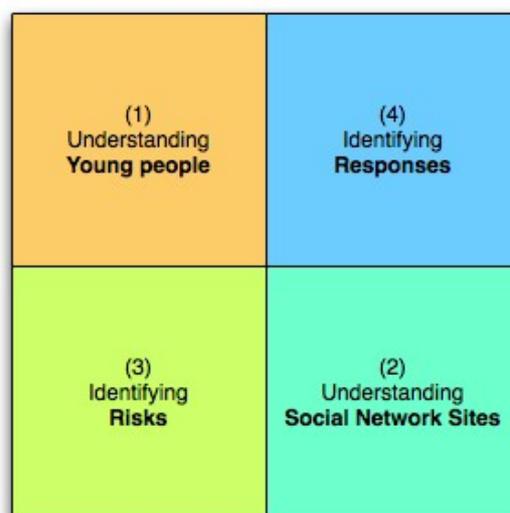
The paper also includes an Annexe providing a non-exhaustive list of potential risks to young people on SNS and possible responses. This is designed to inform the process of completing a risk assessment during the design of an SNS application.

---

1 Livingstone, UK Children Go Online, 2004.
2 Many of the ideas expressed in this paper may be relevant to applications and interventions targeting persons over 18. However, it is not within the scope of this paper to test that hypothesis. It should also be noted that this paper has it's focus on young people more than on children, and additional considerations may be necessary in developing SNS engagement approaches and applications targeted at younger children.

1) Why a different approach for young people?
Law, rights and young people's lived experience

Legal requirements, the Convention on the Rights of the Child, and an understanding of the lived experience of young people all suggest that we need to pay particular attention to the design of social network site (SNS) interventions targeted at under 19 year olds.

- **The law** recognises that young people require specific protections, and places specific obligations on authorities and institutions working with young people to prioritise the safety and well being of the young person.

- **The UN Convention on the Rights of the Child** expresses the specific rights of young people to be protected, to have special provision made for their developmental needs, and to participate in decisions that affect them.

- Most **young people experience their teenage years as a period of dynamic biological and social change** during which issues of personal identity and peer-group relationships can be of heightened importance and during which many young people are, by 'adult standards', less risk-averse.

- Young people growing up today will have **a unique set of experiences and understandings of themselves, of technology and of appropriate behaviours**, different from those of older generations. These experiences and understandings will affect how young people respond to online applications.

The law & policy frameworks
The law recognises young people as distinct from adults and due specific protections. Organisations that work with young people have responsibilities for their safety through child protection and through safeguarding. Child protection involves recognising and responding to signs of physical, sexual or emotional abuse. Safeguarding involves preventative and reactive action to keep young people safe from a wider range of harms. Legal and best practice requirements for those working with young people off-line apply equally online.

Alongside law and policy that refers specifically to young people, any SNS application development needs to take into account how universal laws specifically impact young people. For example, the Home Office Taskforce on Child Online Protection guidance on Social Networking Sites[3] notes of the Data Protection Act 1998 that *"there is a strong argument that service providers need to take extra care when processing information about children, to ensure compliance with the Act. For example, there is a requirement that processing has to be 'fair'. Fairness often involves explaining to individuals how, why and by whom information about them will be used. Service providers should ensure that the information they provide to children and young people is appropriate for the user age group – what might be within the reasonable expectations of, and fair to, adults, might not be apparent or fair to children."*

Our legal frameworks are also joined by extensive industry codes and agreements, many of which address issues specific to young people. For example, industry developed guidance about location aware mobile phone and internet services requires parental consent before location-aware services are activated for users aged under 16[4].

---

3 2008
4 http://mobilebroadbandgroup.com/social.htm (Accessed 3rd November 2008)

Rights: protection, provision, participation

Whilst there is a legal and moral obligation on agencies working with young people to ensure young people are protected from harm, responses to promote young people's safety cannot be based upon external protection alone, but need to engage young people actively as participants in their own protection.

The United Nations Convention on the Rights of the Child (UNCRC), ratified by the UK Government in 1989, provides a framework for considering Provision, Participation and Protection for young people. The provision, protection and participation articles of the convention act both to balance and to re-enforce each other.

