An analysis of three user studies of Web 2.0 applications reveals the most important requirements related to ethical issues. The development of features that support these requirements should be tailored to the type of application and specific community needs.

Web 2.0 applications use World Wide Web technology to enhance creativity, communication, collaboration, and the sharing of information and content. O’Reilly Media first used the term Web 2.0 in 2004 to describe a second generation of the Web based on user communities and a range of special services, such as social networking sites (SNSs), blogs, wikis, video- and photo-sharing sites, and folksonomies, that foster—each in its own way—collaboration, participation, and the easy exchange of information among users.¹

These emerging applications are changing the way we interact with others. We share our private photographs and videos on the Web—not just with family and friends, as we did a generation ago, but with the world. We use information from free Web-based encyclopedias like Wikipedia written collaboratively by volunteers. We use short postings (tweets) to inform our friends and family about what we are doing at each moment and to check the news. We discuss politics on Internet forums, instead of at the local pub or bar. We write software together with people living on the other side of the globe whom we have never met.

In addition to sharing experiences, these developments offer many new opportunities such as social networking, increased creation of user-generated content (UGC), and more community involvement and activism; but they also introduce obvious ethical dilemmas and risks. What we put on the Internet so eagerly can be misused. SNSs like MySpace may connect people, but they can also be vehicles for bullying and harassment. Exploiting personal information has generally become easier because people disclose such information more frequently without reflecting on the possible consequences.²

The standards that we as software developers should follow when developing applications are well-defined and understood. We have a moral duty to protect the public’s
welfare and the privacy of those affected by our software. We also have pragmatic reasons for doing this: People want others to treat them morally. Those who have a bad experience with an SNS might stop using it or use it less. People worried about what is going to happen to the content they put on a video-sharing site like YouTube might never start using it.

The emergence of Web 2.0 applications requires reconsideration of ethical norms governing their development and use, prompting questions such as: What kinds of problems do users of these applications experience? What do people really worry about when they provide personal information, discuss the latest news, or put their photographs on the Web? What do existing real-life communities expect from Web 2.0 applications? What should developers do to promote trust in such applications and guarantee user privacy?

**RESEARCH FOCUS**

For the past three years, we have participated in Citizen Media (www.ist-citizenmedia.org), a European research project that explores how exploiting multimedia UGC, such as photographs and video footage, in innovative ways in user communities and social networks might improve the daily lives of European citizens.

Considering ethical issues raised by the new technology was part of our research. Developers have attempted to implement ethical rules in software applications, such as designing e-mail programs that stop users from unethical behavior. We believe that people should judge what is ethical or unethical, but that the applications should support users with respect to ethical behavior. In other words, developers can promote social norms or etiquette within the Web 2.0 environment to create a basis for trust and privacy.

To investigate user concerns regarding typical Web 2.0 applications such as blogs and SNSs, we conducted one study in Norway with 200 participants and two studies in Belgium: one consisting of 30 members of two online communities and the other consisting of 50 individual participants and 85 families. The studies, outlined in Table 1, included all age groups from young people to senior citizens, all skill levels from proficient technology users to nonusers, and different types of communities from informal to well-structured. The focus was on applications targeting nonprofessional users, supporting social networking, and sharing of UGC.

Based on these studies, we identified the most important requirements of Web 2.0 applications related to trust, privacy, and etiquette. The “Key Concepts” sidebar discusses these ideas as well as the differences between ethics and laws.

**Table 1. Overview of three studies on Web 2.0 applications.**

<table>
<thead>
<tr>
<th>Study 1</th>
<th>Purpose</th>
<th>Investigate problems experienced by users of SNSs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Focus</td>
<td>Existing applications</td>
</tr>
<tr>
<td></td>
<td>Level</td>
<td>Macro</td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td>Norway</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Survey</td>
</tr>
<tr>
<td></td>
<td>Subjects</td>
<td>200 members of four SNSs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Study 2</th>
<th>Purpose</th>
<th>Investigate opinions and fears related to information and communication technology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Focus</td>
<td>Existing and future technology</td>
</tr>
<tr>
<td></td>
<td>Level</td>
<td>Individual</td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td>Belgium</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Case study; blogs and diaries used for data collection</td>
</tr>
<tr>
<td></td>
<td>Subjects</td>
<td>30 members of two online communities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Study 3</th>
<th>Purpose</th>
<th>Investigate effects of existing practices on usage of social Web 2.0 applications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Focus</td>
<td>Existing and future technology</td>
</tr>
<tr>
<td></td>
<td>Level</td>
<td>Group</td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td>Belgium</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Case study; interviews, observations, content analysis, logging, and monitoring used for data collection</td>
</tr>
<tr>
<td></td>
<td>Subjects</td>
<td>Neighborhood community consisting of 85 families and a well-structured community consisting of 50 members</td>
</tr>
</tbody>
</table>

