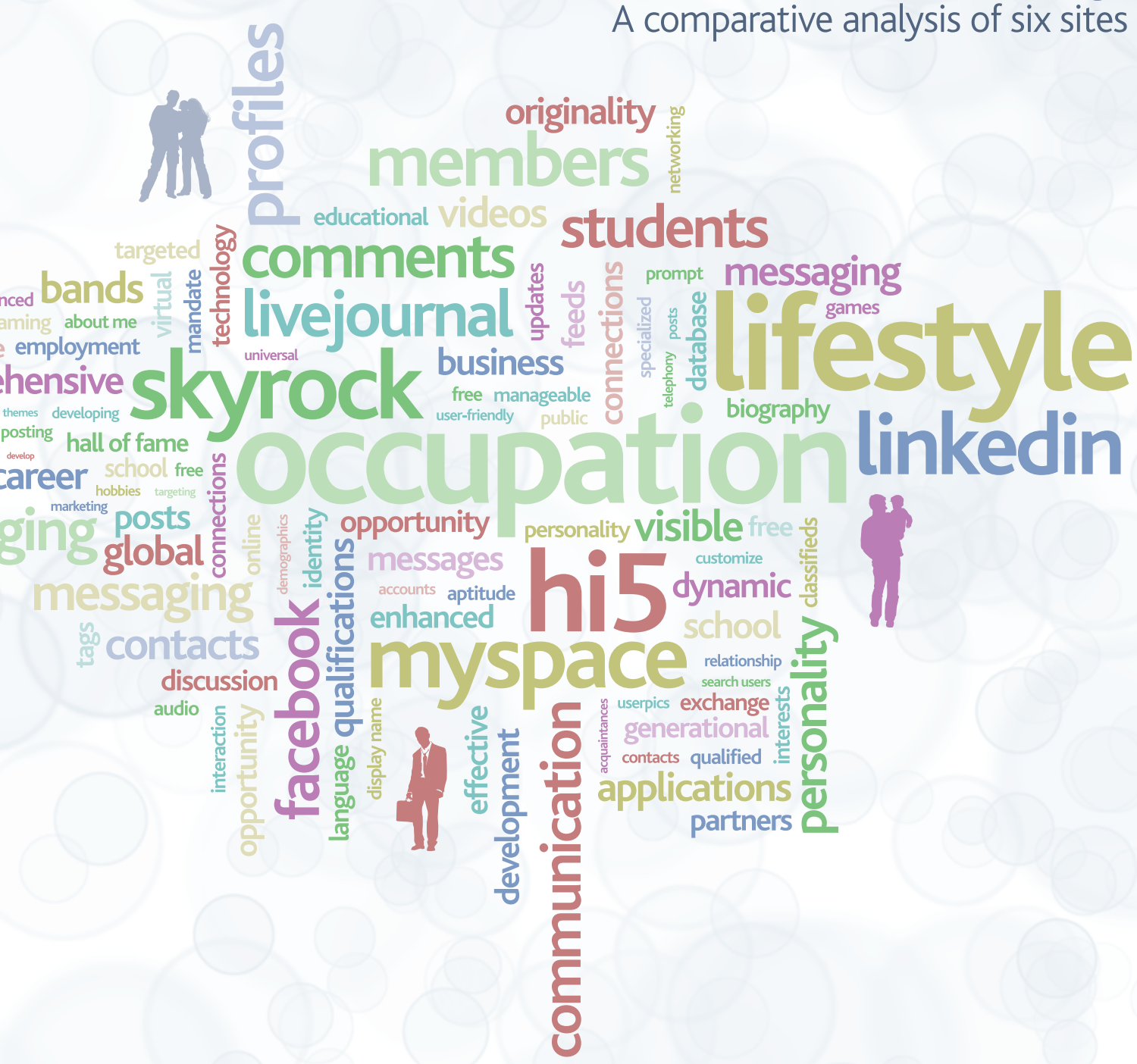
Social Network Site Privacy

A comparative analysis of six sites



The Office of The Privacy Commissioner of Canada
www.priv.gc.ca | February 2009
Researched by: Jennifer Barrigar

This report was prepared for the Office of the Privacy Commissioner by Jennifer Barrigar, a consultant and researcher with experience in both privacy law and developments in internet technology. It was originally commissioned in late 2008, and a final report was delivered to the Office in February 2009.

Social networks frequently make amendments or additions to their privacy policies and protections. As a result, some of the observations made in this report may appear outdated or even incorrect. This is certainly the case with Facebook, one social network that has undertaken successive rounds of privacy amendments in 2009.

This is not the case with many of the other social networking sites identified by Ms. Barrigar. They are among the most popular sites with Canadians, but are largely developed and headquartered outside Canada. As a result, they offer significantly different levels of privacy protection for their users. This report identifies areas where these sites need to improve their policies and take steps to effectively protect the personal information of their users.

Colin McKay
Director of Research, Education and Outreach

Office of the Privacy Commissioner of Canada
Toll-free: 1-800-282-1376 | Phone: 613-995-8210 | Fax: 613-947-6850 | TTY: 613-992-9190
112 Kent Street | Place de Ville | Tower B, 3rd Floor | Ottawa, Ontario | K1A 1H3
Catalogue no. IP54-28/2009 | ISBN 978-1-100-50025-6

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper is intended to provide a comparative privacy analysis of social network privacy in Canada. It attempts to do so first by identifying six (6) social network sites currently popular and available in Canada. Each of these sites is examined individually, looking at the stated mandate, the financial underpinnings (where available), its history and the user demographics.

Privacy is, of course, an incredibly broad concept. In order to limit what could otherwise have been a virtually limitless analysis, the paper sets out ten (10) categories of activity common to social network sites, and proceeds to canvas the policy choices of each of the selected sites for each category. While this will not, of course, cover all the privacy implications endemic to each site, it does provide a platform for understanding privacy issues and the policy choices sites have made regarding those particular issues across the board.

Recognizing the seeming dissonance between the expressed desire for privacy and the lack of user uptake of existing privacy tools, the paper attempts to bridge that gap. Drawing on the theory of privacy as contextual integrity, the project seeks to find ways both to facilitate deeper user understanding of the context in which they operate on a social network site as well as ways to make privacy controls and tools meaningful for users and more effective in allowing users to make the privacy choices that matter to them.

This analysis indicates that in order to further privacy on SNS, it will be necessary to provide users with the appropriate tools to allow them to understand the context in which their information exists and to enable them to select appropriate levels of information sharing and enact appropriate protections upon their personal information to enforce those self-determined levels and accordingly produce a SNS privacy that is meaningful and intuitive for users.

Building upon this user-centered understanding of privacy, then, the paper concludes by providing a comparative analysis of the sites under each of the selected categories and putting forward recommendations to facilitate the desired user comprehension and privacy control and by so doing create opportunities for improved privacy protection.

A: SCOPE

This paper will provide a comparative study of six (6) selected social network sites from a privacy perspective.

For the purposes of this analysis, I apply boyd & Ellison's definition, namely that social network sites are "web-based services that allow individuals to (a) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[1] Each of the selected sites meets these criteria, although they do not all organize their services in the same fashion.

I also rely on boyd & Ellison for their articulation of the distinction between "social network site" and "social networking sites." Although both appear in the literature seemingly interchangeably, the language of this paper will be that of "social network site". This decision is not merely stylistic – rather in choosing to emphasize the network as an object rather than the action of networking, I hope to underscore that the primary action of these sites is not (new) relationship initiation but rather the articulation and making visible of social networks[2] both as they exist and as they develop.

The 6 sites that will be assessed are (in alphabetical order):
1. Facebook (http://www.facebook.com)
2. Hi5 (http://hi5.com)
3. LinkedIn (http://www.linkedin.com)
4. LiveJournal (http://www.livejournal.com)
5. MySpace (http://www.myspace.com)
6. Skyrock (http://www.Skyrock.com)

These sites were selected based on popularity, but also to facilitate the efficacy of the final product by providing an appropriate breadth and diversity to the analysis. Four (4) of the 6 sites appear on the list of Canada's Top 100 web sites as of 31 January 2009[3], while the other two (2) are also well known sites that have appeared on that list in the recent past. The SNS' were also selected to reflect a variety of interests – journaling, professional networking, and music platforms – and user-bases.

Of course, each SNS is its own platform, offering a nearly unlimited variety of options for interaction with the site and other users. To attempt to review every aspect of every site is beyond the scope of this analysis. Accordingly, this paper aim to examine the privacy-specific characteristics of each SNS under the following headings:
- Registration information;
- Real identities v pseudonyms;
- Privacy controls;
- Photo tagging;
- Accessibility of member information to others;
- Advertising;
- Data retention;
- Account deletion;
- 3d party applications; and
- Collection of non-user personal information.

Having reviewed each selected SNS under these categories, the report will then attempt to identify where sites have made particularly strong or weak choices with regard to privacy, and to identify opportunities for improved privacy protection on SNS.

A Note on Age Limits

Originally, the categories also included an assessment of site policies on age limitations and policies. However, on 10 February 2009 the EU announced an agreement with 17 SNS to "improve the safety of under 18s who use social networking sites."[4] Given that this Agreement is likely to have an impact on site policies regarding age for the sites who are signatories (of the 6 sites assessed in this paper, three of them – Facebook, MySpace and Skyrock – are signatories of the agreement) as well as having potential impact on those who are not direct signatories, it was determined that analysis of the pre-Agreement policies would not be productive for the project of going forward with SNS privacy.

Those who wish to pursue this area are encouraged to consult the EU Agreement[5] itself, as well as looking to previous work on issues for youths and children in online environments[6] and the difficulties of age verification.[7]

B: CONTEXTUALIZING THE INQUIRY

Any review of the way(s) in which society intersects with SNS and the information on SNS will quickly discover that the presumption that information on SNS is public is so frequent as to seem ubiquitous. Certainly at present is seems that "the personal information users are revealing even on sites with access control and managed search capabilities effectively becomes public data."[8] It is also true, however, that while studies may not show SNS users using the existing privacy controls in the way(s) or to the extent that might be expected, they do show that users have "strong concerns about privacy of their public information."[9] In order to reconcile this seeming inconsistency, Grimmelmann suggests that we must focus our inquiry on the user herself – "the smaller we can make the gap between the privacy they expect and the privacy they get, the fewer bad calls they'll make."[10]

Helen Nissenbaum's theory of privacy as contextual integrity may be of use here. Nissenbaum starts with the recognition that "Almost everything – things that we do, events that occur, transactions that take place – happens in a context not only of place but of politics, convention and cultural expectation."[11] Building on this, she then suggests that things will be experienced as privacy violations when one of two norms is violated: the norm of what information is appropriate to collect, and the norm of how information flows and whether it is appropriate to distribute that information. Understanding context is consistent with Grimmelmann's recognition that "[t]he key principle is to understand the social dynamics of technology use, and tailor policy interventions to fit."[12] Let us look, then, at the context of SNS (and the expectations of users) in order to ascertain what and how privacy issues may be viewed.

To begin with, let us consider the "publicness" of SNS. It has been suggested by some that any attempt to conceptualize SNS as non-public is just the result of confusion about "what is private and what is public on the Internet."[13] Writing this off as mere confusion, however, simply encourages an increase in education around Internet use generally and SNS specifically – an approach which does not seem to have been entirely effective thus far. A proactive approach to analyzing SNS issues must begin with an inquiry into the presumptive binary opposition of public and private.

Considering this question, danah boyd posits SNS as a "mediated public" – that is, an environment "where people can gather publicly through mediating technology." She suggests that mediated publics differ from physically public spaces in having 4 unique features: (1) permanence of record; (2) searchability; (3) replicability/portability; and (4) invisible audience.[14] As Albrechtslund points out, this has its own implications, since "[o]nline social networking can have a touch of private communication to it due to its situational mundane character, but mediated publics are obviously not private. This dilemma is, of course, a central part of the discussion concerning surveillance and privacy issues, and it is especially evident in connection with secondary uses of available information at social networking sites."[15] The boundaries of public and private become less clear in SNS, leaving the participants in the SNS cycle (the site users, the site owners/administrators and the marketers seeking to build on the data collected in these seemingly public online spaces) without markers for how to best proceed. In part, this may be because the issue needs to be further nuanced – it is not a question of where the boundaries of public/private are placed or even whether such absolute boundaries can be placed at all, but rather a question about expectations regarding public and private, rather than bounded spaces.

In 2006, Acquisti & Gross noted that "evidence may suggest that privacy attitudes have some effect on determining who joins the network, but after one has joined there is very little marginal in information revelation across groups – which may be the result of perceived peer pressure or herding behavior."[16] Certainly peer standards seem to have an impact on SNS behaviours – "teens center their understanding of context on other people"[17] and in the SNS situation where boundaries are unclear it is fair to surmise that all users of SNS, not just teens, are taking cues for behavioural expectation from others on the site.

Communication and information sharing on SNS' are open in a (in some ways at least) self-perpetuating way. Regardless of the actual scope of SNS, "teens are not focussed on situating their acts broadly. While their potential audience might be global, their imagined audience is very local, primarily consisting of people whom they know."[18] The user

focuses on "friends" then, and engages in self-presentation and social communication that is for and about that imagined audience. This combination of the imagined audience and peer standards shaping choices may create an "illusion of privacy."[19] Applying the notion of privacy as contextual integrity, however, may lead us beyond the idea of privacy as an illusion, and into the more productive question of expectations of privacy within the space. That is, if the user's understanding is focussed on a particular audience and takes into account peer standards in developing an expectation of privacy, perhaps the best way to facilitate privacy in SNS is not to challenge these user expectations, but rather to map privacy controls on to the site in a way that will best enable the user to achieve her expectations and/or to more fully understand the context in which her SNS use takes place so that those expectations themselves become more nuanced.

Openness is, to some extent, a "designed aspect of the system...to fulfill one's goal often requires a more permissive approach to profile privacy."[20] Nor are users necessarily used to needing privacy mechanisms in such interactions – as Dwyer et al note, "[o]ffline, most social transactions leave behind no trace. This lack of a record is a passive enabler of social privacy. Therefore these sites need explicit policies and data protection mechanisms in order to deliver the same level of social privacy found offline."[21] This need for privacy and data protection mechanisms, however, creates a particular tension for site operators, since "a priori the site operator has diverging privacy goals. On the one hand, he needs enough personal user information to be disclosed in order to attract new users. On the other hand some information must be kept at the community level to create sufficient benefit from community membership."[22] If we want to focus our inquiry on what privacy means to the user and how s/he may best protect it then, it may not be sufficient to expect site administrators to make all the choices.[23]

The trick to making SNS privacy meaningful to the users then is not merely the creation of privacy policies and controls, but rather finding ways to normalize privacy choices within the SNS context so that not only those who are currently using SNS actively engage with them but so that as new users join, privacy becomes as viral as other behaviours.


communication
college
virtual gifts
current
wall
tagging
efficient
photos
social
effective
adaptable
applications
viewable
acquaintances
location
enhanced
entertaining
group
chatting
accessible
company
coworkers
network
universal
free
link
youthful
system
posts
dynamic
status
quick
settings
friends
applications
updates
messages
communicate
feeds
popular
generational
sharing
high school
security
pokes
games
practical
convenient
data
inventive
developing
professional
comprehensive
messaging
albums
cookies
relationships
membership
innovative
viewable
resourceful
significant

Facebook

Facebook

www.facebook.com

Mandate

Facebook bills itself as "a social utility that helps people communicate more efficiently with their friends, families and coworkers."[24]

History

Facebook was established 4 February 2004 by Mark Zuckerberg, its current CEO. The company itself is privately owned and operated by Facebook Inc. The current headquarters are in Palo Alto, CA, with international headquarters (for Europe, Africa and the Middle East) in Dublin, Ireland.[25]

Facebook was originally created at Harvard University, and indeed in its earliest inception was a Harvard-only application, only allowing users with a Harvard.edu email address to join. In March 2004, membership expanded to include other ivy league US colleges Stanford, Columbia and Yale. From there, the site incorporated any university and college student in the US. In September 2005, Facebook expanded to include high-school students. In October 2005, international school networks were added. Finally, in September 2006, the site again changed to allow anyone over the age of 13 to join.

Financials

The website is free to use.

Facebook received $500,000 in initial funding from Peter Thiel, co-founder of PayPal in the summer of 2004. In April 2005, it received $12.7 million from Accel Partners. A further $25 million has been invested in Facebook by Greylock Partners, Meritech Capital Partners, Accel Partners and Peter Thiel.[26]

In October 2007, Microsoft purchased a 1.6% stake in Facebook for $240 million – a deal that valued Facebook at an overall $15 billion. Notwithstanding this valuation, beginning in Fall 2008, the company dictated that its employees could sell stock at prices based on no more than a $3.75 billion valuation.[27]

With regard to other revenue, Facebook does allow users to purchase virtual gifts. Each virtual gift on Facebook costs $1USD.

In a recent interview, Mark Zuckerberg refused to comment on how much revenue is received from the Gifts application, as well as on Facebook's revenues from self-serving advertising, though he did hint that self-service advertising revenues alone could exceed a $50 million run rate.[28]

User Demographics

As of January 2009, Facebook was reporting over 150 million active users (that is, users that have returned to the site within the last 30 days).[29] ComScore reports that in December 2008, Facebook received over 222 million unique visitors, and that it demonstrated 127% growth over the past year.[30]

Over 50% of Facebook users today are outside of college, despite the fact that Facebook maintains an 85% market share of US 4-year universities. In fact, the fastest growing demographic of user's is among people age 30 and older.[31]

At this time, more than 70% of Facebook users are outside the United States. Canada has the most users outside the United States, with more than 7 million active users. The UK is in third place, also with more than 7 million active users. Rounding out the top 10 international countries are Australia, Turkey, Sweden, Norway, South Africa, France and Hong Kong.[32]

Registration Information

Upon proceeding to Facebook.com, a user is prompted to enter their full name, email address, password, sex, and birthdate. A pop-up box is available to clarify that birthdate is requested "as both a safety precaution and as a means of preserving the integrity of the site. You will be able to hide this information from your profile if you wish." Signing up indicates that the user has read and agreed to the Terms of Use and the Privacy Policy. After clicking "Sign Up", the user is taken to a CAPTCHA page. When the CAPTCHA phrase is entered correctly, a confirmation email is sent to the email address provided. The user must

click on a link provided in the email to confirm the intention to set up a Facebook account, and to validate that an accurate email address has been provided.