The Convention, which should act as the foundation for any public provision for young people, includes a number of articles particularly relevant to positive activities information and participation online including[5]:
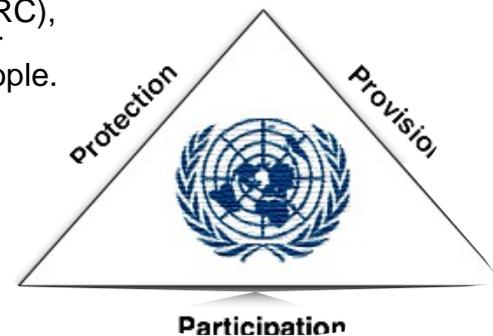
Provision rights
- **Article 31** - All children have a right to relax and play, and to join in a wide range of activities.
- **Article 29** - Education should develop each child's personality and talents to the full. It should encourage children to respect their parents, and their own and other cultures.
- **Article 17** - Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand, and should not promote materials that could harm children.

Protection rights
- **Article 34** - The government should protect children from sexual abuse.
- **Article 36** - Children should be protected from any activities that could harm their development.

Participation rights
- **Article 13** - Children have the right to get and share information, as long as the information is not damaging to them or to others.
- **Article 12** - Children have the right to say what they think should happen and to have their opinions taken into account when adults are making decisions that affect them.
- **Article 16 -** Children have a right to privacy.

Young people's development and lived experience

It is not enough to base the design of SNS applications and engagement approaches on an understanding of the law and young people's rights alone. It is crucial to seek an understanding of:

1. Socio-psychological factors related to young people's development that offer insights into young people's online interaction;

2. Young people's lived experience of engaging with online environments;

Both adults and young people are constantly undergoing processes of change, acquiring new skills and experiences and operating in changing social contexts. Whilst it is not possible to provide a universal description of the factors that define 'youth' we can draw out some general features that youth development literatures suggest are important in understanding how young people experience their teenage years:

---

5 Paraphrased from UNICEF Children's Rights and Responsibilities leaflet (Code: 32124)

- **Identity formation** - young people are often in the process of exploring their own identity. Identity exploration can involve 'trying out' different aspects or expressions of identity to assess how they fit, or how peers respond. With the growth of social network sites much of young people's identity exploration and formation can play out in public or semi-public online spaces.

- **Importance of peers** - a drive for social interaction is a key part of young people's development, with friends, peer groups and relationships with a significant other gaining in importance and displacing many other relationships (family, teacher, youth worker) for young people. However, some research suggests that during early adolescence (11 - 12) young people may experience a dip in their capacity to process social information, gaining in this capacity gradually until around age 16[6].

- **Attitudes to risk** – for many young people their teenage years involve experimentation with risk - seeking to identify limits by testing the boundaries. Risk taking is important for young people's development[7].

Academic understandings of factors impacting upon many young people's experience of online environments must be complemented by working with young people themselves to identify how they understand the online realm. As each age cohort is growing up with new technologies and in new online environments we need to constantly refresh our understanding of young people's experience. It has been argued that new media spaces and network technologies are reconfiguring the way young people understand concepts such as privacy, and even concepts of friendship and concepts of self.

The way young people understand the interaction design of an SNS application or engagement approach will affect how they respond to it – and will affect whether the behaviours that emerge promote, or act against, the safety of individuals and groups.

---

6 Byron 2008, § 2.38
7 Byron, 2008 § 2.29

2) Understanding SNS: the social graph & information sharing

Social Network Sites (SNS) allow users to create public or semi-public profiles, publish content and articulate a list of 'friend' connections with other members of the site.

By recording information about their users, SNS build up a 'social graph' for each individual (a digital representation of an individual user's connections to other users, content, groups, applications and demographics). This 'social graph' can be used to customise a user's experience of an SNS - providing individuals with feeds of information about their friends, their interests or their demographic.

Many SNS have opened up information from their social graphs to third-party application developers who can add features to the SNS, or use data from the SNS to provide extra features to SNS users.

The social features of SNS also allows for information or applications to spread rapidly through individuals networks - passing from 'friend' to 'friend' via recommendation, invitations, status updates or action feed updates.

Using applications to promote positive activities

Whilst the inbuilt features of most SNS (profiles, groups, events, media sharing) can be used to promote positive activities and invite input and feedback from young people, developing custom applications offers even more possibilities.

Applications can use the profile data, social graph and interactive features of SNS to develop new mechanisms for promoting and sharing positive activity information, and for engaging young people in influencing future provision.

Applications can adopt one or more of six key approaches for engaging users and promoting positive activities:

• Providing **profile extras** offering features, design elements or media that a user can add to their profile to display an interest, affiliation or aspect of identity.