**Table 2. Reasons for stopping using a social networking site or using it less over time.**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Number and percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of interesting people/friends using it</td>
<td>62 (24 percent)</td>
</tr>
<tr>
<td>Low-quality content</td>
<td>59 (23 percent)</td>
</tr>
<tr>
<td>Low usability</td>
<td>45 (18 percent)</td>
</tr>
<tr>
<td>Harassment/bullying</td>
<td>24 (9 percent)</td>
</tr>
<tr>
<td>Time-consuming/isolating</td>
<td>16 (6 percent)</td>
</tr>
<tr>
<td>Low trust</td>
<td>15 (6 percent)</td>
</tr>
<tr>
<td>Overcommercialized</td>
<td>15 (6 percent)</td>
</tr>
<tr>
<td>Dissatisfaction with moderators</td>
<td>3 (1 percent)</td>
</tr>
<tr>
<td>Unspecified boring</td>
<td>3 (1 percent)</td>
</tr>
<tr>
<td>Other</td>
<td>15 (6 percent)</td>
</tr>
<tr>
<td>Total</td>
<td>257 (100 percent)</td>
</tr>
</tbody>
</table>

Note: There were 200 participants in all, but 57 participants reported two reasons. Table reprinted with permission from P.B. Brandtzæg and J. Heim, “User Loyalty and Online Communities: Why Members of Online Communities Are Not Faithful,” Proc. 2nd Int’l Conf. Intelligent Technologies for Interactive Entertainment (Intetain 08), article no. 11, ICST, 2008.

**WHAT PROBLEMS DO USERS EXPERIENCE?**

To investigate user problems with Web 2.0 applications, we surveyed 200 members of four Norwegian SNSs. Table 2 shows the number and percent of reported reasons for stopping using a SNS or using it less over time. Bullying, harassment, and low trust were typical ethics-related
Ethics are standards for moral behavior of a particular group. Software engineering ethics are standards for practicing software engineering, such as the IEEE-CS/ACM “Software Engineering Code of Ethics and Professional Practice” and the more general IEEE Code of Ethics. Some of the principles address public interests and protecting the public’s privacy. Software engineers should “accept responsibility in making decisions consistent with the safety, health and welfare of the public ...” (IEEE Code of Ethics, 1st principle) and “work to develop software and related documents that respect the privacy of those who will be affected by the software” (IEEE-CS/ACM, principle 3.12).

Laws and ethics differ in several ways. Some action might be illegal but ethical, and some actions might be unethical but legal. For example, it is ethical to drive fast in an emergency situation, even if it is illegal. Lying to family and friends about income is unethical, but not illegal; lying about income to tax authorities is both unethical and illegal.

Trust is reliance on the truth of a statement or good intentions of a person or an organization. It involves a voluntary transfer of resources—physical, financial, intellectual, or temporal—from the individual or organization (trustor) to another (trustee) with no real commitment from the trustee.

Privacy is the ability of an individual or group to withdraw from society or public attention. It is freedom from disturbance or intrusion and includes the ability of an individual or a group of individuals to protect information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals but share basic common themes.

Etiquette is a code that influences expectations and social behavior. A rule of etiquette reflects often unwritten expectations and may reflect an underlying ethical code.

responses, but site overcommercialization might also be seen in this light in that this can imply financial exploitation.

Harassment/bullying was the fourth most important reason for stopping using an SNS, cited by 9 percent of participants. Several, mostly older teenage girls, reported that they had experienced sexual harassment. A typical pattern was that these girls reported sexual solicitation by older men or boys. Thirteen percent of the users in the total sample reported having had problems on sites such as penest.no (pretty) and deiligst.no (delicious). These are anonymous SNSs where mostly young girls upload quite revealing pictures of themselves. Users can rate how beautiful they are (face or body) on a scale from 1 to 10.

The following quote from a 15-year-old female illustrates both the low trust that exists when communication is anonymous and the sexual risks young people face when using Web 2.0 sites such as Habbo, a “virtual hang-out” for teens: “I used to play Habbo before…. I did not find out if the people I talked to were old or young. I therefore thought it was a huge risk that I may have talked to pedophiles.”

Study participants who suffered from harassment were mainly members of SNSs where, as a matter of site etiquette, users employ nicknames instead of their real names. This suggests that an SNS code of etiquette requiring anonymity might facilitate a more negative outcome in terms of aggression and hostility or “flaming.”