Having clicked on the confirmation link, the user is taken to a 4-step setup process. First, s/he is prompted to confirm or deny a friendship request from someone that s/he knows. This step may be skipped. Next, the user is invited to "find friends" by providing access to her email address book – the explanation makes clear that you are providing information to Facebook. This step too can be skipped.

Step 3 is titled "fill out your profile" and requests that the user provide information about high schools (and year/class), university or college (and year/class) and/or company affiliation. This step can be skipped. Still at step 3, the user is then provided with numerous Facebook profiles and asked to select people s/he may know by clicking on the profile to add them as friends. This too can be skipped.

Finally, at step 4, the user is asked to provide her geographical location (city/town), with the explanation that this will enable her to see the profiles of other people in the network, and them to see hers. A further note explains that this access can be modified in Privacy Settings. This step too can be skipped.

Having completed these steps, the user has a "Facebook profile". The page s/he is taken to then shows any friends/links provided in the set up process, a "People You May Know" bar on the side, and across the top has banners to "find people you know" by searching for them and to "view and edit your profile".

If one does click on "view and edit your profile", it shows a template for information provision which has any information already provided showing, and spaces inviting information under the following headings: Basic Information (Sex with an option for whether to show in profile; Birthday mm/dd/yyyy, with an option for whether to show full birthday in profile, remove year, or show no birth date at all; Hometown; Relationship status; Interested in men/women; "Looking for friendship/dating/a relationship/networking; political views; religious views) Personal Information (a series of boxes for the user to fill in, titled Activities; Interests; Favourite Music; Favourite TV Shows; Favourite Movies; Favourite Books, About Me); Contact Information (email address, with an option to add or remove email addresses; IM information; Mobile Phone; Land Phone; Address Information street/city/zip; and Website); and Education and Work (College/Uni and year, major/concentration, degree with the option to add or remove schools and concentrations; High School name and year, again with the option to add or remove schools; Employer, position description, location and time period, including the option to add another job).

Accordingly, the only information "required" by Facebook in order to sign up for a Facebook account is full name, email address, password, sex, and birthdate. However, the detailed "steps" for "building a profile" as well as the provision of a template that invites the provision of particular information blurs the lines between "required" and "requested" information.

Real Identities v Pseudonyms

Although the Facebook sign-up verifies email addresses, it does not perform independent verification of the full name provided nor does it seem to identify discrepancies between the name provided at sign-up and email address. As such, there are no technological measures or verification to enforce the provision of a "real" name or identity.

It should be noted, however, that the Terms of Use provide that:

> you agree to (a) provide accurate, current and complete information about you as may be prompted by any registration forms on the Site ("Registration Data"); (b) maintain the security of your password and identification; (c) maintain and promptly update the Registration Data, and any other information you provide to Company, to keep it accurate, current and complete; and (d) be fully responsible for all use of your account and for any actions that take place using your account.[33]

Privacy Controls

Facebook has a set of quite extensive granular privacy controls,[34] as well as a Privacy Policy.[35]

There are 4 sections of privacy controls: Profile; Search; News Feed and Wall; and Applications. Within each section, there are further levels of specific controls that can be placed by the user.

PROFILE: The profile privacy settings allow the user to manage who can see her basic information and her contact information. Basic information categories are set out as: profile; basic information; personal information; status updates; photos that have been tagged of her; videos that have been tagged of her; friends; wall posts; education information; and work information. Contact information categories are: IM Screen Name; mobile phone number; other phone number; current address; website; residence; and email. For each of these categories, the user may select the audience permitted to see her information, generally by choosing between allowing access to: "my network and friends"; people at a selected network and friends; friends of friends; only friends; or a customized selection (which allows the user to customize within existing networks, for instance selecting from amongst undergraduates, graduates, alumni, faculty, and staff for an educational institution network).

SEARCH: The search privacy settings control who, on Facebook, will be able to find your profile, with the caveat that those designated as "friends" will always be able to find the user through search. Using these controls, the user is first able to delimit her visibility in a search, using the same categories (my networks & friends; people at selected network & friends; friends of friends; only friends; or customize) as well as adding

extra parameters to the search group, such as allowing those in college networks, high school networks, company networks, regional networks, or no networks also search for her. Further, s/he is then able to circumscribe what information will be seen by those who search for her profile and what contact options are provided to the searcher.

NEWS FEEDS AND WALL: This section of the privacy controls allows the user to exert control over actions within Facebook and over social ads specifically. In terms of the News Feed, the page sets out a list of items that stories will never be published about and a list of applications, from which stories may be published. On this page, the user is also informed that stories will be published in the feed when profile information is edited, a new network is joined or status is updated, and then s/he is given options as to what other activities may be published, including: removal of profile information; writing on a friend's wall; commenting on a note, photo, album, video or posted item; posting on a discussion board; adding a friend; removing relationship status; or leaving a network. Finally, the user has the option to have feed stories shown in her chat, and to determine whether her Wall should indicate what time stories are published. On the next page, the user is informed that "Facebook occasionally pairs advertisements with relevant social actions from a user's friends to create Social Ads. Social Ads make advertisements more interesting and more tailored to you and your friends. These respect all privacy rules."[36] The user is then given the opportunity to select whether to appear in the social ads of friends or of no-one.

APPLICATIONS: The Applications privacy controls are comprised of both an overview of how Applications interact with personal information; and a page of settings for the user to apply privacy settings to her interactions with applications. There are 6 privacy controls available through this page. First, the user is invited to apply controls to limit what types of information friends can see about them through applications that the user does not herself use. There is also an option to opt-out entirely of sharing information through the Facebook Applications Platform, but it can only be selected when the user does not currently have any Applications selected. The user is then informed that "when you authorize an application, it can access any information associated with your account that it requires to work", although contact information is never shared with an application. Next, the user is informed about "Facebook Connect" and given the option to opt-out of allowing friends to view her memberships on other websites through Facebook Connect. Fourthly, the user is given the ability to opt-out of Beacon posting stories on her profile. The final two sections of this control are an explanation of blocking applications and a list of any applications currently blocked by the user; and an explanation of the power to block application invitations from specific friends, and a list of any invites currently on this list.

Photo Tagging

Facebook is currently the top photo-sharing application on the Internet.[37] As of 29 January 2009, there were more than 800 million photos uploaded to the site each month.[38]

Facebook added photos as an application in October 2005. The application allows users to upload an unlimited number of photos, in photo albums of up to 60 pictures. Privacy settings can be set for each individual album, limiting the groups of users that will have access to the contents of an album.

When a user uploads a photo, they are asked to warrant that they have the authority to do so.

Within the Photos application, users also have the ability to "tag" individuals in a photo by adding associating metadata with the photo. If the tagged individual is another Facebook user, the act of tagging initiates a notification to the tagged user that they have been tagged in a photo, and provides them a link to see the photo, and the ability to request removal of the tag. The creation of a tag also creates a link between the photo and the profile of the Facebook user so tagged.

Photos may be tagged by any Facebook user who has access to the photo, and any name may be added, including that of individuals who are not Facebook users. When a non-Facebook user is tagged in a photo, a pop-up invites the tagger to add the email address of the tagged individual in order to provide them with notice of the tag and to add them to your friends list. Individuals who receive such an email will be able to view the photo, but no other content on the site.

Accessibility of Member Information to Others

Accessibility of information is, of course, subject to the privacy controls selected by the individual user.

NEWS FEED: Initiated in September 2006, news feeds are set up so that after logging in to Facebook, users see a "news feed". This feed will contain items culled from activities undertaken by those on their Friends list. In turn, some of a user's personal information and Facebook activities will be published to their friends' news feeds. Currently, the user is able to opt-out of some information being shared on the feeds, including: removal of profile information; writing on a friend's wall; commenting on a note, photo, album, video or posted item; posting on a discussion board; adding a friend; removing relationship status; or leaving a network. It should be mentioned in relation to Feed's that some Applications (such as Social Ads or Beacon) may include information in the News Feed controls, but the Feed privacy controls will not apply to these features. User control of what information these features may supply to the Feeds (where available) will be located in the Applications privacy controls.

FACEBOOK SEARCH: Facebook users can join one or more networks on the website, each denoting a school, place of employment, geographic region or social group. These networks enable users to connect with other members of the same network. When users search Facebook, viewing of detailed profile information is restricted to users from the same network or confirmed friends. Those searching for a user outside their network or friends list may (depending on privacy settings selected by that user) be

able to find acknowledgement that a profile exists, but will see only the most basic user data – user photo, name, and option to poke or connect.

PUBLIC SEARCH: Originally, only registered Facebook users could search for other Facebook users, and information was limited based on shared networks. In September 2007, however, Facebook introduced public search listings. A public search listing will generally show the Facebook user's profile picture and name. Public searches will allow non-members to search Facebook, as well as permitting some major search engines to index the public search listings. Users may, however, use privacy controls to opt out of having their information included in the public search listings.

Advertising

Facebook generates much of its revenue from advertising.

In August 2006, Facebook and Microsoft formed a strategic relationship for banner advertising syndication. This advertising deal was expanded to cover international markets in October 2007. Microsoft is Facebook's exclusive partner for providing banner advertisements.

Facebook launched the Social Ads[39] and pages feature in November 2007. Essentially, this allows advertisers and businesses to create a presence on Facebook (previously the province only of individuals), and then to capitalize on this presence by affiliating themselves with users. When a Facebook user interacts with an advertiser page, a Feed story is generated as to the content of that interaction.

The Social Ads part of the feature launches as well when the Facebook user interacts with an advertisers page. The Social Ad generated will include the fact of the interaction, the user's name and profile picture and text chosen by the advertiser. These ads then appear in the feeds of the user's friends. Ads may also be demographically targeted within the friends list, aiming at users who share a location, age, sex or other criteria found in the user's Facebook profile. Through the privacy controls, users have the ability to opt-out of appearing in social ads that are sent to their friends' feeds. There does not appear to be a similar control for opting out of receiving such ads containing friends' information.

Facebook's other well-known advertising feature is Beacon, which launched in November 2007. Beacon operates in a similar function to Social Ads, by associating individual Facebook users with advertisers and then transmitting the fact of the interaction to that user's friends, however where Social Ads focussed on interactions with advertisers who had a Facebook presence, Beacon broadcasts interactions with 3d party websites. Advertisers are able to add code to their websites that will facilitate Beacon interaction, and in so doing determine which interactions with the site will generate Feed messages.[40] Users are able to opt-out of Beacon.

Data Retention

Facebook collects both personal information provided by the user and what they term "Web site use information collected by us as you interact with our Web site." Both types of information are discussed in their Privacy Policy.[41]

Facebook's Privacy Policy is available through a link at the bottom the user's Facebook page, and is current to 26 November 2008. There are a few noteworthy features about it: (1) the policy is verified by Trust-E; (2) the Policy begins with a statement of "Facebook Principles" that is written in easy to understand language and keys on the individual user's control over her personal information and her access to information others want to share; and (3) some attempt has clearly been made to eschew legalistic language and relay the information in more reader-friendly terms.

Personal information provided by the user includes information provided upon registration and setting up a profile as well as relationship information, messages sent, searches, group formation and joining, event set up and participation, application additions and other information transmitted through various Facebook channels. The Privacy Policy indicates that this information is collected in order to provide the Facebook service and personalized features. When information is updated, a backup copy of the prior version is retained for an unspecified "reasonable period of time" in order to enable reversion to the previous version if necessary.

Web site information includes browser type and IP address, which is gathered for all Facebook visitors. In addition, Facebook uses cookies, both session ID cookies (which terminate once the browser is closed) and persistent cookies (which may be removed or blocked via the browser's settings if the user so desires). While the Privacy Policy deals with what information is collected and why, it does not set out retention periods for the information.

Facebook also collects and retains information of non-Facebook users that has been provided by users. Their Privacy Policy indicates that non-Facebook users may contact Facebook to request that this information be removed from their database.

Account Deletion

Facebook's original approach to account deletion was problematic – while accounts could be deactivated and thus removed from public view, the information contained in them was retained on Facebook's servers, purportedly to aid in the reinstatement of user profiles when a user returned to Facebook. Users who wished to permanently erase information were able to delete items in their profile on a one-by-one basis, a time-consuming but effective way to manage the information collected on their profile though not the Facebook generated profile.

As of 29 February 2008 Facebook changed its account deletion policies, allowing users to contact Facebook directly to request that a user account be permanently deleted from the website. Users who do not wish permanent deletion still have the option of deactivation, whereupon information will be retained on Facebook's servers though not accessible to Facebook users.

Third Party Applications

The Facebook Applications Platform was added in May 2007. It provides a framework for 2d party developers to create applications that will interact with core Facebook features. As part of Platform, Facebook Markup Language was also introduced in order to customize the look and feel of applications.

The Facebook Platform allows third parties to create applications that will access Facebook's database. Although not created by Facebook, these Applications function similarly to Facebook Applications, and accordingly generally have the ability to publish to a user's Feed and access some degree of user information.

In order for these 3d party Applications to function within the Facebook environment, they require the flow of personal information from Facebook to the Application host or developer. This is acknowledged by, at the time of installation of an Application, presenting the Facebook user with information about information sharing choices[42] and how the Application will interact with their Facebook account.

According to the Facebook Application Terms of Use, when the user adds one of these 3d party Applications, they agree to share all information except contact information:

> Examples of Facebook Site Information. The Facebook Site Information may include, without limitation, the following information, to the extent visible on the Facebook site: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, the text of your "About Me" section, your relationship status, your dating interests, your relationship interests, your summer plans, your Facebook user network affiliations, your education history, your work history, your course information, copies of photos in your Facebook Site photo albums, metadata associated with your Facebook Site photo albums (e.g. time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your Facebook in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall ™, a list of user IDs mapped to your Facebook friends, your social timeline, and events associated with your Facebook profile.[43]

As EPIC notes, it is significant that these 3d party Applications do not only access the information about the user who has added the application and consented to this information sharing. Rather, under these terms these Applications by default also get much information about the users friends and any other network members the user can see. Thus, "without any action from a user, an individual that has never joined any application will have their information sent to the third party application when their friends or associates in their networks join."[44]

Though Facebook's terms of use for the user explicitly requires that users release Facebook from responsibility for any damages accrued by installing or using these Applications, the Facebook Developer Terms of Service does impose some controls on how developers may use Facebook user information, including the requirements that:

> You must treat all users' privacy with the same respect we do. If you directly collect personally identifiable information from users, you must post a privacy policy detailing what you'll do with that info.
>
> - You must be honest and accurate about what your application does and how it uses information from Facebook users. Your application cannot falsely represent itself.
> - You can only show information from Facebook Platform to a user if you retrieved it on behalf of that particular user.
> - You can only cache user information for up to 24 hours to assist with performance.
> - You can't use Facebook Platform for anything that infringes on anyone's rights or intellectual property, generates spam, phishes or is illegal.[45]

Under these terms, any information that the application develops or collects on its own can be kept indefinitely and may be associated with Facebook information that it is permitted to store, for example User ID. While intuitively it may appear that there is a disconnect between the Developer Terms of Service limit of 24 hours to cache information and the ability of 3d party Application Developers to keep some information indefinitely, the distinction is between Facebook information proper and information generated by the application -- Facebook is saying 3d parties cannot cache Facebook info more than 24 hours, but that any information generated by the 3d party application itself is purportedly separate from Facebook information and it is this separate information that may be retained indefinitely.

Recently, Chris Kelly (Chief Privacy Officer and Head of Global Public Policy at Facebook) responded to a question about monitoring the third party developer community by stating that Facebook does monitor every request for information made by an Application, and additionally suggesting that Facebook may be moving towards a more aggressive monitoring stance as well as employing an in-house "application validation" program to allow internal review of the data to ensure that only relevant data is being collected.[46]

Collection of Non-User Personal Information

Facebook does collect non-user personal information from Facebook users, for example when telling a friend about the site (using contact importer or friend finder features) as well as when non-users are tagged in Photos. According to the Privacy Policy, the contact information collected is retained and used to send notification/invitation as well as up to 2 reminders to the individual.

Even after notifications and reminders have been sent, Facebook retains the information in order to register a friend connection if your invitation is accepted, to allow you to see invitations you've sent, and to track the success of their referral program.


students
database
opportunity
capability
accessibility
connections
community
friends
unique
establishment
solutions
originality
enhance
companions
openness
applications
content
creativity
improvement
integration
security
resourceful
acceptance
messages
global
personality
virtual gifts
implementation
possibility
employment
profitable
company
registration
exchange
statistics
identification
expansion
careers
personal
advertising
contacts
develop
technology
communication
accounts
mandate
notifications
documentation
potential
entertainment
Hi5

Hi5

www.hi5.com

Mandate

Hi5 describe themselves as "as online place to meet friends."

History

Hi5 was founded in 2003 by Ramu Yalamanchi, an Indian-American entrepreneur and current CEO of Hi5. In January 2003, with $250,000 in initial funding, Yalamanchi and Akash Garg first launched an "online matchmaking network" called Sona, to serve the South Asian market. Sona's intention was to replicate the concept of match.com, but on an international scale.[47]

By December 2003, the site has been re-launched as Hi5, an international social networking site.[48] The site was originally launched in English in all markets.

According to its founder, Hi5 took six months to amass its first 1 million users (July 2004), and as of June 2008 Hi5 adds "a million members a week."[49]

The founders of the site quickly began to target Spanish-speaking markets when they noticed its popularity in those areas and the relative similarity among Spanish-speaking users. Further supporting this decision was the fact that at that time MySpace was not allowing the registration of users from outside the US, filtering users by their IP address. The Hi5 market was intentionally targeted internationally.

Financials

The company was profitable by October 2004.

The site appears to be feeling the impact of the global economic crisis, with reports of employee layoffs and advertisers pulling out of the site due to reduced rates of unique visitors.[50]

In 2008, Hi5 also started making money off the sales of virtual gifts, with each gift costing "coins", which are in turn purchased with real money, to the tune of $1USD per gift. [51]

User Demographics

Worldwide, more than 80 million people have registered accounts with Hi5, and the site draws nearly 46 million unique users per month (as of April 2008, reported by Hi5).[52] In July 2008 Hi5 reported that based on the comScore Media Metrics figures for June 2008, it was the "fastest growing global social networking web site in [sic] first half of 2008".[53] In the same month, comScore reported that the site "exceed[ed] 50 million monthly unique visitors." [54]

Hi5 is the top social networking service for the Spanish speaking market.[55] Users of the site come from the following countries, in order of largest percentage: Mexico (13.9%), Thailand (13.7%), Portugal (6.3%), Peru (5.9%), and the US (5.6%). Canada does not rank in the top 25 countries.