• Sending **alerts** to the user who has added the application. Via alerts on screen or messages to a user's on-site mailbox or e-mail address.

• Encouraging users to **message friends** with enhanced messages (e.g. super-poke), to invite them to add an application, with information provided by the application.

• Updating **action feeds** to alert friends of an application user to how they have recently used that application (e.g. displaying to my friends the message 'Tim has signed up to take part in Arts Unlimited this half term').

• Providing **transactional features** such as the ability to book activities, provide feedback and rate an activity, collaborate with others or share media.

• **Viral marketing** - providing engaging content that users wish to share, or developing games that spread amongst friendship networks. Positive activity messaging may be core to these applications, or woven in once an application spreads.

SNS differ in the exact features applications can exploit (for example, some sites do not allow applications to access a user's e-mail address or send e-mail messages) and the permissions and control over applications they offer a user.

Formerly it has been necessary to write applications on a network-by-network basis (applications for one network would not work on another). However, with the emergence of the 'Open Social' protocol it is now possible to write a single application that can be implemented across multiple platforms, plugging into the different social graphs available on different social network sites. However, two of the main social network sites (Facebook, Bebo) are not currently supporting 'Open Social', instead using similar proprietary APIs.

Ethics and efficacy
Developers of applications to promote positive activities to young people may encounter a tension between making their applications safe and ethically sound, and designing those applications to make the most effective use (in terms of reach and user numbers) of the 'viral marketing' properties of social network sites.

It is important, however, to also recognise that the metrics to measure success in the development of pro-social SNS applications may be different from those metrics used for assessing commercially successful applications. In the case of applications to promote positive activities, the goal (and metric of success) is connected to behaviour change with respect to young people's participation in positive activities, not necessarily directly to the number of people using an application or it's rate of growth.

3) Risks[8]: negative SNS scenarios

The Byron report[9], following the EU Children Go Online project[10] categorises risks to young people online into Content, Conduct and Contact. Whilst EU Kids Go Online includes commercialism as a cross-cutting theme, we shall consider it as an independent category.

As we are concerned in this paper with promoting pro-social and ethical conduct as well as safeguarding young people, we will also include two additional categories: Confusion (applications failing to ensure young people fully understand the consequences of their actions in using them) and Exclusion (application design that fails to take into account issues of equality and diversity).

Content
Young people may encounter harmful, offensive or inappropriate content online.

In the case of promoting positive activities through SNS there are particular concerns about inaccurate content which could, for example, lead young people to try to access activities which are not taking place, or to become stranded away from home because transport information was not included or correct. There are also risks attached to 'User Generated Content' (UGC). An application may risk facilitating the sharing of inappropriate content (e.g. sexualised photos, offensive text or violent videos).

Conduct
Young people may be the perpetrators or victims of inappropriate or illegal conduct online.

As most SNS have age limits on who can join (generally determined as a result of US legislation which prohibits website registrations by under 13s) there is a risk that providing and promoting added value services within SNS may encourage under-age use of a site against it's terms of service.

Information and media about the positive activities an individual is involved in may facilitate cyber bullying.

Some young people may engage in cracking (hacking) to send unauthorised messages or using someone else's password to change that person's profile or application settings. As such, transactional applications may be open to abuse.

Young people may become victims of **crime** if information shared through SNS can be used for identity theft.

Contact
Grooming and contact from predatory adults often represents the most serious concerns of those exploring online safety. The Home Office Taskforce on Child Internet Safety's 'Good practice guidance for providers of social networking ... services 2008' highlights a range of techniques that abusers have used to make contact and establish relationships with young people. These include "gathering person details, such as age, name, address, mobile number, name of school and photographs", "offering cheap tickets to sporting or music events", "offering virtual gifts, such as rewards, passwords and gaming cheats", "asking children and young people to meet off-line" and "using school or hobby sites to gather information about a child's interests, likes and dislikes". The Taskforce also note "Having made contact with a child or young person, abusers may also use that young person as a

---

8   This section draws upon a comprehensive literature review on opportunity and risk of Social Network Sites created as part of the Youth Work and Social Networking Project (NYA, 2008). A full list of references is available in the Interim Report of that project which can be found at http://blogs.nya.org.uk/ywsn/
9   Livingstone et. al. 2008
10 Hasebrink, Livingstone et. al. 2007

means to contact and get to know their friends by using the links to their 'friends' in user profiles."

Whilst, according to US research[11], few online sexual solicitations result in aggressive attempts to meet, this remains a real and serious risk.