However, several SNS users experienced harassment on sites with a bad reputation for abuse. Hence, harassment may be facilitated by a certain kind of SNS that has particular community goals and policies regarding etiquette. Such harassment will cause users to have less trust in the SNS, and perhaps they will ultimately stop using it.

Our data suggests that girls between the ages of 14 and 16 are particularly vulnerable to risky behavior on such SNSs. One explanation is that young online users are less inhibited when they are anonymous because they feel safer than if their identity is known. At the same time, anonymity can cause users to become frustrated and less trusting of others because they are insecure about whom they are communicating with. Is the other person pretending to be older, younger, a girl, or a boy? However, uninhibited communication and presentation might facilitate contact with harm-doers. Some young users may attract the attention of people whom they perceive to be older men looking for excitement, not because the users have disclosed personal information but because of their provocative behavior under anonymity.

In general, the level of visual and informational anonymity that a media environment provides relates to the degree to which individuals take behavioral risks and experience cyberbullying. On the other hand, studies indicate that openness regarding user identities is more likely to result in reliable content.

Due to the problems caused by anonymity, etiquette is moving in the direction of increased openness and less anonymous participation on Web 2.0 sites. Many SNSs such as Facebook allow people to be increasingly open and present themselves using their real names and pictures, while often restricting access to authorized users only.

WHAT DO USERS WORRY ABOUT?

Users require a general feeling of control about their personal information. This corresponds to the control mechanisms in different forms of mediated interaction designed to protect access to and publication of personal information.

Despite the importance of privacy, users tend not to use such settings when they are too complex or ambiguous, even when aware of the threats of online disclosures. One investigation found that college students do not give much thought to the revelation of personal data on SNSs, perhaps because they are used to providing such information in familiar surroundings (their community), and because they feel assured of the homogeneity of personal information.
Both younger and senior group members were also concerned about the privacy of those in pictures they posted or mentioned in blog comments, and always asked permission before putting this content online to share it with friends or family.

An aspect of privacy that concerned some study participants was ICT’s impact on their everyday lives, both now and in the future. One senior described getting calls on his mobile phone and being reachable everywhere as a form of harassment.

Younger group members worried about the increasing ability of people to report events to news agencies in their social circle. This feeling of trust in people the user already knows could also apply to members of other existing communities.

**WHAT DO ONLINE COMMUNITIES WANT?**

Online communities are groups of people who communicate via computer networks (SNSs, forums, games, and so on) for social, professional, educational, or other purposes. These communities may supplement or replace communication in the real world.

We conducted a study of 30 members of two online communities in Belgium. The first, Seniorennet.be, is built around a website for people more than 50 years old. In this community, the members do not have accomplished information and communication technology (ICT) skills. The second community, Pietel.be, is built around the personal blog of a young man interested in photography. The members are mostly younger people with good ICT skills.

The study participants were divided into two groups, both consisting of seniors and Pietel community members. We asked the first group to answer questions we placed on a blog, shown in Figure 1a, by posting messages and photographs. We asked the second group to report daily in provided diaries, shown in Figure 1b, on similar topics—for example, “Which channels (e-mail, chat, telephone, mobile phone) have you used, why, and with whom?”—for one week.

**Privacy**

An important issue for all the study participants was privacy. When sharing pictures on popular SNSs such as Flickr, the younger participants used the available privacy options. The seniors relied on more traditional ways to protect their content: They did not post pictures but showed them at their homes or at those of family or friends; they also e-mailed pictures to select people. Interestingly, one younger participant took others’ skills into account when choosing how to share his pictures—he put them online for the more experienced friends and family but e-mailed the photos to the less experienced.
or just post them online, instantly, using various media including text, audio, pictures, and video. The majority said that they would never participate in such activities, which could constitute a breach of privacy. For example, if they witnessed a car crash, they would regard putting pictures of the accident online to be a violation of the victim’s privacy. However, they would consider giving the photos to the authorities to help them in their investigation.

Trust

The issue of citizen journalism also raised ethical questions. One study participant thought that using different independent sources, which would be the case if several nonprofessional journalists were to report events, would result in more balanced newsgathering. Another worried that the public might be misinformed if just one person reported on an event, especially if that person was not a professional journalist.

Public welfare

Study participants were also troubled about the effects of new ICT on public welfare. Several senior group members worried about accessibility: They said that new technologies are being developed all the time but that some people cannot benefit due to lack of money or skills.

Many participants reported concerns about technology use and exploitation due to the fact that

- an increasing number of devices are used, each requiring more energy; and
- the devices require constant updates and provisioning of novel power cables, chargers, and adapters, which become more difficult to handle and reuse.