53% of the users are male, 43% of users are between the ages of 15 and 24, with the next-largest age group being people aged 25-34, comprising 22% of users. [56] Demographics of American users show a higher percentage of males, with 40% earning less than $30,000 and 57% without a college degree.[57]

Data provided by Site Analytics shows that in October 2008 Hi5 had just over 2.3 million unique visitors from the US per day.[58] The trend over the past year shows a slight decrease from just over 2.4 million in October 2007. Another statistics company shows an overall decline in all visitors per day over the past six months that has continued into the beginning of December 2008, showing a reach of just over 2% of all Internet users per day.[59]

Registration Information

When an individual seeks to set up a Hi5 account, they are required to provide their first and last name, email address (in order to receive confirmation), and birthdate.

After submitting this information, they are taken to a page that allows them to check their email address book in order to import contacts into Hi5, however this step can be skipped. This page notes that Hi5 will not store user email address and password nor contact friends without user permission.

Next, the user is invited to upload a profile photo, which requires that they warrant that they have the right to use the photo and that the photo does not violate Hi5's image policy. Again, this step can be skipped. The third step is to enter into Hi5 the "activation code" that was sent to the email address provided.

After account confirmation, the user is taken to a "find friends" screen. At this stage, the user has the option of (a) providing Hi5 access to their contacts on any web-based email program, and (b) searching Hi5 for friends by providing an email address.

Once signed in, the user is invited to fill out more profile information, under the headings of Basic, Photo, Contact, and Interests.

BASIC: Basic information consisted of first name, last name, gender, birthdate, hometown, looking to, status, religion, languages, ethnicity, and about me. Interestingly, on all fields except first name, languages, ethnicity and "about me", the user has the ability to place controls on its visibility, choosing between "everyone can see this", "my friends can see this" and "no-one can see this".

PHOTO: individuals are invited to upload a photo for use as a profile photo.

CONTACT INFORMATION: includes an alternate email address, IM Username, cell phone number, country of origin, Zip/Postal code, address, and the choice of a Hi5 URL. Again, the user has the ability to place controls on the visibility of some of this information, including IM Username, cell phone information, and country.

INTERESTS: Consists of a template of boxes that can be filled in, labelled Interests, favourite music, favourite movies, favourite TV shows, favourite books, and favourite quote.

Real Identities v Pseudonyms

Although the Hi5 sign-up verifies email addresses, it does not perform independent verification of the full name provided nor does it seem to identify discrepancies between the name provided at sign-up and email address. As such, there are no technological measures or verification to enforce the provision of a "real" name or identity.

Privacy Controls

Besides the ability to delimit visibility of profile information, Hi5 has a set of privacy controls which users can use to set privacy standards for their accounts under the headings: profile, message and email settings, photo settings, friend update settings, and online status settings, as well as identify and manage blocked users.

PROFILE: Using these controls, users are able to determine who can see their profile (all users or friends only); whether people can see that you've viewed their profile (yes or no); the audience from which the user will receive profile comments as well as whether those profile comments are auto-accepted or not (all users, friends only, or nobody).

MESSAGE & EMAIL: the user is able to choose whether or not all users can submit friend requests to her; to delimit who can send her messages (all users, friends only or nobody); who can send her "fives" (all users, friends only or nobody); and yes or no on whether to receive birthday notifications, email notifications, and newsletters.

PHOTO SETTINGS: allows the user to determine whether or not friends can tag her photos, as well as determining who can comment on photos and whether those comments will be auto-accepted (all users, friends only, or no-one).

FRIEND UPDATES: akin to mini-feed and Feed features on Facebook, this section allows the user to determine whether or not friends will see her updates on their pages, and which users will be able to view her updates on her profile page (all users, friends only, nobody).

STATUS: allows the user to determine whether or not friends are able to view her online status.

Photo Tagging

Within the Photos application, users also have the ability to "tag" individuals in a photo by adding associating metadata with the photo. If the tagged individual is another Hi5 user, the act of tagging initiates a notification to the tagged user that they have been tagged in a photo, and provides them a link to see the photo, and the ability to request removal of the tag. The creation of a tag also creates a link between the photo and the profile of the user so tagged.

Depending on privacy settings selected by the Hi5 user, photos may be tagged by the Hi5 account holder and by friends of that user. Any name may be added, including that of individuals who are not Hi5 users. When a non-Hi5 user is tagged in a photo, a pop-up invites the tagger to add the name and email address of the tagged individual in order to provide them with notice of the tag and to add them to your friends list. Individuals who receive such an email will be able to view the photo, but no other content on the site.

Accessibility of Member Information to Others

FEEDS: Updates about user activities are displayed on the user's profile. Depending on privacy setting, those updates may be viewable by those who visit the profile, and may be shown on the homepage of friends.

INTERNAL SEARCH: Profiles can be limited to being viewable by all users (which includes those without a Hi5 account) or friends only. Although there is an option to limit some profile information, there appears to be no option to remove the profile entirely from searchability. There is also a search feature, which requires that the searcher enter a name or email address "Search" box at the top of the hi5 home page and then click the

arrow (or use the enter or return key on your keyboard). Search results can be refined to search by various options, including email address, name, age, location, and more.

PUBLIC SEARCH: Hi5 profiles are searchable by public search engines and the default setting is that a user's profile can be viewed by all users of the site.

Advertising

The Hi5 FAQ is clear that in order to continue providing SNS for free, they rely on advertising.[60]

The corporate website section on advertising states that: "By using IP and profile-based demographic targeting, hi5 delivers advertising messages with precision. We offer a broad range of advertising products: targeted display banners, rich media placements, and custom sponsorships."[61]

The Privacy Policy[62] is clear that advertising is provided by third party advertising companies, and that these companies may be provided with both user-provided information and personal information collected by technology. Although the Policy is clear that name, address, email address and telephone number will not be provided to advertisers, other personal information (such as age, gender or location) as well as site visit statistics, IP address, information about the internet service provider or mobile device carrier may be provided in order to facilitate personalization. It should also be noted that the Privacy Policy also gives Hi5 the ability to anonymize personal information, and provides that once anonymized, the information may be used and disclosed at Hi5's discretion.

Data Retention

Hi5 collects both personal information provided by the user to the site and what they term "personal information collected by technology".

The user-provided information specified is the registration information (name, email address, gender, date of birth and zip code) and telephone number. It will also include any other information submitted as part of the profile, information entered on any Hi5 network feature (journals, testimonials, groups, message boards) and they state that should an individual contact them via email, they will retain the email address as well as any information contained in the email. This information is used to provide you with "features that the hi5 community offers its members."[63]

While making a clear distinction between "personal information" and "anonymous information" in its Privacy Policy, Hi5 has an interesting clause allowing them to (a) collect and analyze personal information for its own internal purposes; and (b) removal personal identifying information from collected information in order to render it Anonymous.[64]

Hi5's Privacy Policy has a separate section dealing with personal information collected via technology, which includes IP address, browser type, operating system, telephone number linked with SMS communications, as well as using cookies and URLs to gather information about date and time of visit and actions taken during visit. Again, the policy states that such information is collected "to make our Services and solutions more useful to you and to tailor the hi5 community experience to meet your special interests and needs."[65]

Also under the heading of technology, Hi5 explains that if a user searches hi5 by using a toolbar that hi5 or a third party provides, this may result in Hi5 collecting "Anonymous Information" about you automatically, but that "personal information" will not be collected in this case. The terms "anonymous information" and "personal information" are defined in the policy.

Account Deletion

The Privacy Policy provides that if a user wishes to delete her account, s/he may do so by clicking on a link at the account page. When one selects this link, one is presented with a survey asking about country of residence, reasons for cancelling account, gender, other SNS services used and what Hi5 could have done that would have kept you from cancelling. It is possible, however, to delete the account without filling out the survey. The FAQ makes it clear that once the account has been deleted, a user will no longer be able to access or use Hi5 features.

It should be noted that Hi5's FAQ also includes information on "reactivating" your account, which states that you should login with your ID and password and you will be prompted to "reactivate" the account. Although the FAQ cautions that on reactivation some or all information from the account may no longer be available, the ability to reactivate strongly suggests that Hi5's "cancel my account" process is really a deactivation rather than a deletion.

3d Party Applications

As of September 2008, Hi5 had "over 2000 third-party applications on hi5, with more than 72 million total installs."[66]

Hi5's Terms of Use stipulates that such content is not controlled by Hi5 and therefore Hi5 is not responsible for the content, makes no guarantees about the content, and assumes no responsibility for consequences of such content.[67]

Hi5 deals with third party Applications in both its Terms of Service and its Developer License Agreement. Developers are restricted from collecting end-user information except for the purposes of the application, and then only in conformance with the Hi5 Privacy Policy, the Hi5 Developer License Agreement, and with the express consent of the end user. Developer's are not to retain End User information for longer than 24 hours, are to put in place appropriate safeguards and a privacy policy (which must be at least as protective as the Hi5 Privacy Policy), and must

agree not to retain the information after the termination of the use of the Application.[68]

Collection of Non-User Personal Information

Non-user personal information is collected by Hi5 in a variety of ways, primarily through friend searches and invitations to join Hi5 and photo tagging. According to their Privacy Policy, such information is collected and retained by Hi5. Hi5 will use the information to contact the non-user and invite them to visit the site, to register the friend connection if the invitation is accepted, and as a way to track the success of their referrals. Should a non-user wish this information deleted by Hi5, an email address is provided in the Privacy Policy that they can contact to request removal of the information from the database.[69]

Other

Since November 2007 Hi5 has been part of the Open Social initiative, a common set of API's developed by Google to support the rapid rollout of social network applications. It released the first Open Social translation tool for third party developers in September 2008.[70]


Linkedin
investment
updates
profiles
consent
circumstance
messages
identification
advertising
connections
tagging
industry
settings
leveraging
research
service
career
suggestions
recommendations
proposition
classification
aptitude
independent
information
explore
business
mandate
guidelines
specialized
identifiable
partners
employment
contacts
qualified
sponsors
marketing
relationship
capability
qualifications
development
directive

Linkedin

www.linkedin.com

Mandate

LinkedIn states that "the purpose of LinkedIn is to provide a service to facilitate professional networking among Users throughout the world. It is intended that Users only connect to other Users who they currently know and seek to further develop a professional relationship with those Users."[71]

Rather than "friends", LinkedIn allows people to build and maintain a list of contact details of people they know and trust in business. The people in the list are called Connections. Users can invite anyone (whether a site user or not) to become a connection. Connections can then be leveraged as follows:

> LinkedIn offers an effective way by which people can develop an extensive list of contacts, as your network consists of your own connections, your connections' connections (2d degree connections) and your 2d degree connections' connections (called your 3d degree connections). From this network, individuals can learn of and search for jobs, business opportunities, and people. LinkedIn also serves as an effective medium by which both employers and job seekers can review listed professional information about one another. LinkedIn follows strict privacy guidelines wherein all connections made are mutually confirmed and individuals only appear in the LinkedIn network with their explicit consent.[72]

History

LinkedIn was founded in May 2003, "when the five founders invited 300 of their most important contacts to join." Within a month the site already had 4,500 members, and by the end of 2003 it was up to 81,000 members, and within a year of the start date the site was at over 500,000 members.[73]

Financials

LinkedIn is a free service, but offers some additional services as "premium" services for pay. The first of these, LinkedIn Jobs, began in March 2005.

LinkedIn has had a series of investments by partners. In October 2003, Sequoia invested $4.7million, with Greylock providing another $10 million in October 2004. In January 2007 Bessemer & European Founders Fund invested a further $12.8 million, in June 2008 Bain Capital Ventures invested $53 million, and most recently in October 2008 LinkedIn raised an additional $22 million from Goldman Sachs, Bessemer, The McGraw-Hill Companies and SAP Ventures.[74]

LinkedIn's projected revenue for 2008 is between $75-$100 million.

User Demographics

From its inception, LinkedIn has had a strong international component. Currently, most of the traffic comes from the US (48.8%), followed by India (11.3%), the UK (5.1%), Germany (3.6%) and China (3.5%). Canada has the eighth largest percentage by country, at 2.4%.[75]

One statistics company reported over 8.2 million unique visitors from the US alone in the month of October 2008.[76] This is after a steady upward trend from October 2007 when there were just under 3 million unique visitors.

During Summer 2008, TechCrunch published a series of slides comparing LinkedIn's user base to that of other business networking sites. According to this information the average age of users is 41 years and 53.5% of users have a household income over $100,000 with the average household income at $109,703. These statistics show that 64% of users are male, 34% of them own a smartphone or PDA, and 80.1% have a college or university degree or higher, with a full 37% holding a post-graduate degree.[77]

Registration Information

In order to register, the following fields are mandatory for sign up: first and last name, email address, password, country, postal code (although there is a disclaimer attached, indicating that only region code, not postal code itself will be displayed), employment status, industry, education, province, school, and years attended.

Having provided that, the prospective user is then taken to a "How Do You Want To Use LinkedIn" page, which allows them to select various ways in which the network can help the user find information as well as various reasons for contact that the network could bring to the user. The user is able to select from amongst various options and save those settings.

After saving settings, the prospective user is encouraged to check her email in order to confirm her account registration. After confirming via the email, the user must then log in to LinkedIn. On logging in, the user is taken to a page which invites her to enter web-based email information in order to compare data and find contacts that are already on LinkedIn.

On login after providing the registration information, the user is informed that her profile is 15% complete, and given the option to edit/complete it[78] – an over example of the behavioural expectations that operate to blur the lines between "required" and "optional profile" information. If the user chooses to edit the profile, s/he is taken to a page which asks for further information, namely: request for current and past positions and education, recommendations from other LinkedIn users, Connections on the site, website URL. There are also open-ended categories of information, such as summary, lists of awards and honours, professional qualifications and specialties. The user is invited to "add more" to her profile by adding applications from featured partners, and featured applications are shown. Finally, the user is able to further refine her contact settings by first indicating what type of messages s/he is willing to accept (Introductions and mail or only Introductions), selecting various kinds of "opportunities" s/he is most interest in receiving, and a space to add advice for users considering contacting the user, which LinkedIn suggests should include availability and types of projects or opportunities in which you're interested.

Real Identities v Pseudonyms

LinkedIn's User Agreement stipulates that LinkedIn has no obligation to verify (and does not verify) the identity of Users. This is consistent with the sign-up process, wherein the validity of the email address was checked through email confirmation, but no other information was verified in any visible way. The User Do's and Don'ts that are included as part of the User Agreement, however, do indicate that a LinkedIn user should provide accurate information.

The User Settings in LinkedIn do allow a user to select whether to display her whole name, or simply the first name and first initial of the last name.

Privacy Controls

In the "About LinkedIn" section of the company's website, it states "LinkedIn participates in the EU Safe Harbor Privacy Framework and is certified to meet the strict privacy guidelines of the European Union. All relationships on LinkedIn are mutually confirmed, and no one appears in the LinkedIn Network without knowledge and explicit consent."[79] LinkedIn is also a licensee of the Trust-E program.

Privacy controls in LinkedIn can be found under the Accounts & Settings tab.

The Privacy Settings themselves comprise 9 headings: partner sites; research surveys; connections browse; profile views; viewing profile photos; profile and status update; service provider directory; and authorized applications.

PARTNER SITES: the user may choose to allow customization and enhanced/targeted advertising on NYTImes.com and other LinkedIn sites or not.

RESEARCH: again a yes/no option as to whether the user wishes to receive requests to participate in online market research surveys relevant to her professional expertise/area.

CONNECTIONS: User may choose to show or not show her entire connections list to individual connections (though where connections are shared connections, user does not have the ability to make them invisible).

PROFILE VIEWS: Customizing what information other users will receive when they check to see who has viewed their profile – user may select from name & headline only, anonymous characteristics only such as industry and title, or may choose to have no information displayed at all.

PROFILE PHOTOS: Rather than managing her own profile picture's availability, this tab allows the user to determine whose (nobody? Connections only? Network? Everyone?) profile photos should be visible to her.

PROFILE & STATUS UPDATES: The user must make two selections under this tab. First, s/he must determine whether or not to publish profile updates and recommendations. Second, s/he must decide whether or not to notify connections of status updates (choosing "no" will also mean that the user's information is not included in company or industry updates).

SERVICE PROVIDER DIRECTORY: Where a user has been recommended, s/he may indicate whether or not she wishes her information to be included in the Service Provider Directory.

AUTHORIZED APPLICATIONS: Is, of course, a list of applications that have been downloaded and installed on the user's profile.

In addition to the Account Settings designated as Privacy Settings, some of the Profile and Personal Information settings also have privacy implications, including granting the User the ability to determine the visibility of her profile photo and to determine whether and what information will be publicly available from her profile.

Photo Tagging

Users have the ability to upload a profile photo. Groups too may have a photo as part of their group page. However, unlike other social network sites, LinkedIn does not support the uploading of numbers of photos, the creation of photo albums, nor the addition of metadata to photos by means of tagging. The User Agreement also mandates that the photo be business-oriented.

Accessibility of Member Information to Others

FEEDS: profile updates, recommendations, and status updates may be shown on the user's page as well as being viewable by connections, depending on the privacy settings selected.

INTERNAL SEARCH: There are a number of internal ways that searches can be conducted on LinkedIn. One may Add Connections by importing contacts from a webmail provider. In this case, people who are already members of LinkedIn will be identified by an "in" icon. Those who are not already LinkedIn members may be sent invitations through this search as well. Connections may also be sought out by leveraging existing network/identifications – LinkedIn members can go to the "Add Connections" tab and select either "Colleagues" or "Classmates" and then will see former colleagues or classmates who are LinkedIn members and who the user may wish to send an invitation to register a connection with. Finally, it should be noted that LinkedIn allows members to search for Jobs by keyword, which may also result in profile information being shown to the searcher.

PUBLIC SEARCHES: The default setting on LinkedIn profiles is that they be accessible to public search engines. However, through the Account settings, members have the ability to select whether or not their profile information will be available to a public web search first of all; and secondly what information will be viewable through such a search, selecting a combination of basic information (name, industry, location, recommendations), profile picture, headline, summary, specialties, current position and details, past position and details, websites, interests, groups, honours and awards, and the "interested in" field.