Positive activity oriented applications present particular challenges - given that facilitating the sharing of activity information not only enables a potential abuser to become aware of the particular interests of a young person - but activity information may also link a young person to a particular location at a particular time.

It is worth noting, however, that a significant proportion of internet facilitated abuse of young people results from young people actively *seeking out* conversations and contact with strangers. Byron, drawing on SAFT 2006, found that "there is some evidence that those dissatisfied with their offline lives are at increased risk of physical and psychological abuse related to meeting strangers online". It is reasonable to at least consider the hypothesis that promoting positive, developmentally appropriate, activities may support such vulnerable young people in gaining greater self confidence and reducing their risk of online victimisation.

Confusion
SNS and applications can have very confusing privacy settings[12]. It is not always clear to users (young and old alike) who a particular piece of content will or won't be shared with.

During adolescent development most young people may be less capable than most adults would be of critically assessing the impact of a particular action on a SNS. They may be inclined by the importance during adolescence of social feedback and validation to be more open with information than they would if they were supported to reflect upon who they are sharing information with.

Young people may also not fully appreciate the potential permanence of content shared through SNS.

The wider than expected sharing of information, or media intended for a limited and temporary audience becoming permanently available will not necessarily lead to harms for young people - but, as the Home Office Taskforce observations on the Data Protection Act point out[13], applications may have been operating without informed consent.

Exclusion
Different SNS have different user bases - and certain demographics within a local population may be found in certain networks. For example, whilst Facebook, MySpace and Bebo are the most popular networks in England, Hi5 has a significant BME membership, and Orkut can be the predominant network amongst young people with Asian heritage or from Latin America.

Using one SNS over another, or designing Open Social applications in ways which prioritise certain networks, may lead to a negative demographic bias in the young people who can be engaged.

SNS also have age limitations and terms of use which may exclude certain groups of young people.

---

11 Wolak J, Finkelhor D, Mitchell K J, Ybarra M L (2008) *Online "Predators" and Their Victims - Myths, Realities, and Implications for Prevention and Treatment* (American Psychologist, The American Psychological Association)
12 http://www.zephoria.org/thoughts/archives/2008/10/22/putting_privacy.html Accessed 3rd November 2008
13 See §1

4) Responses: ethical principles, risk assessment and safety built in

Any SNS application promoting positive activities and targeted at young people should:

• Adopt **ethical guiding principles** that will inform it's design and implementation;

• Work through a **risk assessment** to ensure that the application and it's implementation does not expose young people to unacceptable risks;

• Consider how it can contribute to make SNS spaces safer as a whole by having **safety built in** and explicitly encouraging positive SNS behaviours;

Ethical principles
Applications designed in the social sector may wish to adopt some of the effective marketing practices from commercial SNS applications. However, it is crucial that socially responsible applications are designed with the UNCRC and an understanding of positive youth development in mind.

1. Applications to promote positive activities to young people should have at their core a vision of supporting young people's positive personal and social development. Where the interests or wishes of young people come into conflict with those of activity providers or promoters, **the interests and wishes of young people should be paramount.**

2. Applications should **ensure they gain <u>informed</u> consent** before using the personal information about young people and their networks which can be accessed through social network sites. This may involve:
    • Providing terms and conditions in clear and easy to read language;
    • Summarising terms and conditions or presenting them in audio and video;
    • Designing the interfaces where young people are invited to confirm their acceptance of T&Cs to ascertain levels of comprehension[14] / only allow young people to confirm agreement if it is clear they have understood the implications of agreeing;
    • Regularly reminding young people of the T&Cs they have agreed to;
    • Allowing consent to be easily withdrawn at any time;

3. Applications should **promote responsible online behaviours**. For example, applications should *not* provide incentives for users to send unsolicited messages to their networks, but *should* encourage users to report any concerns about abusive or unsuitable content to the network or application owner.

4. Applications often aim to become 'viral'. However, applications may wish to explore alternative models of **'organic' or 'rhizomatic' growth**. See http://is.gd/toG

5. Applications **should not sell young people's information** or **target young people with commercial or age-inappropriate advertising**. Applications should respect young people's privacy and should only reveal aggregate information in analytics when it can be suitably anonymised.

Risk assessment framework
Application developers/providers need to carry out a full risk assessment of their applications and the ways in which they will be implemented.

The final section of this report draws on the risks identified in §3 and provides an example of risk assessment and appropriate responses.