These issues are ecological and therefore relate to ethics. Users expect future technology to be green—to consume energy more efficiently and accommodate energy-related interactions as well as reuse of old technology.

WHAT DO OFFLINE COMMUNITIES WANT?

Offline communities are groups of people who know each other in the real world. To investigate whether and how the existing dynamics and practices of these communities influence the usage and experience of social Web 2.0 applications, we conducted a study of two such communities. More specifically, we wanted to identify “the requirements that are extracted from the social background and everyday life of people, with an emphasis on groups or communities and the social relations and practices.”

The two communities differ strongly in hierarchical structure, nature, and members’ commitment level. The first, a neighborhood committee consisting of 85 families with children, has an informal structure without any executive board and each member is equal in terms of participation. The second community consists of about 50 gay males in their forties and fifties, and is well-structured with a chairman and an executive board with clearly defined responsibilities. This community has a small group of very active members (both in the organization and in terms of participation in events) and a larger group of less committed members.

We equipped the study participants with technology resembling that under development. We set up a dedicated online platform for each community using Ning (www.ning.com) and provided the members with various devices, such as digital still cameras, to generate and share content. Figure 2 shows the website for the gay community. The participants could use the devices in, and access their community site from, their home environment for three months. During this period, we conducted interviews, managed focus groups, made observations, and performed content analysis, logging, and monitoring.
We found similar requirements related to privacy and trust in both informal and structured communities. However, the context of these requirements was different due to the communities’ nature. Different approaches thus may be needed when integrating these requirements during the development and implementation of applications and services.

**Levels of trust**

The study revealed that access to a social media application is an important issue to both communities. For example, members should be able to protect the community by giving access only to other members. Our participants described two factors that pertain to trust: technology and community. These factors respectively correspond to two different levels of trust, system trust and interpersonal trust.12 System trust requires that users have sufficient trust in both technology in general—if people do not trust the Internet they will not use it—and in specific technological applications, such as an SNS. When community members lack basic trust in technology, they probably will not be persuaded to upload personal content, no matter what privacy measures are in place. One structured community member observed, “I would not overestimate the security of the Ning site. Of no website at all, actually. But because I would not put anything on a website that others should not see, I am not too worried.”

Interpersonal trust requires that people have trust in their community, and in this case we noticed a difference between the two communities. The structured community places trust in the executive board or in those people who it specifically appoints as gatekeepers. In the informal community, individual members trust one another when granting access to the community site. Here, a distributed system that enables the participants to invite other users without central authorization works well because there is a strong level of trust among everyone. This is grounded in the sense of community that the members share.

**Privacy**

The extent to which the community members trusted their website also determined how they dealt with uploading private, personal content on an SNS. Through the website’s restricted access, users gained confidence to share more personal information than on an SNS with more open access. “On this website, I would put much more personal stuff than on a website that everyone could watch,” commented a female member of the informal community in her thirties. This (restricted access) is important to me, especially concerning the kids.”

Yet given restricted access, people remain aware of what type of content they want to share, as well as with whom they want to share it. However, if the available privacy settings seem too difficult, users are inclined not to use them even if they acknowledge the possible transgression of their privacy.13 This became especially clear in the structured community. Although members expressed the need for private chat, they did not use the corresponding “friends function” of the application because the settings were unclear.

The two communities differed with respect to the type of content users were willing to share. Structured community members shared content primarily related to the community itself—for example, pictures of and comments on community activities. In contrast, informal community members posted more personal content concerning their hobbies and children.

**System trust requires that users have sufficient trust in both technology in general and in specific technological applications.**

Community site users found it important to have control of how and with whom they shared every element of personal information. This is in line with the common social interaction patterns of face-to-face communication: Some information is meant for everyone in a community, while other information is meant to be shared only with a selected member or members. This control was important not only to members who actively uploaded content but also to those who browsed the site passively. “Someone left a love letter for his partner on the homepage,” noted one structured community member. “That is really not what I’m waiting for.”

**Transparency**

The study participants wanted social media applications to be transparent in two ways.

First, they wanted to know about the online activities of people using the community website. Such knowledge fosters trust in the application, other members, and the community itself. Knowledge about the site content’s origin is also important. For example, it should be clear whether advertisements come from inside or outside the community. A male member of the informal community in his fifties said, “The advertising, the moment you click on it, you go from one site to another, and before you know, well, they might ask if you are 18 but on the Internet we are all 18, aren’t we?”