Advertising

Although LinkedIn's Privacy Policy states that they do not sell, rent or otherwise provide personally identifiable information of members to third parties for advertising, this does not mean that personal information is not used for advertising purposes. Rather, the Privacy Policy explains that aggregated anonymous data about service usage is collected and may be provided to third parties for purposes including advertising – this information may be segmented by role, industry, geographic location, or company. It is noteworthy, however, that the Privacy Policy also includes an email address where members may request that their information be exclude from the aggregated research and products based upon aggregated data about User activities on the site.

During Summer 2008, LinkedIn launched DirectAds as a form of sponsored advertising. DirectAds allows users to create advertising that is then targeted by age, gender, industry or seniority of other users who become ad viewers. The ads are then visible on the homepage and profile of the targeted user(s). To date this service is only available in the US.[80]

For larger advertising, LinkedIn offers 3 different ways to target ads: ads can be sent to professionals from all industries and professions; advertising can be targeted at specific segments of LinkedIn Professionals, such as IT Professionals, Entrepreneurs, Finance, etc.; or advertising can be custom-targeted, by industry, seniority, job function, company size, geography, # of connections or gender.[81]

Finally, the Privacy Policy also notes that web beacons may be placed on ad networks within LinkedIn pages in order to allow advertising networks to produce anonymized, aggregated audits, research and reporting for advertisers, as well as to enable other websites to target ads to the member when s/he visits other websites. Information is provided to enable the member to opt-out of web-beacon placement.

Data Retention

LinkedIn's Privacy Policy breaks down the types of information collected by them into a number of categories.

First, there is the personal information that members were required to provide upon registration, namely name, email address, country, zip/postal code, brief professional background information and password.

Profile information is then dealt with separately in the Privacy Policy, with LinkedIn making a clear distinction between the required registration information and additional profile information which is designated as "optional" although it is acknowledged that provision of such information facilitates optimal operation of the site.

LinkedIn also states that they collect information through the website and through the Customer Service website in order to categorize and respond to member needs and deliver "appropriate service levels."[82]

Finally, LinkedIn collects technological information, including web log files, persistent cookies and session cookies. IP files and information about browser and operating system of the user computer may also be logged. The IP address is not considered on its own to be personally identifiable information, and LinkedIn warrants that the linkage between IP address and a member's personal information will not be shared with third parties without consent except when required by law.[83]

Account Deletion

Closing an account is said to remove a member's profile from LinkedIn. Once the account is closed, the user will have no more access to account information or contact information saved within the account, and the profile will be removed from being searchable on the site and through

the public web. The Privacy Policy notes, however, that after closure some data may be retained to guard against fraud/abuse as well as for business purposes such as analysis of aggregated, non-personally identifiable data, or account recovery.

Where a member wishes not only to close an account but to delete all information from LinkedIn, the privacy policy provides an email address where such a request may be directed and promises a response within five business days.[84]

3d Party Applications

LinkedIn does have 3d party applications, as well as "partnerships" with 3d parties.

APPLICATIONS: Products of a Developer. Clicking on the "Applications" tab in the profile will take the user to a page of "featured applications" which also includes the ability to search for more applications. LinkedIn members are able to use a total of 15 applications on their profile and 12 on their homepage. Addition of Applications does allow the Application developer access to profile information and connections information. The Terms of Use provides that in installing an application, you acknowledge that your use of the Application may be subject to the Application developer's terms of use and to the Application developer's privacy policy, which the member will have to accept prior to proceeding with the application.

PARTNERS: are a subset of Platform Developers with whom LinkedIn has a closer relationship. LinkedIn states that they only work with trusted Partners, and accordingly note that the designation of an application as the product of a "trusted partner" may mean that permission to access account information in order to provide the combined/partnered service is automatically granted.

The Privacy Policy explicitly warns that:

> Platform Developers are required to agree to restrictions on access, storage and usage of your information. However, while we typically enter into contractual agreements and take technical steps to restrict possible misuse of such information by such Platform Developers, we may not screen or approve Platform Developers and we cannot and do not guarantee that all Platform Developers will abide by such restrictions and agreements. Certain actions you take through the Platform Applications will be displayed to your connections. You understand that your use of any Platform Applications is on an "as is" basis without any warranty as to the Platform Developers' actions.

Collection of Non-User Personal Information

Non-user personal information may be provided to LinkedIn in order to invite contacts or to list them as contacts. This information is retained by LinkedIn, but will only be used to send invitations and reminders.

No information is provided as to how non-users might request to have their personal information removed from LinkedIn's databases.

Other

In their privacy policy, LinkedIn states that the provision of any information beyond that explicitly required for registration must be understood to be "sensitive" information, but that the provision of that information to LinkedIn constitutes explicit consent to purposes as set out in the User Agreement. On this front, it also notes that while members may withdraw consent for such uses, that withdrawal will not be retroactive.

LinkedIn Privacy Policy indicates that in the event of sale or transfer of ownership of LinkedIn, information may be provided to third party as part of reorganization or sale, and that the third party will retain the right to use the information. Interestingly, there is no statement made as to whether the third party would similarly be bound by the conditions set out in the User Agreement, leading to a situation where consent for use seems to survive sale, but obligations to protect may not similarly survive.


censorship
maintain
current
biography
established
effective
photobucket
publishing platform social
sophisticated
personal
region
easy
shopping
controlled
advertising
art
user-friendly
identity
statistics
educational
manageable
expressive
site
searches
viewable
develop
applications
scrapbook
free
virtual
interaction
marketing
interests
developing
customize
networking
language
database
public
security
privacy
students
continuous
accessible
LiveJournal

LiveJournal

www.livejournal.com

Mandate

The company profiles refers to LiveJournal as a "community publishing platform", a blend between a blog and a social networking site.[85] To this end, the user effectively has three platforms: the ability to create and customize a journal on the web that may be shared; development and maintenance of a "friends list", which will bring content from friends' journals as well as selected RSS content to the journal of the user; and finally a User Page/profile which contains contact information, self-submitted biography, lists of interests, friends, communities, schools as well as images (linked from off-site sources).

The site is an Open Source project, and is run using free and open source server software. Most of the applications are also open source.[86]

History

LiveJournal was started by Brad Fitzpatrick in April 1999.

In 2005, Six Apart bought LiveJournal's parent company, Danga Interactive. Danga Interactive's founder (Brad Fitzpatrick) continued his involvement with the project, working as a staff member at Six Apart into 2007.

In December 2007, Russian Internet Company SUP purchased LiveJournal and established LiveJournal Inc. to run it. Although the Terms of Service still specifies that California is the appropriate jurisdiction and LiveJournal Inc.'s head office is located there, with a satellite office in Moscow, Russian ownership has raised some concerns about the privacy of personal information and the potential for the Russian government to gain access to the information or censor content.[87]

Currently in Russia, LiveJournal makes up the vast majority of the blogosphere, hosting over 80 of the top 100 Russian blogs.[88]

Financials

LiveJournal offers six different types of accounts, with the extent of advertising, size of account, and access to services defined by the type of account selected:

BASIC: the basic account is free for all registrants and offers a limited number of features. Prior to 12 March 2008 Basic service was ad-free. In August 2008 when the creation of Basic account resumed, some advertising display was included.

EARLY ADOPTER: No longer available to new users, this type account was available to users prior to September 2000. Early adopters received some extended features beyond those available to Basic accounts, but did not receive any of the paid features.

PLUS: The Plus account offers the services of Basic along with some enhanced features and expanded storage. The account is free, but is subsidized by advertising viewed by the individual user throughout LJ as well as by most visitors to their content.

PAID: Paid accounts are available for set terms, and offer the user the most extended and basic features possible in LJ. Paid accounts are non-transferrable and non-refundable.

PERMANENT: These cannot be "signed up for" by a new user – rather, a permanent account has access to all the features of a Paid account but have no recurring fees attached to them. Possession of these accounts usually indicates LJ founders, administrators or those who have been otherwise involved with LJ.

SPONSORED: Sponsored accounts offer free services, including access to the majority of paid account features. The cost of this account is subsidized by sponsors.

The site also offers a "Gift Shop" where one can purchase virtual gifts (from $.099 USD) for friends on LiveJournal. It is also possible to purchase account "add ons", such as the ability to add extra userpics and an increase in storage space.

User Demographics

Alexa breaks down the percentage of LJ users by country, showing the top five countries as Russia (29.5%), US (24.7%), Ukraine (3.5%), Singapore (3.4%) and the UK (2.9%). Canada ranks 11th, at 2.1% of the total users.[89]

Like Facebook, LiveJournal also maintains its own statistics page, containing data updated every 24 hours. The site shows over 17 million accounts, with just under 2 million remaining active. An age distribution of users put the mean age at 20 years, with most users falling between 18 and 24 years.[90]

As for traffic, one statistics company reported 4.5 million US visitors in October 2008. They show that the most common age range of users is slightly higher, being 18-34. The statistics show a fairly even split between college graduates and non-graduates.[91]

Registration Information

Interestingly, when one registers for a LiveJournal account, one is not asked for first or last name. Instead, one is asked to provide the name/pseudonym for the account. One is also asked for email address, password (a sidebar requires that password include both letters and numbers), birthday (a sidebar notes that the information is required by law but that by default only month and day will be displayed), and a CAPTCHA phrase.

After providing this registration information, accepting the Terms of Use and Privacy Policy and acting on a checkbox as to whether or not to receive LJ announcements, the user then goes to a "Quick Start Setup" page. This page allows users to set up themes (appearance and layout) for the journal, as well as to provide further personal information. The page is clear that all fields on this page are completely optional. It asks for "name" (with the pseudonym provided at registration filled in by default), gender (option of unspecified), location (country, state, city). The template also has space for adding interests, broken down into: music, movies/tv, books. Hobbies, other. Finally, a blank space exists for the provision of a bio or other information.

After providing (or not) this profile information, the user is given the option to upgrade to a paid account. After this, the LJ account has been set up, and it requires on the confirmation via email to activate it. Upon confirmation, the user is taken to an LJ page that contains information on what (and how to use) various features are, such as profiles, friends, journals, communities.

Users are able to upload "userpics" which are used to mark posts. These pictures may be photos of the user or anything else within the bounds of acceptable use – in fact, communities of "icons" proliferate on LiveJournal for users to search, find, download and use various pics.

Real Identities v Pseudonyms

LiveJournal does not mandate the provision of "real" identities – it allows users to sign up using the identity of their choices (pseudonym or not). It does, however, confirm email addresses.

Interestingly, LiveJournal's Terms of Service require users to "provide accurate, complete and current information about themselves in all required fields" during registration.

Privacy Controls

Compared to other SNS or blogging sites, LiveJournal has a very rich set of privacy features (filters, custom groups, communities, "friends only" posts, etc. A minimum security level may be set for the journal as a whole, as well as privacy settings being available on a post-by-post basis, with the user having the ability to designate each post as public (viewable by all users), friends (viewable only by those on friends list), private (viewable only by the writer) or custom (viewable only by user-designated custom friend groups).[92]

Using profile management tools, the user may also elect not to have her profile information be publicly viewable.

Photo Tagging

Images may be added to journal entries, either by using HTML, Photobucket (a third party site on which the user would have to set up an account but which supports remote loading to LJ) or LiveJournal Scrapbook. To add images to comments or profile page, HTML must be used.

Users may place security settings on LiveJournal Scrapbook, selecting either Public (visible to anyone), Registered Users (visible to any logged-in user), All Groups (visible to anyone on the user's friends list) or Private (visible only to the user). Security levels may also be applied to individual galleries/albums, and the security level selected for the gallery is inherited by every photo within that gallery.

For security reasons, LiveJournal prevents the use of scripting languages to embed objects on LiveJournal, and thus the addition of metadata tags to photos is not permitted within LiveJournal. Manual links may be created in the text of the journal but will not associate directly with the image.

Accessibility of Member Information to Others

FEEDS: there are not "feeds" of profile information as we are familiar with them on other sites, however, by using the Friends List, users will receive content posts from friends, communities and RSS feeds to which they've subscribed.

INTERNAL SEARCH: LiveJournal supports a variety of search methods. Individual users may be searched for my username, email address, or IM identity, as long as that information has been made publicly searchable by the account holder. Users may also search by communities, by interests, by latest posts (a collection of the latest LJ posts), looking through the friends page of their friends, random searching, through schools or by using the "Explore LiveJournal" feature. Premium account holders may also have other methods of searching, including directories and regions.

PUBLIC SEARCH: There is no way to set up a LiveJournal profile so that it will not be publicly visible. Users may use security settings to ensure that entries are not publicly viewable, however, and may also edit their profile settings to manage what profile information will be publicly available. The Viewing Options page in LiveJournal also has tools to minimize the journal's appearance in public search engines.

Advertising

LiveJournal uses advertising to ensure that some account levels are available free of charge to users. Whether or not advertising is seen depends on the account level:

Early Adopter/Basic accounts: ads will be seen when viewing a Plus account's journal, friend's page and profile, but not on one's own journal.

Plus accounts: Ads will be displayed on the user's journal and seen on most pages of the LiveJournal site.

Paid/Permanent accounts: When logged in, the user will not see advertising on LiveJournal, even when viewing a Plus account journal.

Logged-out Users: will see advertisements when viewing a Plus or Basic account's journal, as well as on LiveJournal pages.[93]

Interestingly, LiveJournal users are given the option to choose their ad settings. To do so, a user provides account type, gender, year of birth, location (city, state, zip/postal code, country) and then selects 5 or more of the provided categories of advertising that are of interest to them (such as: art & humanities; personal electronics; news; shopping; pets etc.) On this page, Users are assured that LiveJournal will not share personally identifiable information with third parties.

When providing advertising, LiveJournal targets ads by: user preferred ad categories, gender, age, location, interests, or a small portion of public page contents. Ads are targeting not only with reference to the user herself, but also to information about the viewer and governed by LiveJournal's own ad preferences. Targeting may be achieved through data aggregation, though the Privacy Policy maintains that such aggregate information will not be personally identifiable.

According to both their Privacy Policy and their FAQ # 267,

> LiveJournal adheres to its Privacy Policy at all times. Your email address, any personally identifying information, and protected entries are never shared with advertisers or partners. LiveJournal and its advertising partners may use browser cookies to improve the precision of ad selections for users. LiveJournal does not store personally identifiable information in its cookies, nor do we allow our partners to do so.

According to the Terms of Service, where an account contains advertising, the user must agree not to obscure any advertisements from general view.

In terms of cookies by advertisers, LiveJournal has an interesting section in their Privacy Policy where they set out a list of ad networks and third parties with whom LiveJournal has relationships, including URLs, in order to allow users to manage cookies set by those third parties.

Data Retention

LiveJournal's privacy policy is written is very clear and understandable form. According to it, they collect:

- Information provided on registration, LiveJournal product and service use, and posted content;
- Personal information provided by entering promotions or contests on the LiveJournal site;
- Aggregate de-identified information;
- Information about transactions, such as credit card information for payments; and
- Technological information, such as IP address, cookies, pages searched for, and logs.

This information is used for internal LiveJournal processes and is not sold.

Account Deletion

When a user chooses to delete an account, they are informed that information from the deleted account will be saved for 30 days, after which it will be permanently deleted. Also, the user is provided with a survey to take to determine the reason(s) why the user has chosen to leave LiveJournal.

3d Party Applications

Neither LiveJournal's Terms of Service nor its Privacy Policy mention applications or third party applications.

Collection of Non-User Personal Information

A non-account holder who posts as a "guest" will have the content of that post collected by LiveJournal. Similarly, any information about a non-user that is provided in a user's journal may be collected as part of the collection and retention of content. Neither LiveJournal's Terms of Use nor its Privacy Policy include provisions for how non-users might have their information deleted by the site.

Other

Unlike other sites, it is noteworthy that the comments feature in LiveJournal may enable the display of IP addresses to the owners or maintainers of LiveJournal journals where the functionality to do so has been enabled at that journal.


MySpace
self-expression
lifestyle
friends
videos
hobbies
education
music
public
personal statements
profiles
photos
contests
groups
settings
musicians
youth
unique
networking
private messages
display name
notifications
personal
sharing
targeted
advertising
bulletins
bands
personality
usage
innacurate information
opportunity
classifieds
streaming
polls
third party
interaction
tracking
user-provided
monitored
visitors
update feeds
internet
customized
password

MySpace

www.myspace.com

Mandate

The company slogan is "a place for friends."

It has also been described as "primarily aimed at youth, giving them the opportunity to relate to brands and bands, as well as self-express."[94] Users of the site are able to browse profiles of other users, blog, email and join groups. MySpace also includes video and music content, as well as classified ads. Musicians are able to establish a presence on the site, add friends, stream music and sell music.[95]

MySpace is set up so that the user can customize the layout and colors of their profile page with virtually no restrictions, provided that advertisements are not blocked or covered up. Some problems arise from this policy, including unskilled users overloading their pages and causing browsers to freeze as well as security concerns arising from the ability by users to embed code in their pages.

History

MySpace was founded in 2003 as the social networking site within e-Community, a group of community websites. In January 2004 it was launched as its own site.[96]

MySpace was purchased by NewsCorp on 19 July 2005, and is now part of the Fox Interactive Media division.

Currently, the site has 200 million accounts and 110 million active users each month.

Financials

MySpace is a free site, supported by advertising. There is the possibility, however, that in the future it may incorporate for-purchase Premium Services.[97]

With regard to revenue strategy, the CEO of MySpace has said that "Our international strategy is different than our competitors. We look at advertising dollars, and 95% of all advertising revenues come from 9 countries."[98]

The newly introduced platform, MySpace MyAds is helping revenue. After only three weeks of existence, in November 2008 it was bringing in an average of $140-$180,000 per day. 2008 revenue was estimated at $750 million, with MySpace revenues for the fiscal year ending June 2009 estimated at $1 billion.[99]

User Demographics

Reviewing international use of MySpace shows that the largest number of MySpace users are found in the US (70.4%), Germany (3.5%), UK(3.4%), Italy (2%) and Mexico (2%). Canada ranked ninth at 0.9% of all users.[100]

In the month of October 2008, MySpace had almost 55 million unique visitors, a downward trend over the past year since peaking at 66 million unique visitors in November/December 2007.[101]

According to MySpace's own statistics, 25% of Americans are users of MySpace, and 85% of users are 18 and over. On average 300,000 new people sign up on the site per day.