---

14 E.g. Inviting a young person to type our a phrase from the T&Cs to confirm agreement.

It is important to understand that some risks, such as publicly revealing the location of a young person at a given time, should always be avoided - whereas other risks, such as revealing location data to a limited group of friends, may or may not be acceptable risks, depending on context and the attitudes to risk of the activity/application providers involved.

Safety built in
Even if all the applications designed to promote positive activities are designed with safety, ethics and social responsibility in mind - there will remain many SNS applications which model bad practice and potentially increase the risks to young people.

Banning or blocking access to these applications is not a viable option - and so young people need to develop the critical skills and capacities to navigate the risks these other applications may pose.

Socially responsible applications may be able to contribute to making SNS safer as a whole by:

- Modelling good practice and encouraging young people to be conscious and critical of the bad practice of other applications;

- Highlighting the safety features of SNS, such as privacy settings;

- Offering 'Report Abuse' features (including the CEOP report abuse button) and explaining that these can be used to report any abuse on the SNS, not only abuse that involves this specific application;

- Helping young people to visualise the impact of certain actions on SNS. For example, explaining that accepting 'Show this in my action feed' will display a message to up to N hundred people.

Annexe 1: Risk assessment framework

The following is a non-exhaustive list of possible risks to young people originating from social network applications along with a sketch of possible responses. Many of these risks also apply to SNS engagement approaches using the inbuilt tools of SNS.

The purpose of this matrix is not to act as a definitive guide to all possible risks and responses, but to provide an wide ranging overview of some of the potential issues to consider to stimulate discussion and reflection.

Cat.	Risk	Examples	Possible Responses
Content	Inaccurate content	Young people access or share inaccurate information about positive activities. May lead to risky real world activity (e.g. turning up somewhere that is closed / being stranded without travel etc.)	Rigourous procedures for ensuring data standards. Encourage young people to confirm activities before travelling. Provide ways to report wrong data & ensure rapid response. Provide emergency contact details with activity information.
		User generated content/ discussion around an activity may provide incorrect information.	Regular moderation of user generated content.
		The application uses semantic web techniques to combine information, but ends up wrongly matching up data and media.	Allow application provider to set a tolerance level for errors. Provide ways to report wrong data. Provide tools for updating incorrectly matched data.
	Inappropriate User Generated Content (UGC)	Inappropriate photos, videos or text are shared about/attached to an activity. E.g. sexually provocative photos, content containing offensive swearing.	Active moderation of user generated content. Clear guidelines about appropriate content. Send message to anyone whose content is removed explaining the reasons.
		Users share content without having the consent of individuals featured in the content.	Request users confirm they have consent before uploading and provide clear materials to explain what getting consent means. Provide option for anyone to request content is removed. Rapid moderation to respond to content removal requests.

Cat.	Risk	Examples	Possible Responses
	Re-use of User Generated Content (UGC)	User Generated Content is taken and re-used in a different context without the consent of the young people concerned.	Ensure content is clearly licensed / encourage users to consider the licence they place content under. Provide young people with details of how they can request that content is removed from third-party services. Provide clear guidance to partners accessing UGC about complying with the licence under which UGC is shared.
	SPAM	An unauthorised party gains access to the application and uses it to send unsolicited messages to application users. These messages may appear to come from a trusted organisation.	Make sure good security practices are always in place. Ensure processes are in place that allow you to retract unauthorised messages. Take law enforcement action where necessary and ensure applications provide audit trails to support law enforcement.
		The application can be abused to circulate unverified information.	Actively monitor for abuse and having procedures in place to suspect or patch the application where relevant.
		Data can be harvested from the application which can be used to target SPAM to young people.	Provide guidance to young people on keeping their contact details private. Monitor for this form of abuse.
Con duct	**Cyber bullying**	The application facilitates the flow of information used in bullying.	Work with young people to identify potential cyber-bullying risks and to limit data sharing which may fuel bullying. Provide young people with details of how they can remove content / request that content is removed and act rapidly to remove content.
		The application is used as a tool for bullying.	Consider ways applications can be adapted to prevent bulling activity. Provide clear mechanisms for young people to report abuse and ensure there is a rapid response to such reports. Provide guidance and signposting to support for victims of bullying.
	Cracking	A young person's account is accessed by an unauthorised party and false data shared.	Ensure it is possible to delete and remove any content posted through the application. Provide guidance on not sharing passwords and keeping accounts secure. Consider preventing 'personality changes' by users of an application.