Second, the application itself should be transparent with respect to the presentation of personal content. For example, it should be clear which messages or comments on the website everyone can see and which are viewable only by the specific persons addressed. Without this...
A lack of identity may turn online activity into a major risk and may also engender low degrees of trust among SNS members. The level of harassment and low trust experienced in social networking environments may decrease if developers try to create SNSs where it is part of the code of etiquette for members to disclose their real names or to identify themselves with more openness, such as on Facebook.

This suggestion runs counter to traditional advice with regard to privacy and safety issues. For example, children are discouraged from publishing personal information about themselves online as a protective tool against invasion of their privacy (see www.safekids.com). However, this strategy might also do children a bad turn, in that they may become subject to increased sexual solicitation. The challenge is therefore to simultaneously ensure privacy and promote norms for openness in regard to identity.

Anonymity has its place in certain kinds of speech and dialogue. However, it may also have unwanted consequences: Anonymity might reduce the quality of communication, put both children and adults at increased risk of harassment, and result in members of an SNS having less trust in the site itself and other members.

User control of content

Web 2.0 applications should put users in control of all of the actions they can perform and all the content they generate, including photos, video, text, and comments. Users should feel that they control how and to whom they are distributing content, and be sure that nothing untoward can happen. For example, users should be able to delete their comments on an issue if they want to. Another example is functionality ensuring that users cannot show private photos to unauthorized people by mistake.

Green technology

Reducing the complexity and sheer size of Web 2.0 software, and the tendency of some software’s performance to degrade, is one way to adopt a more ecological approach. Developers should avoid including functions and features that are rarely, if ever, used. Such approaches might also have other beneficial effects, such as increasing ease-of-use and trust of the application.

Public welfare

When developing new Web 2.0 technologies, designers and developers should do their best to make them readily accessible to everybody by providing simple and easy-to-learn solutions. Hardware developers should minimize the energy consumption of the devices used with such applications.
T he ability to generalize the findings of a case study beyond the immediate community, neighborhood, or company under investigation has often been questioned. To alleviate this problem, we combined our case studies with a survey. Further, our studies combined several data collection methods and included different age groups, skill levels, and community types. Our findings are, however, limited to the applications and contexts we investigated. We therefore encourage other researchers to replicate our studies and thus extend knowledge of the user requirements for Web 2.0 applications.

Acknowledgments

We thank the Citizen Media partners for their contribution to this research. We are grateful to the participants in our studies, as well as the reviewers, for their constructive comments and Chris Wright for proofreading the article. This research received funding from the European Community’s Sixth Framework Programme under contract Citizen Media, 038312.

References


Amela Karahasanovic is a research scientist at SINTEF ICT, Oslo, Norway, and an adjunct associate professor at the University of Oslo. Her research interests include modeling user requirements and usability evaluation. Karahasanovic received a PhD in computer science at the University of Oslo. Contact her at amela@sintef.no.

Petter Bae Brandtzæg is a research scientist at SINTEF ICT and a PhD candidate at the University of Oslo. His research interests include social media, user behavior, and privacy issues. Brandtzæg received an MS in psychology at the Norwegian University of Science and Technology, Trondheim, Norway. He is a member of ECREA and the ACM. Contact him at petter.b.brandtzag@sintef.no.

Jeroen Vanattenhoven is a researcher at IBBT-CUO, Katholieke Universiteit Leuven, Leuven, Belgium. His research interests include user experience of games and communication of user research toward system design. Vanattenhoven received an MS in industrial engineering electronics—ICT at Group T, Leuven, Belgium. Contact him at jeroen.vanattenhoven@soc.kuleuven.be.

Bram Lievens is a senior researcher at IBBT-SMIT, Vrije Universiteit Brussel (VUB), Brussels, Belgium. His research interests include domestication research and living labs related to new and emerging technologies, mobile services and applications, and open innovation in ICT. Lievens received an MS in communication science at VUB. Contact him at bram.lievens@vub.ac.be.

Karen Torben Nielsen is a scientific researcher at IBBT-SMIT, VUB. Her research interests include user and community research and social requirements for ICT. Torben Nielsen received an MS in cultural sciences at Universiteit Maastricht, Maastricht, the Netherlands, and an MS in journalism at Erasmusshogeschool Brussel, Brussels, Belgium. Contact her at karen.torben.nielsen@vub.ac.be.

Jo Pierson is a senior researcher at IBBT-SMIT and a professor in the Department of Communication Studies, VUB. His research interests include the meaning and use of media, digital media marketing, and user involvement in the development process based on ethnographic and living lab studies. Pierson received a PhD in social science at VUB. Contact him at jo.pierson@vub.ac.be.