In terms of Canadian users, MySpace indicates that as of October 2008 there were 4,465,000 unique visitors/month to the site. Male users represent 62.7% of users, with women representing 47.3% of users. Age demographics indicate that 35.1% of users are in the 18-34 age range, while an additional 34.2% are in the 35-54 range.[102]

Registration Information

In order to sign up for an account, a prospective user is required to provide: email address, password, a display name as well as a first and last name, location information (country, state, postal code) date of birth (with an option as to whether other user's can see birthday notification), gender, country site and language, a CAPTCHA code, and a checkbox to confirm that signing up agrees to the Terms of Service and Privacy Policy.

Following this, the User is taken to a 3-step "get started" process, where s/he is invited to: upload a profile picture; provide educational information (school name, city, province, country, years attended); and find friends by searching the contacts on the provided webmail address

(a pop up notes that MySpace will not retain the password used to access the account). Each of these steps can be skipped if the user so chooses.

After confirmation email, the user is then free to begin customizing her profile, both with the addition of more information and in terms of design and layout. At this stage s/he is presented with numerous tabs: contact info; account; password; privacy; spam; notifications; applications; MySpace ID; Mobile; Calendar; Miscellaneous.

Contact information requested by the template is display name (a message underneath the slot encourages users to add multiple names, real names, former names to facilitate being "found"); first and last name (underneath which there is a checkbox to opt-in to having full name show whenever the display name and photo are shown); maiden name; contact email address; alternate email addresses (the user is told this will only be used for search purposes); IM Ids, location information (country, province, city, zip/postal code).

Real Identity v Pseudonym

MySpace's registration information makes a distinction between user name and display name. Although it is mandatory to provide a first and last name, the user has the option whether to have these displayed or whether to display only the selected display name.

Although email is confirmed, no confirmation was done of other information provided.

MySpace's Terms of Use does state that users must submit accurate registration information and maintain its accuracy.[103]

Privacy Controls

The profile setup includes a tab titled Settings: Privacy. Under this heading, users are able to make decisions about: whether or not an "online now" icon should be attached to the profile; whether or not to show birthday to friends; whether or not to allow users to share/email photos uploaded by the user; whether to block users who are under 18; a list of other users who have been blocked; and the option to determine whether the user profile will be viewable by everyone, everyone over 18, or friends only.

Though not designated as "privacy controls", the settings tabs also allow the user to identify the level of spam s/he's willing to receive, as well as to manage communications such as messages, friends requests, comments, group invitations, event invitations and IM invitations. Similarly, under "notifications", users may manage what events generate an email notification to them from MySpace from among a variety of actions including messages, comments, friend requests, photo comments and tags, video subscriptions, blog subscriptions and comments, group invitations, forum replies and event invitations. The user is also able to unsubscribe from the monthly MySpace newsletter on this page.

Under "MySpace ID", the user also learns that s/he may link her MySpace account to 3d party services. Any services so linked to are shown on this page with the user being able to control which data is shared with the service or to remove the service entirely.

Finally, under the "applications" tab, users are able to determine whether they wish to receive messages and comments from applications as well as to set privacy access levels for applications installed by friends (the user may choose not to share data, to share basic data only, to allow access to public photos and photo albums as well as basic data). This page also shows the user a list of applications s/he is currently using, as well as a list of those s/he has blocked.

Photo Tagging

Members do have the right to tag photos. When a photo is tagged, a link is created between the photo and the profile of the Member tagged.

When seeking to tag a photo with the name of a non-MySpace member, a box pops up for email address of the individual and offers to send them an email link to the photo.

Accessibility of Member Info to Others

FEEDS: Where a user selects "Friend Updates" they will be able to see feeds of activities undertaken by those on their Friends list. Friend Updates also includes tabs that will allow the user to customize (a) what information about friends is shown in these updates and (b) what information about them is shown on the friend update feeds of their friends.

INTERNAL SEARCH: Users are able to search for other MySpace users by name, email address, IM. The User does have the ability to limit what information is shared in such a search, by marking the profile as "private" in which case only limited profile information is shown.

PUBLIC SEARCH: Public search engines are able to index the portion of a user's profile that is publicly displayed.

Advertising

In late 2008, MySpace developed HyperTargeted ads and SelfServe ads.

MySpace's MyAds platform allows advertisers to target ads to users by gender, age and geography (which can be further subdivided into "National US", "regional", "city/state" or "zipcode"). The MySpace MyAds FAQ (targeted at advertisers) also notes that since the targeting is based on user-provided information, MySpace does not guarantee the accuracy of the information, and further that they will not use geolocation technologies to enhance geographic targeting.[104]

The MySpace Terms also contains a provision recognizing that advertisements may be delivered by third party Internet advertising companies who may use technologies including cookies to collect

information and data. An email address is provided in order to allow users to find information about the techniques and privacy policies of these companies, as well as to allow them to opt-out of such information collection.[105]

Data Retention

MySpace collects email address, first and last name, postal code, gender, and date of birth at registration. MySpace may also collect information from participation in MySpace activities such as sweepstakes, contests and surveys, content on the site, and information submitted to MySpace for review or communication.

MySpace may also collect profile data such as: birthdate, interests, hobbies, lifestyle choices, groups with whom you are affiliated, videos and or photos, private messages, bulletins or personal statements.

MySpace also collects technological information about users, including IP address, aggregate user data, and browser type. They state that this information will be used to manage and improve MySpace services, track usage and for security purposes.

The MySpace Privacy Policy makes an interesting distinction between Registration Data and other profile information, stating that "MySpace determines the purposes of collection, use and disclosure of the Registration Data you provide and, as such, is considered the data controller of this information. Because the Member, not MySpace, determines the purposes for which Profile Information is collected, used and disclosed, MySpace is not the data controller of Profile Information that Users provide on their profile.

Account Deletion

Under "change account settings", MySpace users are able to select a "cancel my account" button. After clicking it, information on how to cancel the account will be sent to the user's email address. MySpace is clear that deletion is permanent, and that while an email address may be used to re-register, the profile will need to be rebuilt because the information is not retained.

3d Party Applications

Applications for MySpace are similar to those available for Facebook, including Applications such as "Mobile", "News", "Classifieds", "Karaoke" and "Polls".

As of 5 February 2008, MySpace announced that users would be able to add games, email and other third party applications to their MySpace accounts. The MySpace Developer Platform was fully launched in March 2008. MySpace emphasizes that developers will only have access to publicly available data, and further that users will be able to restrict profile access to "friends only" and in so doing prevent developer's from accessing it. Developers will have special pages for each application on which they will be able to sell ads, sponsorships and products, however no ads will appear on the applications themselves when installed.[106]

MySpace is also currently working to launch MySpace Music:

> The new joint venture, which tosses music rights from the big labels together with the existing MySpace Music property and users, is announcing a number of launch advertising partners this afternoon, including McDonalds, Sony Pictures, State Farm and Toyota. Each of these ad campaigns are rumoured to be in the single or double digit millions of dollars.[107]

MySpace's Terms of Use include a statement about third party applications that MySpace will not be responsible for the content, accuracy or opinions expressed on websites linked to applications, and that the websites are not monitored or vouched for in any way by MySpace – essentially, that access to third party sites is done at the user's risk.[108]

The Terms also provide that third party applications are separate from MySpace, that MySpace cannot and does not control third party developers, and that MySpace encourages users not to provide information to a third party application unless the user knows the party with whom s/he is interacting.[109]

Collection of Non-User Personal Information

There is no mention of non-user personal information in either the Terms or the Privacy Policy. In Photo Tagging, however, one can enter the email address of a non-user to send them a link to a photo. Similarly, in searching one may enter email addresses, IMs etc. in order to search – there is no indication whether MySpace retains this information.

Other

MySpace's Privacy Policy contains a section on Access that grants MySpace members the right (whenever possible) to review the Registration Data that MySpace retains about them, and to correct any personally identifiable information they hold that a Member informs them is incorrect. There is no indication whether the right of access extends to information beyond the Registration Data.


visitors
video
telefun
members
france
promotions
gender
personality
physical description
social
terms of service
user
strangers
blog stars
language
optional
activation
downloads
competitions
expression
mobile
opinions
ring tones
people
blog of the week
interactive
teen
friends
relationship status
sms
security
template
telephony
chat
french
collect information
games
customization
relationships
targeting
SkyRock

SkyRock

www.skyrock.com

Mandate

The logo for Skyrock includes a tag-line that reads "Free People Network".

Skyrock's Terms of Service describe it as "an interactive platform, which includes but is not limited to hosting and blog services, profiles, chat, the posting of comments, editorials, information, games and competitions, e-mails, instant messaging, forums, the possibility of sending SMS, and ring tones and logo downloads for mobile telephones.[110] It has also been described as a "French teen blog platform." [111]

History

Skyrock Property is a privately held French company, based in Paris France. It was originally founded in 1985 by Pierre Belanger as a French radio station. The website Skyrock.com was first registered online on 13 May 1998 in connection with the radio station.

The website "Skyrock.com" is published by Telefun SAS (Societe par Actions Simplifiee). Telefun Online Services is now a separate entity from Skyrock Music.[112]

Belanger founded the Skyrock Blogs (Skyblogs) platform in 2002, and the current social network site has evolved from this foundation.

In May 2007 the social network site was rebranded as Skyrock.com, and became a "full-scale social network, with new functionalities such as adding friends, an inbox, chat rooms and member profile."[113]

Financials

Skyrock is 70% owned by Axa Private Equity.[114] AXA's website describes Skyrock's development programme as based on:

- Growth in Internet & Mobile activity (25% of revenues), boosted by the increase in the number of blogs, new functions (audio, video), the increasing power of on-line advertising on the blog website (new advertisers, special transactions), and the development of its telephony offer.
- Growth in radio business (75% of revenues); thanks to the 2006 plan for re-allocation of frequencies, a potential increase in national radio coverage from 33 million to 45 million inhabitants.[115]

Skyrock has been for sale since June 2008. In an article on its status, it is revealed that revenue "has grown from less than €5 million in 2005, less than €10 million in 2006 and €15 million last year [2007] to a forecast €20 to €25 million in 2008."[116]

User Demographics

International use of Skyrock shows that the highest number of users are from France (72.8%), followed by Belgium (8%), Switzerland (3.8%), Algeria (3.2%), and Morocco (2.1%). Canada ranks 6th, with 1.8% of users. The US makes up only 0.5% of the total users.[117]

Over the past year, usage statistics vary from a high of 600,000 unique users in January 2008 to just under 200,000 in December 2008.[118]

In February 2008, the statistics showed that "Skyblogs counts more than 22 million subscribed users, 14 million active blogs, and 5.3 million profiles. The site is the world's 17th site globally in page views, has more than 20.2 million monthly unique visitors, and counts a whopping 1.8 billion comments, 22.5 million videos and 400 million pictures."[119]

Registration Information

To sign up for an account, an individual must provide: username, email address, password, language, gender, birth date, country and postal code. Users may also provide their name. On this first page, user's are ask to designate whether or not Skyrock users may search for them using their email, first or last name; and whether they wish to be informed of promotional offers. The user is then asked to confirm that s/he has read and accepted the Terms of Service and to enter a CAPTCHA code.

On completing these steps, the user is taken to a new screen entitled "Blog & Profile". At this screen, the user is asked to provide a title for her blog (mandatory) and "present" it; to provide birthday (mandatory) as

well as the option to provide country, region, city and a little "about me" biography. On this page the user may also upload a profile photo and select wallpaper for her profile.

After this, the user must activate her profile using the confirmatory email sent to her email address. After this is completed, the account is activated. The user is then taken to a "welcome" screen that invites her to create a blog (including photos, video etc); create a profile; or invite friends to Skyrock.

If the User chooses to further flesh out her profile, s/he clicks on "edit my profile" and is prompted to add additional information to her profile: sex (boy/girl); birthday (the only mandatory piece of information); country, region and hometown; relationship status; searching for; occupation; where you live; personality; whether or not User is a smoker; physical description information (hair colour, eye colour, height, weight), and spoken language. The template then provides an open box for "presentation" (a brief bio) and lists of "like" and "dislikes".

Real Identities v Pseudonyms

At registration, the user is asked to provide a username – provision of an actual first and last name is optional. The provided email address is confirmed via the confirmation email, but no other information is verified.

The GTU provides that the User must provide "true, accurate, up-to-date and complete information on the User's Identity and age as requested in the registration form."[120]

Privacy Controls

There do not appear to be privacy controls available to users on the site.

When editing her profile, the User is able to opt-out of "show the visits".

Photo Tagging

Users are able to post up to 24 photos to their profile. Metadata tagging does not seem to be facilitated.

Accessibility of Member Information to Others

FEEDS: Logging on to the Skyrock "homepage" shows a variety of information about other users. It lists how many blogs & profiles are on the site as well as how many chatters are currently online. It showcases a "Blog & Profile of the week" with a photo, username and a description ("just love making other people happy <3") of the 16 year old female. There are links to click to see the profile and blog of this user. There is a link to Skyrock Chat. There is a "Blog Stars" Hall of Fame, again showing user picture, username and a description. There is a window showing 8 "new members" by photo and username. There is a Top 100 Blogs list, a Music Blogs list, and a Last videos list.

INTERNAL SEARCH: Finally, in the middle, there is a search function, allowing the user to search profiles using criteria of sex and country. An advanced search function is possible, which allows the user to search for: girls, guys, or guy or girl; age; country; city; status (single, indifferent, significant other); looking for; here for; occupation; location; personality; eye colour; height; hair colour; smoker.

PUBLIC SEARCH: Skyrock profiles are searchable through the public web. When a found, a profile may include username and photo, description, links to contact, add as a friend, etc and well as profile information, a friends list, and a list of favourite blogs (all standard profile information). There does not appear to by any way to limit public access to this.

Advertising

Skyrock has benefitted from its alliance with the namesake radio station, with early cross-promotion helping to drive Skyrock growth.[121]

The Skyrock GTU deals with advertising, stating:

> 3.i As consideration for the free nature of the Services offered to Users by Telefun, Users authorise Telefun to associate advertising or promotional messages such as text, images, video or sounds chosen by Telefun and that are in any format, with the Content the User posts on any one of the Services whatsoever. In general, Users accept that Telefun may use (and refer to) the Content posted by the User in order to ensure the promotion of its Services. Users may not, under any circumstances, claim any remuneration or compensation whatsoever in respect of this authorisation. If Users wish to withdraw this authorisation, it is up to them to close their Personal Account . Said withdrawal has no retroactive effect. Any advertising or promotional action that may have been undertaken by Telefun when the User closed his/her Personal Account shall continue for the full planned duration.

Skyrock does sell advertising for the site, but it is unclear whether they use site information to target that advertising.

Data Retention

Skyrock collects all information, data, text, software, music, sounds, photographs, images, videos, messages or other contents or material. The GTU explicitly provides that technological information may be collected by use of cookies, IP address collection etc.

Account Deletion

Users may opt to delete only their profile or to delete their Skyrock blog. There is a large "caution" that deleting the blog means all information (blog, profile, photos, etc) will be gone.

The GTU has an interesting provision stating that:

> 2.d. When a User's Personal Account is closed, regardless of the reason for closure, the data concerning said Account and in particular the traffic data, is deleted or made anonymous. However, operations to delete or make certain categories of data anonymous may be deferred for a maximum of one year with a view to ensuring the safety of Telefun facilities and for the purposes of the search for, identification and punishment of criminal offences, with the sole aim of making information available to the judicial authority if need be.

3d Party Applications

Although Skyrock has many applications, they seem to be internal rather than provided by third parties.

Collection of Non-User Personal Information

Since registration is not necessary in order to peruse Skyrock, Skyrock necessarily collects information about non-user via traffic data. In the case of chats, contests and other applications, it is possible that personal information may also be provided to Skyrock by non-users. Finally, in seeking to tag photos, it is possible for an email address to be provided to Skyrock in order to send a link to the photo to a non-user. The GTU contains no provisions dealing with this information, nor with any action a non-User may take to remove her information from Skyrock's possession.

D: Comparative Analysis

Registration Information

Required v Requested Information

The Rome Memorandum recommends that sites be "honest and clear about what information is required for the basic service."[122] On the face of it, sites are complying with this recommendation – looking at each of the selected six sites, it seems that first there is a screen requiring certain limited information that is required in order to sign-up for an account, and the information that is solicited later by way of prompts to build or fill-out a profile.

Looking at the process as a whole, however, the distinction is far less clear. An individual setting up a profile goes through the steps as a single process – s/he provides the required registration information, activates the account through email, then proceeds to setting up a profile by providing further information. As such, a user may not be clear on what information is required for registration and what is additional profile information.

Further, each of the sites employed some form of "template" for profile creation, with categories and spaces for users to fill in profile information. By so doing, the information may be considered to have been, if not required, at least solicited or recommended to be provided by the site – the distinction certainly may not be clear to the user.

LinkedIn and MySpace's Privacy Policies explicitly recognize this distinction, with LinkedIn specifically noting that information other than required information is "sensitive" information but that providing it to the site constitutes explicit consent for its use for the purposes set out in the User Agreement, and MySpace stating that MySpace is the data controller of the required registration information but not of any additional information submitted as part of profile information.

Susan Barnes suggests that "[a]sking for this type of information and setting up requirements for membership tend to make kids think it is safe to reveal personal information online."[123] Although Barnes' article focussed on youth use of social networks, the point can be expanded – when a site invites the provision of particular information, it facilitates both its provision and the assumption that it is safe.

Recommendation 1: Sites should strive to comply with the Rome recommendation to more clearly delineate what information is required in order to access the service. In itself, however, this may not be sufficient.

Recommendation 2: Sites must recognize that the distinction between required information and that which they solicit or suggest for profile and site use optimization is not a clear one, and that accordingly it may be disingenuous to apply different standards to the different information.

Security

During the registration process, a few security-focussed steps came to our attention.

Facebook, LiveJournal, MySpace and Skyrock all used CAPTCHA[124] challenge/response algorithms on their registration pages in order to ensure that accounts were being signed up for by individuals, not bots. ENISA recommends that sites "promote stronger authentication and access control where appropriate."[125]

Recommendation 3: Sites should be encouraged to incorporate CAPTCHA algorithms to promote stronger authentication and control.