Cat.	Risk	Examples	Possible Responses
Cont act	**Grooming**	Information provided through the application can be used by predatory adults in grooming.	Ensure young people are encouraged to be critical about who they share information with. Actively check young people's privacy settings. Support young people to visualise the scope of their shared information. Provide guidance that explains how predators could use the shared information. Actively monitor for contact that gives rise to concern.
		The application can be used by predatory adults in grooming.	Ensure there are clear report abuse features linked to the CEOP Report Abuse service. Provide safety guidance for young people – and encourage peers to be vigilant. User automated services for highlighting potential abuse of the application/service. Ensure all contact through the application is logged for use in law enforcement.
		The application can be impersonated by predatory adults to facilitate grooming.	Provide ways for users to ensure they are using the official application. Take immediate action to remove any applications attempting to impersonate the official application.
	Inappropriate contact between young people and staff	Staff use SNS/applications in ways that blur professional boundaries.	Provide staff with clear guidance about appropriate use of SNS/applications. Monitor staff use of SNS/applications.
	Intrusion on young people's space	The use of SNS is seen by young people as an inappropriate encroachment by adults on young people's own space.	Co-design services with young people. Ensure all applications and engagement respects principles of voluntary engagement.
		Information from applications is used as part of a 'surveillance state' and is linked with other datasets such as the child protection register.	Recognise that young people engage in identity play on SNS and information portrayed through sites may not be authoritative. Ensure terms and conditions and data licensing protects young people's privacy.
	Custody issues / particular issues relating to young people at risk	The location of a young person subject to a custody battle, or specifically at risk is revealed to family or other parties.	Work with child protection services to ensure specific guidance is being provided to children at risk. Ensure young people have control over how their information is shared and can understand the implications of information sharing.

Cat.	Risk	Examples	Possible Responses
	Mobbing	Using location data large groups of young people gather and overwhelm services.	Exercise caution when designing location aware services. Actively listen and monitor emerging discussions through SNS/applications and prepare online and offline responses where relevant. Support the reconfiguration of public services to have greater flexibility.
Commercial	**Revealing Information to SNS provider**	SNS providers use data to target advertising.	?
		SNS providers sell/release data to third parties	Ensure guidance is provided to young people on opting out from agreements which may allow their data to be shared.
		SNS providers assert ownership over UGC.	Carefully review all terms and conditions. Considering encouraging the hosting of UGC outside of an SNS where the license terms are acceptable to the parties involved.
	Revealing information to other applications	Information is revealed to another application which uses this data in unsafe ways.	Ensure applications only exchange data with other trusted applications. Provide clear guidance for young people on how to take care in sharing their data.
	Data mining	Data gathered by the application is mined by third parties.	Ensure data cannot be accessed by third parties and license terms do not permit unsuitable data-mining.
Confusion	**Over-sharing**	Young people share data they did not intend to share.	Design application interaction to encourage young people to reflect before sharing data ('speed bumps' to data sharing). Allowing information to be easily removed.
	Permanent information	Information shared is permanently available and may impact on young people's future education, career or relationship prospects.	Design application interaction to encourage young people to reflect before sharing data ('speed bumps' to data sharing). Allowing information to be easily removed. Consider introducing an 'information entropy' which leads to information expiring after a set period of time. Consider using meta data tags to ensure information is not archived by third-party services.
Exclusion	**Age restrictions**	The 'pull' of an application encourages young people who are below the allowed age for a particular SNS to attempt to use it.	Ensure information services which provide for under 13s/14s can also be accessed outside of social network sites. Provide clear guidance about the age limitations on the use of applications, and do not provide information within applications for age groups who should not be using the application.

Cat.	Risk	Examples	Possible Responses
	Platform bias	Applications are designed for specific platforms (e.g. Facebook) and young people using other platforms cannot access the added value features that the application offers.	Ensure services can also be accessed outside of social network sites. Consider developing using the Open Social feature-set in order to maximise application compatibility. Work with young people from within a local area to identify actively used SNS and ensure that applications are available and promoted within these sites. Consider developing applications to operate successfully at different 'critical mass' levels depending on the site they are operating on.

Next Steps

This is a draft paper. Comments are invited to tim@practicalparticipation.co.uk or through online discussions.

Please notify tim@practicalparticipation.co.uk of any wider online discussions of this paper, or include a track-back to the blog post inviting feedback at http://www.timdavies.org.uk