Similarly, in setting up the original password for the site, it was noteworthy that some sites had sidebars that either explained minimum secure password standards for the site or simply validated that a submitted password met the minimum standards. Again, this is a fairly simple security procedure but one with value for the protection of such personal information-laden accounts.

Recommendation 4: Sites should be encouraged to set and explain minimum secure-password standards for user accounts.

The requirement of a birthday for setting up an account is a contentious one. While some sites asked for birthdate, LiveJournal's account set-up had a sidebar that explained not only that birthdate was required by law, but informed the user that by default the site would only display day/month of birthdate for some added security. Similarly, LinkedIn's registration process required a zip/postal code, but a sidebar explained that only a region code would be visible – again, a useful way to collect needed information at registration while still limiting the public visibility of potentially personally identifiable information. Sites should consider at least including an explanation that birthdate collection is mandated by law, as well as potentially instituting a separation between registration and profile information such that the provision of birthdate for registration would not automatically result in the birthdate being part of the profile unless the user opted to do so by providing that information a second time at the profile stage.

Recommendation 5: Sites should institute a clear distinction between information required for registration and profile information. Information collected for registration purposes should not automatically appear on the profile unless the user chooses to add that information to the profile.

Recommendation 6: Wherever possible, sites should consider developing codes that allow the user to locate herself geographically without providing explicit personal information such as ZIP/Postal codes.

Settings

Jones & Soltren recommend that sites seek to merge the provision of profile information with privacy settings. Of all the sites surveyed, Hi5 is the only one that displays any aspect of this – a sidebar at the time of information provision allows the user to select who can see each piece of information (except first name, language, ethnicity and about me) from amongst "everyone can see this", "my friends can see this" and "no-one can see this". Although this will be discussed further in the section on privacy controls, sites should consider wherever possible mapping the privacy settings on to the original information provision, thus making the decisions both accessible and meaningful to the user.

Recommendation 7: Sites should consider wherever possible mapping the privacy settings on to the original information provision, thus making the decisions both accessible and meaningful to the user.

Real Identities v Pseudonyms

The Rome Memorandum recommends that providers "[i]ntroduce the creation and use of pseudonymous profiles as an option, and encourage its use."[126] The sites surveyed employed a range of strategies on this. While Facebook and Hi5 did not allow for the use of either pseudonyms or the limiting of information, LinkedIn gave users the option to display only the first name and the first initial of the last name, MySpace required the provision of a first and last name but allowed users to opt to display only a "display name" pseudonym, and LiveJournal and Skyrock both focussed on the pseudonym, with LiveJournal requiring only a pseudonym for registration, while Skyrock asked for a username but allowed the user to provide a first and last name as well if they so chose.

Recommendation 8: At a minimum, users should have the option to provide and use pseudonyms for their SNS account.

Privacy Controls

The UK Office of Communications report notes that in their review of attitudes, behaviours and use of social networks, "[t]here was an assumption that the social networking site had taken care of any privacy and safety issues."[127] In looking at this issue, therefore, it is important to consider not only whether or not there are privacy controls available to the user, but also how accessible they are, the default settings, and what level of informational self-determination they provide the user.

Hewitt & Forte's study indicated that "[s]tudents who raised privacy concerns seemed to be either unaware of privacy options offered of the site (such as creating special, limited profiles for viewing by specific users) or the design on these privacy features did not conform with the expectations and experiences of privacy they brought to the site."[128] Again, it is important then to ensure that privacy controls may be easily mapped on to user's understanding and use of the site.

Default Settings

Research shows that "users tend not to change default settings."[129] As such, the default settings are an important area of consideration. Given this, ENISA recommends that that appropriate defaults be set.[130] Obviously sites will need to balance the privacy interests of users with the desire of users to obtain the most functionality from the site as well as the site's own interest in data collection, both to meet the needs of users and to support a model which is financed by advertising. However, at a minimum it is suggested that privacy should be opt-out, rather than opt-in,[131] and accordingly that sites may wish to err on the side of privacy while providing users the ability to actively increase the levels of information sharing and visibility if they so desire.

Recommendation 9: Default settings should protect privacy rather than presume information sharing.

Recommendation 10: Language is important. Users should be given the option to opt-in to increased information sharing, rather than positioned as "opting-out" of privacy.

Integrating Privacy

On the sites reviewed here, the sites that did have privacy controls primarily offered them as a separate action, one that the user needed to seek out in order to access.

ENISA recommends that "SNS's themselves should, where possible, use contextual information to educate people in real time."[132] Similarly, the Rome Memorandum remarks (about privacy controls) that "[e]ven if this

information is displayed on the screen when a user signs up for a service, and can also be accessed later if the user so wishes, the goal to inform users about potential consequences of their actions during the use of a service...may be better served by built-in, context-sensitive features that would deliver the appropriate information based on user actions."[133]

As previously mentioned, Hi5 links privacy controls with the registration and profile-building process – at the time the information is originally collected, the user is able to select levels of privacy for the information. There is, of course, the ability to return to the privacy settings and change them later, as well as to exert further controls on information through this tab. Nevertheless, the simple strategy of tying privacy settings to the information when it is provided is a good one that is recommended to all sites.

Recommendation 11: Sites should consider wherever possible mapping the privacy settings on to the original information provision, thus making the decisions both accessible and meaningful to the user.

LiveJournal is the other site surveyed that had a novel approach to integrating privacy control in the user experience of the site. LiveJournal allows users to set privacy controls to the journal as a whole, as well as to set them for each entry, choosing to make an item visible to all users, visible to friends only, or visible only to the author. LiveJournal also allows the creation of communities, where posts within a community will be in that community rather than on the individual user's journal, and may be friends-locked to further reduce visibility if so desired. Allowing users to select privacy levels on an entry-by-entry basis makes them engaged and active partners in their own privacy, and makes privacy levels meaningful in a way that one-time overarching settings may not be. While this strategy may be unwieldy in terms of "feed actions", sites might consider implementing this item-by-item integration of privacy settings into, at the very least, posted items, notes and other personal entries.

Recommendation 12: Privacy controls need not be overarching and separate settings. Where possible, sites should consider item-specific privacy settings to enhance user control of information sharing.

Marketing

The Rome Memorandum recommends that sites "[a]llow for user control over secondary use of profile and traffic data: e.g. for marketing purposes, as a minimum: opt-out for general profile data, opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data."[134] None of the Privacy Controls on the sites surveyed met this recommendation. At a minimum, privacy control tabs should include a heading for advertising which indicates clearly what information may be used for advertising purposes and (by preference) allow users to delimit the use of their personal information. Although this information may be made available in privacy policies and terms of use, it should also be clearly identified and easily available within the Privacy Controls.

Recommendation 13: Privacy settings should include a heading for advertising which clearly indicates what information may be used for advertising purposes and allows users to control the use of their personal information for these purposes.

Feeds

Facebook's Privacy Controls had extensive information available about information feeds: a list of what actions will never be included on the list; a list of applications that may provide information to the list; and a series of options that the user is able to opt-out of having published on her feed.

Recommendation 14: Sites should be encouraged to add granular controls in order to both inform the user of what information is shared through internal feeds and enable her to customize it to her desires.

Search

The ability to search within the site for other users is a key feature of these sites. Accordingly, it is important that sites incorporate privacy controls that allow the user to determine what terms s/he may be searched for by, as well as to delimit visibility in searches and select what information will be visible as a search result.

Recommendation 15: Privacy controls should allow the user to determine which information fields may be searched.

Recommendation 16: Privacy controls should allow the user to understand and select what information will be visible in a search result.

Recommendation 17: Privacy controls must allow the user to control her visibility in internal searches.

Facebook also enables the user to select what means of contact will be offered to a user who has found their profile via a search, while Hi5 allows users to shape from whom they will accept friend requests and how they may be contacted. Sites are encouraged to consider such controls.

Recommendation 18: Sites are encouraged to consider adding privacy controls to enable the user to select whether and how s/he may be contacted following an internal search.

Applications

The issue of 3d party applications will be considered in more depth later in this analysis. Nevertheless, an important aspect of privacy controls must be the user's ability to manage the sharing of her personal information with third parties.

Facebook offers opt-outs for participation in some Applications, such as Beacon and Facebook Connect, as well as offering users the ability to manage what types of their information friends will be able to see when they use non-shared Applications. However, on the question of third party

applications, Facebook's approach will only allow the user to opt-out of information sharing with Applications if s/he herself is not using any Applications. This does not, of course, address the concerns raised by many that 3d party applications gain access to personal information not only of the user who activates an application but of friends of that user as well, meaning that individuals may have their personal information shared with Applications without their knowledge or explicit consent. MySpace's privacy controls, on the other hand, permit a user to set privacy of her own information in regard to friends' use of Applications, letting the user opt to share no information, to share basic information only, or to share all public information. Sites should be encouraged to adopt the model chosen by MySpace, and in so doing allow users more privacy over the sharing of their personal information with applications.

Recommendation 19: Privacy controls should facilitate user control over the sharing of her personal information with third party applications both when she accesses those applications and when friends use the applications.

Comments & Wall Posts

As Patricia Lange points out, especially in an atmosphere of liberal (almost automatic) friending, comments and wall posts are an important part of the social process on such sites,[135] and danah boyd discusses the effect that comments by others may have on the user because of their visibility and incorporation into the user profile.[136] Given the importance of comments then as well as the way comments may reflect on the user, it is important that the user be able to apply privacy controls on both the comments themselves and their visibility. In this regard, Hi5's privacy controls were noteworthy, allowing users to delimit both who was authorized to comment and whether those comments would be automatically accepted or not, with the user needing to "accept" non-automatic acceptance comments before they appear publicly.

Recommendation 20: Users should be able to apply privacy controls to the reception and visibility of comments from other users.

Photos

Although the issue of photos will be discussed in greater detail in the next section, it is noteworthy that Hi5's privacy controls allow users to shape whether or not friends are able to tag photos they upload, and to determine whether friends may comment on photos and whether those comments will be automatically accepted or must be manually accepted before appearing.

Photo Tagging

In our review of sites, 3 of the sites (Facebook, Hi5 and MySpace) permitted the addition to photographs of metadata tags identifying users and non-users.

Currently, users may "tag" a photo. The act of tagging creates a link to the profile of the user who has been tagged. Users are made aware that they have been tagged in a photo, are able to view the photo, and may remove the tag.

Non-users of the sites may also be "tagged" in photos. In this case, the site will collect name and email address and send the non-user a link to the photo.

Consent

Both the Rome Memorandum and the ENISA recommendations addressed the issue of consent for photo tagging. The Rome Memorandum recommends that "tagging of photos...should be bound to the data subject's prior consent"[137] while ENISA recommends that sites "require consent from data subjects to include profile tags in images."[138]

None of the sites reviewed currently require consent prior to the addition of a tag to a photo. Instead, anyone with access to the photo may tag the photo and the user is informed and given the right to remove the tag after it has been created.

Recommendation 21: Sites should be encouraged to comply with the Rome Memorandum and ENISA recommendations by changing the photo tagging process, allowing viewers of a photo to posit a tag, but not creating the tag until the user who has been tagged has consented to that tag being created.

Tagging of Non-Users

The ability to tag non-users in photos is a problematic one. An individual so tagged may not be aware of the tag, and as such has no ability to control their own personal information. In addition, the current models for non-user tagging collect the email address of the non-user in order to notify her that she has been tagged. As Grimmelmann notes, "[p]eople who have chosen not to be on Facebook at all have made a clear statement of their privacy preferences and deserve to have that choice honoured."[139] In order to honour that choice, individuals who are not users of the site should not be able to have their personal information (name attached to photo) placed on the site, which would remove the need to collect their personal information (email address) in order to notify them.

Recommendation 22: Non-users should not be able to be tagged in photographs posted to the site.

Privacy Controls

Some of the sites offered limited controls over photos and tagged photos within their Privacy Controls – Facebook, for instance, allows users to select the audience who will be able to see photos of them that have been tagged.

This is not to say that sites do not offer privacy controls for photos themselves. Most of the sites that allowed photos also allowed users to apply privacy levels by photograph and by album. However, these controls

were generally linked to the photo application itself, rather than available with the rest of the privacy controls. Sites should consider centralizing privacy controls by putting photo privacy settings in with the other privacy controls.

Recommendation 23: Photo privacy settings should be included with other privacy settings to facilitate discovery and implementation of the options.

As noted previously, Hi5 does have a setting within their privacy controls that allows users to determine whether or not others will be able to tag photos that they upload.

Recommendation 24: Photos should not be taggable by default – users should have the ability to select whether or not photos may be tagged.

Sites may also wish to consider adding a privacy setting that allows users to opt-out of being tagged in photos altogether.[140]

Recommendation 25: Privacy settings should allow users to determine whether or not they wish to be tagged in photographs.

Accessibility of Information to Others

To some degree, of course, having one's profile accessible to others is a core feature of social networks – after all, if one wasn't visible, friendable, or contactable, there wouldn't be much point in being on a social network in the first place. This viewability imperative has impacts on privacy choices however. Adam N. Joinson theorizes that "[t]he surveillance and social search functions of Facebook may, in part, explain why so many Facebook users leave their privacy settings relatively open. If social searching is a public good, then reciprocity rules would dictate that by enabling a degree of surveillance of oneself, one would should [sic] also be able to engage in reciprocal surveillance of others."[141]

One answer to this potential unwillingness to actively restrict the accessibility of one's information to viewers may be found in the suggestion by Sören Preibusch et al to establish a multi-tiered understanding of data. They propose the development of 4 levels of data, ranging from "private" (which would only be available for the site's internal use, such as the email address provided on sign-up); "group" (available for the site's internal use and viewable by limited group such as a network); "community" (available for SNS internal use and accessible by all registered/logged in users, for instance user status, contact lists, profile details and profile photo); and "public" (available for SNS internal use and accessible by anyone, such as the fact that a user does have a profile on the site and user name).[142] While this hierarchy does not seem to solve the problem in its entirety, it may be a helpful way for sites to conceptualize information when setting defaults, although users should still have the ability to control accessibility of data through privacy controls.

Generally, user's information becomes available to others by one of three methods: feeds, internal search, and public search.

Feeds

The Rome Memorandum recommends that "restriction of visibility in profile information" be allowed.[143]

Monica Chew et al note that "[t]here are two fundamental ways in which lack of control over activity streams may compromise a user's privacy. First, a user may not be aware of all the events that are fed into their activity stream. Second, a user may not be aware of the audience who can see their activity stream."[144] Accordingly, they make 5 recommendations for feeds: (a) that users should be aware of what information goes onto feeds; (2) that users should have control over what information goes onto feeds; (3) that users should be explicitly aware of who the audience are for feeds; (4) users should be able to control who the audience are for feeds; and (5) developers should build applications in such a way that the creation of feed information is more in line with user expectations.[145]

Some of the sites – notably Facebook, Hi5 and MySpace – had some level of user control over what information was included in their feeds and who the audience for those feeds might be. MySpace also included a control over what type of information from friends the user would be fed. Sites should be encouraged to give users the most flexibility possible in shaping what information goes onto feeds and who has access to those feeds. Facebook's recent move to allow users to create groups and manage visibility elements this way should be encouraged.

Recommendation 26: Sites should be encouraged to provide users with the most flexibility possible in determining what information goes onto feeds and who has access to those feeds.

Internal Search

All of the 6 sites reviewed had internal search engines, allowing users to search by name or email. Some also included searchability by other profile features, such as geography, interests, relationship status etc.

Some of the sites allowed users to determine whether they were searchable (LiveJournal), who they might be searchable by (Hi5) or to limit the information visible on a search result (Facebook, LinkedIn, MySpace).

The Rome Memorandum recommends that sites allow "restriction of visibility in community search functions."[146] danah boyd writes of frequently being able to surprise interviewees who perceived their profiles to be private by demonstrating that when the user is a member of a network, other members of that network are able to view their profile.[147] Users must be given a clear understanding of visibility and the tools with which to manage that visibility. Among other issues, users must be able to choose whether to be automatically visible to extended networks.

Recommendation 27: Users must be given a clear understanding of the visibility of their profile information in searches.

Recommendation 28: Users should be given the privacy tools to manage their visibility in searches.

Recommendation 29: Automatic visibility to extended networks should not be the default setting for internal searches.

Public Search

All 6 of the sites were indexable on public search engines, and thus viewable to some extent by non-members of the site. In some cases, non-members of the site were also able to use the site itself for searches.

The Rome Memorandum recommends that "non-indexability of profiles by search engines should be a default."[148] At present this is not the case. Facebook defaults to indexability, although users have the ability to opt-out of being included. Hi5 too defaults to accessibility of profiles to public search engines, as to LiveJournal, MySpace and Skyrock. LinkedIn too has a default setting of availability, but this is less surprising given that it's focus is on professional rather than personal visibility. The ability to opt-out of public search visibility should not be sufficient – rather, sites should conform to the Rome recommendation of a default setting (that could be opted-out of at the user's desire) of non-indexability.

Recommendation 30: Non-indexability of profiles by search engines should be a default setting.

ENISA also recommends that sites "pay attention to search results: data should either be anonymized, not displayed, or the user should be clearly informed that they will appear in search results and given the choice to opt-out."[149] On most sites, a profile that is marked "private" or information that is "private" or "friends only" will not appear, or will only appear in a limited form. In addition, LiveJournal offers tools that allow users to minimize their appearance in searches, as well as the entry-by-entry security settings on entries that will prevent anything not public from appearing on a public search. LinkedIn, while defaulting to accessibility, does allow the user to control whether to appear in searches and, if so, what information should be available. Sites should be encouraged to build increased nuance into users' ability to manage the appearance of their personal information in public searches.

Recommendation 31: Users should have the ability to manage whether and what profile information appears in public searches.

Advertising

Advertising is key to the business model of most SNS. As Matthew Hodge explains, the relationship is cyclical: users are granted accounts free of charge and set up a profile using storage space on the central site computer that they can access at will. In return, the site gets "hits" and accumulates multiple users. In order to effectively advertise, marketers want to know that there is an audience and if possible to be able to target that audience effectively, a feature that is facilitated by the existence of the site and the collection and use of information by the site. Finally, when marketers purchase advertising on the site, this underwrites the provision of free accounts to users.[150] Sören Preibusch et al make a similar point, adding that this model is attractive to advertisers not only because of the ability to target, but because of the accuracy of targeting since self-reported information has a greater accuracy rate and the visibility of networks facilitates validation of targeting classifications.[151]

Transparency

The sites all acknowledge the role of advertising in supporting the site (to some degree) and are clear in privacy policies and terms of use that information is used for advertising. Nevertheless, there appears to be a disconnect between this notice and users' understanding. As Jones & Soltren note this "disclosure is certainly legal, and users are receiving the use of an extremely useful and popular site for free in exchange for it. Unfortunately, not all users understand the terms of the bargain; our survey showed that 46% of Facebook users believed that Facebook could not share their information with third parties."[152]

Recommendation 32: Sites should be encouraged to be more transparent about their relationships with advertisers, and to foreground that information when users sign up for accounts.

Clarity

Beyond facilitating an awareness of the presence and role of advertising, sites must also be clearer about the relationship between user information and their advertising sales.

The Rome Memorandum notes

> ...we will never share your personal information with third parties is an example – while this statement may be formally correct in the eyes of the service provider, some providers fail to clearly communicate the fact that e.g. for displaying advertisements in the browser windows of a user, the IP address of these users may be transmitted to another service provider delivering the content of the advertisements, in some cases based on information processed by the social network service provider from a user's profile.[153]

Although the privacy policies of each of the sites acknowledged that information would be used in some way for advertising, none of them provided a clear statement of what information would be used, nor of how it would be shared. Sites were more likely to state that they would not share particular items of personally identifiable information (name, email, etc) than to list what information could or would be shared.

Recommendation 33: Sites should be encouraged to be clearer about what information is or may be used for advertising purposes.

Aggregating Information

Many of the sites claim to create and share aggregate information to facilitate advertisement targeting. As EPIC points out, however, "...sites do not elaborate on what information they provide to advertisers in

aggregate usage information, nor do they note the potential for third parties to disaggregate the information."[154] This information should be included as part of the privacy policy.

Recommendation 34: Users should be made aware of what information is provided to advertisers in aggregate information.

LinkedIn provides an email address where users are able to request that they be excluded from aggregated data and products based on aggregated data.

It should also be noted that Hi5 states that other than name, address, email address and telephone number, they have the ability to anonymize information, and further that anonymized information is not personal information and may be used at the discretion of Hi5. Given that technological changes may mean that today's anonymized information is tomorrow's personally identifiable information, sites should be cautioned against sharing anonymized information with third parties.

Recommendation 35: Sites are encouraged to apply the highest standards of de-identification, aggregation and anonymization to personal information before sharing it with third parties.

Recommendation 36: Anonymized information in non-aggregate form should not be shared with third parties.

3d parties

Some of the sites identified their advertising partners to users. Facebook's exclusive banner advertising partner is Microsoft. LiveJournal's privacy policy includes a section listing the advertisers with whom LiveJournal is affiliated and providing URL's to enable to user's to check out the privacy policies of those companies and seek to manage their privacy with those companies. Similarly, MySpace lists an email address that users may contact in order to find out about the techniques and privacy policies of advertisers and opt-out wherever possible.

Alternatives to Advertising

The Rome Memorandum recommended that sites consider the introduction of a fee as a way of financing the service, instead of using profile data for marketing.[155] Of the sites reviewed, only LiveJournal offers this option. LiveJournal offers 6 levels of accounts, including a basic account with no advertising and limited functions, a Paid account, with no advertising and increased functionality, and a "Plus" account, where the functionality of the Paid account is supported by advertising rather than payment by the user. On the surface this option is attractive, but sites who consider it should be careful – implementing a system where those who cannot afford to pay for their privacy have none (or less) is problematic.

Opt-out

Sites like Facebook and MySpace have different ad programmes, both "direct" ads and general banner advertising. This allows them to offer users the option of opting out of the direct ads (Social Ads and Beacon for Facebook, DirectAds for MySpace), a policy which should be encouraged. The ability to opt-out of these programmes, however, should not be confused with opting out of site advertising (or the use of personal information for site advertisement targeting) altogether.

Skyrock indicates that users may only withdraw from advertising by closing their account.

Recommendation 37: Users should have the ability to opt-out of Direct advertising.

Web Beacons

LinkedIn's privacy policy notes that web beacons may be placed by some advertisers and provides an opt-out for users.

Recommendation 38: Advertising within the site should not include the use of third party web beacons or similar user monitoring.

User Input on Targeting

Grimmelmann suggests that "[b]y allowing users to better direct how their profiles are used commercially, Facebook would further users' interest in shaping their social identity."[156] Currently both LinkedIn and LiveJournal offer users some form of input into what kinds of advertising and offers most interests them. Sites should be encouraged to adopt this practice – not only does it facilitate user recognition that there will be advertising, it may also have the effect of providing more useful targeting information for advertisers, who can be sure that users are actually interested in receiving ads in a particular category.

Recommendation 39: Sites may wish to consider allowing user input into directing advertising.

Engagement Ads

On 31 January, 2009 Facebook announced the creation of a new feature: "Engagement Ads". This feature will "allow multinational companies to selectively target its members in order to research the appeal of new products. Companies will be able to pose questions to specially selected members based on such intimate details as whether they are single or married and even whether they are gay or straight."[157] Since the feature has not been rolled out yet, it is difficult to know what privacy controls Facebook will make available for this feature. Grimmelmann has remarked on "the Facebook pattern" of launching a feature first and then waiting for complaints before partially retreating.[158] It is hoped that Facebook will not follow that pattern this time, but rather will provide users with notice of the program before implementing it and give them reasonable time period to opt-out (or in) to participation. Failing this, at a minimum, participation in the program should be opt-in, and personal information should not be shared with advertisers if at all possible.

Data Retention

Obviously it is key to each of these sites that they collect and retain data, both personal information and technological information linked with the account. Rather than parse the individual policies of the 6 sites, this section will attempt to set out some of the issues associated with Privacy Policies and data retention.

Privacy Policy

For each of the 6 sites, privacy policies (or, in the case of Skyrock, the General Terms of Use into which data protection terms are incorporated) are not negotiable and signing up for the account indicates acceptance of the terms. In no case, however, did the Privacy Policy even pop-up for a clickthrough review before sign-up – at most, users had to actively check a box indicating their acceptance of Terms and Privacy Policy. Sites should be encouraged to foreground these documents.

Recommendation 40: Sites should move towards a "clickthrough" model in order to ensure that users review the policies prior to signing up for the service.

Purposes for Collection

Jones & Soltren critique the Facebook privacy policy, noting that (a) the uses for which information is collected are nonexistent and (b) the identification of the targets of potential disclosure are too broad.[159] To illustrate this, they give the example of asking users if Facebook can share your information with other companies under the terms of the policy – 47% of users were under the (mis)apprehension that Facebook could not share information.[160] Nor is this issue unique to Facebook – rather, all the privacy policies were troublingly vague about the link between each piece of information and the reason for its collection and the ways it might be used or disclosed. While understanding that these are new and ever-evolving business models, sites should strive to be as clear and detailed about the purposes for collection as possible.

Recommendation 41: Policies should identify the purposes for which personal information is collected.

Recommendation 42: Policies should be clear about what information may be disclosed, to whom and for what purposes.

Retention Period

Sites should be clear about the retention period for the data collected. While the existing policies state the information is used to provide services, it is not clear whether the information will be deleted as soon as accounts are terminated and, if not, what period data will retained for (and why) before being destroyed. Only Skyrock had a provision to this effect, stating that when an account is closed the data will be deleted or anonymized.

Recommendation 43: Policies should be clear about the period for which data collected will be retained.

In the Skyrock policy, there was a caveat that the deletion or anonymization might be deferred for up to 1 year for safety, law enforcement or judiciary purposes. Given the risks of re-identification of anonymized data, sites should not be able to anonymize and continue to use the personal information of members after the member closes an account.

Recommendation 44: Closure of an account indicates the withdrawal of consent for the use of personal information by the site. Information that is retained post-account deletion should not be used by sites.

Access

The collection and retention of personal information raises the question of access, which is addressed sparingly (if at all) in the policies of these sites. Some might argue that since the personal information is visible to the user, the right of access is met[161], but this is not necessarily the case. Indeed, since personal information is collected by technological means (cookies, IP address, browser information) as well as that provided by the user and others, a right of access could be very instructive for the user in understanding the scope of personal information collected and used by the site.

MySpace is the only site whose policies speaks to a right of access, but it is clear that the right of access and correction granted by them applies only to registration data (that required in order to sign up) and does not include other profile data that was not mandatory to provide. This is not a sufficient right of access – users should have a right of access and correction to all of their personal information collected by the site.

Recommendation 45: Users must have a right of access and correction to all of their personal information collected by the site.

Redress

Punishment should be meaningful enough to act as deterrents. Although these policies did prohibit many behaviours (spamming, data mining, spidering, use for commercial purposes), violation of the terms results only in closure of the account. As Jones & Soltren point out, simply losing the account is not sufficient penalty[162] nor in fact is it much of a deterrent since (given that only email is used to verify account set-up) it seems likely that those who lose an account could simply open a new one.

Recommendation 46: Penalties for violation of the User Agreement should be meaningful enough to act as deterrents.

Changes/Notice

Most of the privacy policies and terms of use either place responsibility for the user for remaining current on any changes to the policy or indicate that the site will post a public notice of changes to the policies. This type of blanket consent in inappropriate – consent should be understood as an active an ongoing process.[163] Accordingly notice in some form should always be provided for changes. For incidental

changes it may be sufficient to post a public notice, but for changes that meaningfully impact the terms, email or other private communication may be preferred. In addition, as EPIC notes, mere notice of the change is not enough. The changes should be explained to users, along with a detailed discussion of any specific impacts the changes will have.[164]

Recommendation 47: Absent notice of policy changes, continued use of the site should not be considered sufficient to constitute acceptance of terms.

Recommendation 48: Notice of policy changes should include an explanation of the scope and impact of the change.

As Grimmelmann points out, the initial design (or the design at time of sign-up) is what the user consents to. The rollout of new features changes the service and thus requires new consent.[165] Again, whether the notice is public or private may depend on the extent of the proposed change, but notice should certainly be provided in advance of changes taking effect.

Recommendation 49: Notice of policy changes should be provided prior to changes taking effect.

Account Deletion

Currently, at least some of the sites demonstrate a collapse of the categories of "deactivation" and "deletion" of accounts. These options should be clearly differentiated, and the implications of each decision communicated to the user before the choice is finalized.

Recommendation 50: User option to "deactivate" and "delete" accounts should be clearly distinguished from each other.

Deactivation

Users should be given the option to "deactivate" an account. Current practices have the sites indicating that when a site is deactivated, the information remains but is not available to users of the site. This retention of information should not be open ended -- a limited period for which the information will be retained should be clearly indicated, and accounts not reactivated within this period should be completely deleted.

Recommendation 51: Deactivation of an account should not result in perpetual retention of data. Limited retention periods for deactivated accounts should be set and clearly communicated to the user at the time of deactivation.

Recommendation 52: Where an account is not reactivated within the specified retention period, the account should be deleted.

Deletion

ENISA recommends that "providers should offer convenient means to delete data completely."[166] Facebook, LinkedIn and MySpace all require more than a click of a button to delete an account – Facebook and LinkedIn require the user to email the site requesting deletion (LinkedIn guarantees a response within 5 days) while MySpace allows the user to click to request cancellation, but then sends information on how to delete the account via the email address provided at registration.

Recommendation 53: Sites should offer a convenient means to delete data completely.

Concern on the part of the site that users will delete without thinking or wish to reactivate are understandable. LiveJournal informs users who wish to delete their account that the information will be saved for 30 days, then will be permanently deleted.

Partial Deletion

Skyrock allows users to delete the entire blog or simply the profile. Similarly, Facebook offers users the option of deleting on an item-by-item basis where the user does not wish to cancel the account but does with to manage the information.

Surveys

A number of the sites direct the user who wishes to delete her account to fill out a survey indicating why s/he is using, other SNS s/he uses, what the site could have done to retain their interest etc. None of these surveys was a required step for cancellation/deletion of the account. It is unclear, however, what use this information will be put to, how long it will be retained, and if it will be linked with personally identifiable information in any way.

Recommendation 54: Where survey information is collected on deletion, the information collected should not be linked to personally identifiable information of the departed user.

3d Party Applications

Of the 6 sites, 4 of them incorporate 3d party applications. By definition, these applications are not created by the site itself, instead being created under a Developer License. The sites that have 3d party applications universally provide in their Terms that they are not responsible for data actions of 3d party developers. However, it is noteworthy that the sites have created contractual relationships which place obligations on the 3d party developers, the applications are accessed through the site, and personal information is shared between the site and the application.

Recommendation 55: Sites that engage in relationships with 3d party developers must have clear contractual or other requirements binding the 3d party developers to appropriate levels of protection of personal information.

As Joinson points out, "[m]any of the applications are social in nature (e.g. comparing oneself with others, asking questions to friends, viewing people from one's neighbourhood), and often circumvent elements of the default privacy settings."[167] As such, they are objects of privacy concern.

Clarity
Sites should clearly explain the policies and procedures regarding 3d party applications, as well as clearly outlining what personal information is disclosed to 3d party developers.

Recommendation 56: Policies should be clear on what personal information is disclosed to 3d party developers.

Recommendation 57: Policies should be clear on policies and procedures regarding 3d party developers.

Controls
When a user adds a 3d party application, they are asked to agree to sharing of information. Currently, this is accomplished by means of a general statement as to what kinds of information may be shared. However "[s]ince this TOS agreement is present on every application and the majority of applications do not appear to use user personal data, the warning becomes meaningless."[168] Wherever possible, consents to information sharing required before adding an application should be application specific.

Recommendation 58: Explanations and consents to information sharing with 3d party developers should be application specific.

Recommendation 59: Prior to accessing a 3d party application, users should be required to consent to information sharing with that particular application.

Recommendation 60: Applications should not request nor collect personal information beyond that required for the individual application.

LinkedIn recognizes two types of 3d party applications, those created by Developers and those created by a sub-set of Developers that LinkedIn identifies as "Partners". Although users still add partner applications at their own risk, LinkedIn indicates that partners are to some extent verified by LinkedIn and accordingly consent to share necessary information may be deemed. This is problematic – any time personal information is being shared with 3d parties, consent should be explicit, not implied.

Recommendation 61: Consent to sharing personal information with 3d party applications must be active and explicit, not implied.

As discussed under "Privacy Controls", users should also have the ability to control sharing of their personal information with 3d party applications. Facebook offers users the ability to manage what types of their information friends will be able to see when they use non-shared Applications. Facebook does offer the possibility of opting out of sharing personal information with applications, however Facebook's approach will only allow the user to opt-out of information sharing with Applications if s/he herself is not using any Applications. This does not, of course, address the concerns raised by many that 3d party applications gain access to personal information not only of the user who activates an application but of friends of that user as well, meaning that individuals may have their personal information shared with Applications without their knowledge or explicit consent. MySpace's privacy controls, on the other hand, permit a user to set privacy of her own information in regard to friends' use of Applications, letting the user opt to share no information, to share basic information only, or to share all public information. Sites should be encouraged to adopt the model chosen by MySpace, and in so doing allow users more privacy over the sharing of their personal information with applications.

Recommendation 62: Privacy controls should allow users to control the sharing of their personal information with 3d party applications, both when they access an application and when their friends access an application.

Enforcement
Although each of the sites that incorporates 3d party applications has some form of Developer License Agreement that governs the 3d parties, the sites Terms also indicate that the site is not responsible for the 3d parties, and that user's understand that use of applications is at their own risk. Felt & Evans recommend that "privacy policies should be enforced by the platform and applied to all data that has been entrusted to the social networking site."[169]

As discussed, Facebook has recently indicated a more active stance on this issue, mentioning a more aggressive Facebook policy on monitoring 3d party application's requests for information as well as the development of an internal application validation program to ensure that only relevant data are being collected. Sites should be encouraged to pursue these kinds of approaches.

Recommendation 63: Sites should enforce the terms of their contracts with 3d party developers, especially with regard to the collection, use and retention of personal information of users.

Recommendation 64: Privacy policies should be enforced by the site and applied to all data that has been entrusted to the social networking site.

Minimization of Sharing
Felt & Evans studied 150 Facebook applications, and conclude "that nearly all applications could maintain their functionality using a limited interface that only provides access to an anonymized social graph and placeholders for user data."[170] Sites should be encouraged to explore Felt & Evans' "privacy by proxy" approach, as well as to work with developers to find strategies to reduce information sharing to the lowest levels necessary for application functionality.

MySpace's developer platform allows developers access only to publicly available information, thus any information user's designate as private is not available to the developers. This is consistent with Felt &

Evans' findings that "applications do not need the extensive personal information that is available to them. Although two-thirds of applications depend on public friend data, far fewer require access to private data."[171] As part of their commitment to minimizing data sharing with 3d party applications, sites should work with developers to limit information needed for application functionality to publicly available information wherever possible.

Recommendation 65: Sites should work with 3d party developers to reduce information sharing to the lowest levels necessary for application functionality.

Recommendation 66: Sites should work with 3d party developers to limit the information required by applications to publicly available information wherever possible.

Collection of Non-User Personal Information

Users

The Rome Memorandum recommends that providers "inform them about the do's and don'ts of how they (the users)may handle third party information contained in their profiles (e.g. when to obtain the data subject's consent before publication and about possible consequences of breaking the rules."[172] Currently, although users may be asked to confirm that they have the authority to upload information (for instance a photograph which may contain images of another person) there is no real explanation available about the reasons for caution, recommendations for best practices nor warnings about penalties.

Recommendations 67: Sites should develop and clearly provide information to users about how to manage third party information contained in their profiles.

Collection/Retention

Every one of the sites allows users to search by email address, meaning that at least potentially sites are collecting the email addresses of non-users. On sites other than LiveJournal, email addresses are also collected to invite non-users to the site. LinkedIn allows users to list non-users as contacts. Finally on Facebook, Hi5, MySpace and Skyrock users are able to tag non-users in photographs and may provide an email address when they do so. As Grimmelmann notes, "[p]eople who have chosen not to be on Facebook at all have made a clear statement of their privacy preferences and deserve to have that choice honoured."[173] Sites should take this under advisement and should not retain the personal information of non-users. Where an email address of a non-user is provided for contact purposes, sites should not retain the information.

Recommendation 68: Sites should neither collect nor retain the personal information of non-users.

Removal

Only Facebook and Hi5's policies contain information about how a non-user may contact them to request removal of their personal information. Any site that collects the personal information of non-users should make available information about how non-users can request the removal of their personal information from the site's databases.

Recommendation 69: Sites that do collect personal information of non-users should provide clear information to allow non-users to request the removal of their personal information.

Notification

Even where a non-user can request the removal of her personal information from the site, it is perhaps unreasonable that non-users should be expected to monitor SNS in order to know when their personal information may have been collected. Grimmelmann suggests that sites should "proactively offer this sort of opt-out to any non-user as soon as it acquires enough information about them (e.g. an email address or IM screen name); it should also purge from its servers any other information linked with the email address whose owner has opted-out."[174]

Recommendation 70: Where sites do collect personal information of non-users, they should pro-actively notify non-users of the existence of this information and provide them with the means to request its removal.

Recommendation 71: Where a non-user has requested the removal of her personal information, all information linked to that individual should be removed from the site.

E: CONCLUSION

Nissenbaum's central recognition was that "there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes'."[175] Accordingly, violations of the conventions and expectations of a particular context would be experienced by those within that context as privacy violations. She identified two different norms, the violation of either of which would constitute a privacy violation: the norm of appropriateness and the norm of information flow/distribution. Interestingly, examples she used in her original article map beautifully on to SNS privacy issues.

First, the norm of appropriateness – she suggests that violations of appropriateness could include "appropriating information from one situation and inserting it into another."[176]

Second, the norm of information flow – where "[c]onfidentiality is generally the default – that is, friends expect what they say to each other to be held in confidence and not arbitrarily spread to others."[177]

The privacy issues that arise in SNS often seem to come from a gap between the contextual understanding of users and the actual scope of information flow on SNS and beyond SNS. Users may feel that their personal information has been misappropriated or wrongfully distributed when it is used for advertising purposes, when it appears in public search engines, when performances they targeted at one (imagined) audience have repercussions with a larger and unexpected audience. A SNS which seeks to provide meaningful privacy controls and protections must, therefore, work to identify and understand the expectations of users. Where business models necessitate it, this may also involve working to expand the scope of their understanding by providing clear information as to the practices of the site, thus allowing the user to develop a more accurate understanding of the context in which s/he is operating.

Matthew Hodge makes an interesting point about the privateness of SNS information in the seemingly public SNS space – he suggests that it be thought of as analogous to a safety deposit box (in a public bank) or perhaps a storage locker in a (public) storage facility.[178] Thought of that way, seeking to protect privacy by insisting that users need to recognize that the safety deposit box is in a public space and thus not private or that the storage locker is in a public facility and thus not private is obviously problematic. Rather than seek to emphasize the publicness of the space, we seek instead to provide tools for privacy even within those public spaces – to create locks for doors, passwords for entry, smaller private spaces within the larger public space.

Similarly in seeking to further privacy in SNS, we need to focus on providing users with appropriate tools. Tools to understand the context in which their information exists (through increased clarity in language and policy and making sure users are aware of the entire context in which their information sharing takes place) but also tools to enable them to determine appropriate levels of sharing and to enact appropriate protections upon the information to enforce those self-determined levels.

This doesn't happen at an overarching level – rather, privacy understandings and controls must happen at a granular level and be integrated into the regular practices of those spaces in order to become meaningful.

F: FOOTNOTES

[1] danah boyd and Nicole Ellison. (2007). Social Network Sites: Definition, History, and Scholarship. JCMC, 13 (1). [Special Issue of JCMC on Social Network Sites, Eds.: danah boyd and Nicole Ellison.]

[2] boyd & Ellison supra note 1 at 2

[3] Alexa Top 100 Sites in Canada. Shows Facebook at #3, MySpace at #15, Skyrock at #44 and LiveJournal at #89.

[4] European Union (2009) Press Release: Social Networking: Commission brokers agreement among major web companies. 10 February 2009

[5] European Union (2009) Safer Social Networking: The Choice of Self-Regulation

[6] See for example Steeves, Valerie (2004). Young Canadians in a Wired World, Phase II – Trends and Recommendations. Ottawa: Media Awareness Network; Livingstone, Sonia and Magdalena Bober. (2003). UK Children Go Online: Listening to Young People's Experiences. London: Economic and Social Research Council; Livingstone, Sonia & Magdalena Bober. (2003). Children's Use of the Internet: Reflections on the Emerging Research Agenda. New Media & Society 5(2): 147-166; Livingstone & Bober (2004). UK Children Go Online: Surveying the Experiences of Young People and their Parents. London: Economic and Social Research Council ; and Sonia Livingstone (2006). Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. Computers, Phones, and the Internet: Domesticating Information Technology. Eds. Kraut, R. E., M. Brynin and S. Kiesler. New York: Oxford University Press.

[7] Adam Thierer (2007) Social Networking and Age Verification: Many Hard Questions; No Easy Solutions Progress & Freedom Foundation Progress on Point Paper No. 14.5

[8] Ralph Gross and Alessandro Acquisti. (2005). Information Revelation and Privacy in Online Social Networks. Proceedings of WPES'05 (pp. 71-80). Alexandria, VA: Association of Computing Machinery. [Gross & Acquisti] at 9

[9] Catherine Dwyer, Starr Roxanne Hiltz and Katia Passerini (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of AMCIS 2007, Keystone, CO. at 4

[10] James Grimmelmann. (in review). "Facebook and the Social Dynamics of Privacy." at 43

[11] Helen F. Nissenbaum (2004) Privacy as Contextual Integrity. Washington Law Review, Vol. 79, No. 1 at 137.

[12] Grimmelmann supra note 10 at 2

[13] Privacy International Social Network Sites and Virtual Communities 18 December 2007. Accessed 29 March 2008.

[14] danah boyd (2007) "Social Network Sites: Public, Private or What?" Knowledge Tree 13 May. Accessed 1 February 2009. http://www.danah.org/papers/KnowledgeTree.pdf

[15] Anders Albrechtlund (2008). Online Social Networking as Participatory Surveillance. First Monday 13 (3).

[16] Alessandro Acquisti & Ralph Gross (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In P. Golle & G. Danezis (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36-58). Cambridge, U.K: Robinson College, June 28-30. at 10.

[17] danah boyd (2008). Taken Out of Context: American Teen Sociality in Networked Publics. University of California-Berkeley Dissertation at 159 [boyd 2008]

[18] boyd 2008 supra note 17 at 144

[19] Susan B. Barnes (2006). A privacy paradox: Social networking in the United States. First Monday 11 (9), July 2006.

[20] Adam N. Joinson (2008). Looking at, looking up or keeping up with people? Motives and use of Facebook. SIGCHI 2008, 1027-1036.

[21] Catherine Dwyer et al supra note 9 at 2

[22] Sören Preibusch, Bettina Hoser, Seda Gürses, & Bettina Berendt. (2007). Ubiquitous social networks ? opportunities and challenges for privacy-aware user modelling. Proceedings of the Workshop on Data Mining for User Modelling at UM 2007, Corfu, Greece, June 2007 p 4.

[23] This is not to say that SNS' do not have the requisite privacy and data protection mechanisms incorporated into the sites. Rather, it seeks to recognize that the interests of the user in her privacy may not mirror those of the administrator and accordingly that this privacy analysis must go beyond existing controls to identify

what issues users are experiencing and how best to enable them to control their personal privacy.

24 Facebook Statistics

25 Crunch Base Company Profile: Facebook.com

26 Crunch Base profile supra note 25

27 Spencer E. Ante (5 August 2008) Has Facebook's Value Taken a Hit? Business Week

28 Michael Arrington (December 2008) Interview with Mark Zuckerberg Crunch Bas

29 Facebook Statistics supra note 24

30 Sharon Gaudin (26 January 2009) Internet Hits Major Milestone Surpassing 1 Billion Monthly Users ComputerWorld

31 Facebook Statistics supra note 24

32 Jeremiah Owyang (9 January 2008) Social Network Stats: Facebook, MySpace, Reunion Web Strategy by Jeremiah

33 Facebook Terms of Use

34 Facebook Privacy Controls

35 Facebook Privacy Policy

36 Facebook Privacy Controls: Social Ads

37 Facebook Statistics supra note 24

38 Facebook Statistics supra note 24

39 Facebook Advertising

40 Security analysis suggests that Facebook user opt-out of Beacon does not prevent the advertisers from collecting the information and sending it to Facebook – rather, it prevents the information, once received, from being sent to Feeds if the user has not opted in. With this control taking place at the Facebook level rather than the 3d party level, this means essentially that advertisers are collecting and transmitting to Facebook the information of all users of their sites, regardless of whether they have opted out of Beacon, deleted or deactivated their Facebook accounts, or are not and never have been Facebook users. Facebook claims that if it is unable to associate data it receives with a Facebook member, the data is deleted. The question of the collection of the data and its transmission to Facebook remains an issue, however, and the design of Beacon and the activities of those 2d parties who integrate the program onto their sites are ripe for further privacy examination. See (3 December 2007) Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking Users Who Opt Out of Are Not Logged In CA Security Advisor Research Blog.

41 Facebook Privacy Policy supra note 35

42 The standard template asks a user whether they will allow the application to: know who they are and access their information; put a box in their Facebook profile; place a link in the left-hand navigation menu of their account; publish stories in their News Feed and Mini-Feed; and place a link below the profile picture on any profile. The options are all pre-selected, though the user may de-select any of them. Failure to agree to the Application knowing who they are and accessing their information will, however, result in a notice that the Application is unable to be installed without this permission.

43 Facebook Application Terms of Use.

44 EPIC: Facebook Privacy .

45 Facebook Developer Terms of Service.

46 David George-Cosh (28 January 2009) We're Worried About Canadian Spammers: Q&A with Facebook's Privacy Chief Chris Kelly National Post.

47 Srarama Mitra (8 June 2008) Social Networking Without Boundaries: hi5 CEO Ramu Yalamanchi

48 Hi5 Timeline

49 Interview with Ramu Yalamanchi supra note 47

50 Interview with Ramu Yalamanchi supra note 47

51 Erick Schonfeld (10 December 2008) Hi5 Hopes to Make Real Coin with Virtual Gifts TechCrunch

52 Hi5 Advertise

53 Press Release (23 July 2008) Hi5 Is Fastest Growing Social Network in the World for the First Half of 2008

54 Hi5 Timeline supra note 48

55 Interview with Ramu Yalamanchi supra note 47

56 Social Media Statistics: Hi5

57 Quantcast: Hi5 Network

58 Site Analytics: Hi5.com

59 Traffic Rankings: Hi5.com

60 Hi5 FAQ: Advertising

61 Hi5 Advertise

62 Hi5 Privacy Policy

63 Hi5 Privacy Policy supra note 62

64 Hi5 Privacy Policy supra note 62

65 Hi5 Privacy Policy supra note 62

66 Hi5 Timeline supra note 48

67 Hi5 Terms of Service

68 Hi5 Developer Platform: Hi5 Platform Terms and Conditions

69 Hi5 Privacy Policy supra note 62

70 Hi5 Timeline supra note 48

71 LinkedIn User Agreement at cl. 3

72 CrunchBase LinkedIn.com Profile

73 LinkedIn Company History

74 LinkedIn Company History supra note 73

75 Alexa Traffic Rankings: LinkedIn.com

76 Site Analytics: LinkedIn.com

77 LinkedIn Demographic Data June 08

78 LinkedIn About Us

79 Joop Dorresteijn (16 July 2008) LinkedIn Introduces Targeted Advertising The Next Web.

80 The beta page for DirectAds can be found at https://www.linkedin.com/directads/start.

81 LinkedIn: Advertising: Precision Targeting

82 LinkedIn Privacy Policy

83 LinkedIn Privacy Policy supra note 82

84 LinkedIn Privacy Policy supra note 82

85 LiveJournal Our Company

86 LiveJournal Code

87 Robert Amsterdam (Dec 2007) SUP's Shenderovich Talks About LiveJournal Purchase
88 LiveJournal About Us supra note 85
89 Alexa Traffic Rankings: LiveJournal.com
90 LiveJournal Statistics
91 Quantcast Audience Profile: LiveJournal.com
92 LiveJournal FAQ #24
93 LiveJournal FAQ #262
94 Social Network Stats supra note 32
95 CrunchBase Profile: MySpace.com
96 Tom Anderson MySpace History FreeMySpace
97 MySpace Help: Is MySpace Free?
98 Erick Schonfeld (8 September 2008) TC50: MySpace CEO Chris DeWolfe Says 95% of Ad Revenues Comes From 9 Countries, Announces New Google Gears Project TechCrunch
99 Jordan McCollum (6 November 2008) MySpace Revenue Up, New Ads Up Even More Marketing Pilgrim
100 Alexa Traffic Details: MySpace.com
101 Site Analytics: MySpace.com
102 MySpace Canada Advertising
103 MySpace Termscl.1
104 MySpace FAQ: MyAds MySpace Online Advertising
105 MySpace Terms supra note 103
106 Associated Press (5 February 2008) MySpace Opens Up To Third Party Applications Marketing Mag.ca. See also Associated Press (5 February 2008) MySpace To Launch Third Party Applications CTV
107 Michael Arrington (14 September 2008) MySpace Music Already Has Revenue Locked, May Raise Outside Capital at $2 Billion Valuation TechCrunch
108 MySpace Terms supra note 103
109 MySpace Privacy Policy
110 Skyrock Terms of Service
111 Robert Andrews (26 October 2008) Skyrock.com's Sale Hampered By Crunch, Confident Will Survive "Dark Days" paidContent: UK
112 Skyrock Terms of Service supra note 110, s. 8 Legal Information
113 CrunchBase Company Profile: Skyrock.com
114 Skyrock Sale Hampered by Crunch supra note 111
115 AXA Private Equity: Investors Details Page: LBO SmallCap Investments: Skyrock
116 Robert Andrews (10 June 2008) Skyrock.com Seeking Sale To Big Telco Player, Talks Ongoing paidContent: UK
117 Alexa Traffic Details: Skyrock.com
118 Site Analytics: Skyrock.com
119 Jean Yves Chainon (20 February 2008) From Traditional to Digital: Skyrock Blogs Phenomenal Transition Editors Weblog.org
120 Skyrock Terms of Service supra note 110 at 1a.
121 From Traditional to Digital supra note 119
122 International Working Group on Data Protection in Telecommunications (3/4 March 2008) Report and Guidancenon Privacy in Social Network Services (Rome (Italy) [Rome Memorandum]
123 Barnes supra note 19
124 CAPTCHA: Telling Humans and Computers Apart Automatically
125 European Network and Information Security Agency ENISA Position Paper No. 1 (2007) Security Issues and Recommendations for Online Social Networks ed. Giles Hogben [ENISA] Recc SN.5 p 4
126 Rome Memorandum supra note 122 at 5
127 UK Office of Communications (2008) Social Networking: A Quantitative and Qualitative Research Report Into Attitudes, Behaviours and Use at 55.
128 Anne Hewitt and Andrea Forte. (2006). Crossing Boundaries: Identity Management and Student/Faculty Relationships on the Facebook. Poster presented at CSCW, Banff, Alberta at 2.
129 Ralph Gross and Alessandro Acquisti supra note 8 at 7. See also W. MacKay Triggers and Barriers to Customizing Software In Proceedings of CHI 91 ACM Press 1991 153-160.
130 ENISA supra note 125 Recc. SN.8, p 5.
131 Harvey Jones and Jose Hiram Soltren. (2005). Facebook: Threats to Privacy. MIT 6.805/STS085 at 31.
132 ENISA supra note 125 Recc. SN.1. p 4.
133 Rome Memorandum supra note 122 at 5
134 Rome Memorandum supra note 122 at 6
135 Patricia G. Lange (2007). Publicly Private and Privately Public: Social Networking on YouTube. JCMC, 13 (1). [Special Issue of JCMC on Social Network Sites, Eds.: danah boyd and Nicole Ellison.] at 6.
136 boyd 2008 supra note 17 at 165
137 Rome Memorandum supra note 122 at 6
138 ENISA supra note 125 Recc. SN.12 at 5
139 Grimmelmann supra note 10 at 46
140 Jones & Soltren supra note 131 at 34
141 Joinson supra note 20 at 2
142 Sören Preibusch et al supra note 22 at 4
143 Rome Memorandum supra note 122 at 6.
144 Monica Chew, Dirk Balfanz, and Ben Laurie. (2008). (Under)mining Privacy in Social Networks. at 11
145 Chew et al supra note 144 at 3
146 Rome Memorandum supra note 122 at 6
147 boyd 2008 supra note 17 at 161
148 Rome Memorandum supra note 122 at 6
149 ENISA supra note 125 Recc. SN. 14 at 5
150 Matthew J. Hodge (2006). The Fourth Amendment and privacy issues on the "new" internet: Facebook.com and MySpace.com. Southern Illinois University Law Journal, 31 at 118.
151 Sören Preibusch et al supra note 22 at 2.
152 Jones & Soltren supra note 131 at 23
153 Rome Memorandum supra note 122 at 6
154 EPIC Social Networking Privacy p 6.
155 Rome Memorandum supra note 122 at 6
156 Grimmelmann supra note 10 at 46
157 Rupert Neate and Rowena Mason Networking Site Cashes In On Friends: Facebook founder finally finds a way to profit from its 150m members' private data. Telegraph newspaper 31 January 2009.

158 Grimmelmann supra note 10 at 35
159 Jones & Soltren supra note 131 at 23
160 Jones & Soltren supra note 131 at 21
161 Jones & Soltren supra note 131 at 24
162 Jones & Soltren supra note 131 at 26
163 Jennifer Barrigar, Jacquelyn Burkell, Ian Kerr. (2006) Let's Not Get Psyched out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information 44 C.B.L.J. 54.
164 EPIC supra note 154 at 5
165 Grimmelmann supra note 10 at 48
166 ENISA supra note 125 Recc SN.9 at 5
167 Joinson supra note 20 at 9
168 Adrienne Felt & David Evans (2008) Privacy Protection for Social Networking APIs W2SP '08. at 3
169 Felt & Evans supra note 168 at 3
170 Felt & Evans supra note 168 at1
171 Felt & Evans supra note 168 at 4
172 Rome Memorandum supra note 122 at 5
173 Grimmelmann supra note 10 at 46
174 Grimmelmann supra note 10 at 47
175 Nissenbaum supra note 11 at 137
176 Nissenbaum supra note 11 at 140
177 Nissenbaum supra note 11 at 141
178 Hodge supra note 150 at 121