Elektrotehniški vestnik 77(1): 5-12, 2010
Electrotechnical Review: Ljubljana, Slovenija

User Created Content Privacy or Big Brother Is Watching You

Sara Stančin, Sašo Tomažič

Faculty of Electrical Engineering, University of Ljubljana
E-mail: sara.stancin@fe.uni-lj.si

Abstract. In the last couple of years, the diversity of online cultures on the Internet is being enriched for a phenomenon called "user-created content". Individuals are publicly sharing their thoughts, preferences, experiences, and feelings in the form of up-to-date online profiles and journals of their lives. Freedom of individual expression and the potential for unlimited participation in producing and publishing contents is leading to an immense user information flow and data-collection. Ingenious exposition of privacy and identity publicly enables user monitoring and surveillance. Monitoring performed by users, accompanied by user mutuality, empowering, and sharing, is considered to be useful, as it is fundamentally social, and can be part of subjectivity building. The opposite case however, when monitoring lacks the voluntary engagement of each participant, is much alike Orwellian Big Brother since privacy infringements can arise. The amount of available personal information makes "user-created content" services very useful to businesses for marketing purposes, to governments for law enforcement use, and to organizations or individuals involved in illegal activities and frauds. The possible privacy intrusions are not greatly recognized by users. While UCC users desire social connections and interaction, they are also naively and innocently inviting unknown individuals into relative intimacy.

Keywords: User-Created Content, Privacy, User Data Collection, Monitoring, Surveillance

Uporabniško ustvarjena vsebina ali nadzor zasebnosti

Povzetek. Fenomen uporabniško ustvarjenih vsebin je v zadnjih letih obogatil raznolikost spletnih kultur. Z dnevnim ažuriranjem svojih osebnih profilov in dnevnikov posamezniki javno izražajo svoje misli, želje, izkušnje in čustva. Svoboda izražanja misli in tehnične možnosti skupaj omogočajo neomejen proces nastajanja in objavljanja uporabnikovih vsebin, kar vzporedno ustvarja velik pretok podatkov in nastajanje velikih podatkovnih zbirk. Tovrstno izpostavljanje lastne zasebnosti in identitete na spletu daje širok prostor in možnosti za spremljanje in nadzor posameznika. Tak nadzor, ki si ga medsebojno dovoljujejo in ga vzajemno izvajajo uporabniki, se na splošno šteje za individualno in družbeno koristnega, saj krepi socializacijo in gradi uporabnikov nazor. Vendar, kadar uporabnik eksplicitno ne dovoljuje nadzora ali se ga celo ne zaveda, postane ta nadzor vse preveč podoben Orwellovemu Velikemu bratu saj lahko prihaja do nezaželenih posegov v uporabnikovo zasebnost. Zajeten obseg razpoložljivih osebnih podatkov, ki izvirajo iz uporabniško ustvarjene vsebine, lahko izkoriščajo različni poslovni subjekti v tržne namene, vlade pri izvajanju pravnih predpisov in različne protipravne združbe ali posamezniki za prevare in druge protipravne dejavnosti. Uporabniki se pri tem v veliki meri ne zavedajo nevarnosti posegov v svojo zasebnost, ki izhaja iz javnega objavljanja lastnih osebnih vsebin. Iz želje po vzpostavljanju socialnih stikov uporabniki lahkomiselno vabijo neznane in nepreverjene osebe v svoj razmeroma intimni svet.

Prejet 17. november,2009
Odobren 14. december,2009

Ključne besede: uporabniško ustvarjena vsebina, zasebnost, zbiranje uporabniških podatkov, nadzor

1 Introduction

The ongoing growth of the Internet has influenced the modern society and human lives in many ways. One of the greatly recognized influences is the one the Internet has had on the ways people communicate with each other and on the ways people socialize in general. By going online, people can be in contact and interact with a variety of other online individuals. With forming diverse online cultures, the Internet as a network and as an interactive medium, brings together a wide range of different people who might have otherwise never met.

In the last couple of years, the diversity of online cultures is being enriched for a phenomenon called *user-created content* (UCC). Media content creation and free web publishing by people for whom such activities are not common in their professional lives have so become an integral part of online cultures. Individuals who usually do not have the knowledge and the equipment, and sometimes not even the talent, of their professional counterparts are intensively trying to express themselves publicly in various ways. A large and growing share of the society is spending more time and attention on UCC sites than on other channels and media.

Creating and, without prior editorship, directly publishing content enables producing applicable services. By using new technology, individuals have the opportu-

nity to satisfy their needs for social connections, individual expression and the desire to distinguish oneself among the rest of the community. By creating media content such as pictures and videos, and writing intriguing and penetrating texts, they interact with one another and present themselves as active observers of the society that surrounds them. Different charity and other benevolent actions initialized and performed through UCC web sites have also pointed out how efficiently critical masses can be mobilized and consequently, the positive impact these services can have on society.

Exposing oneself to the public has become a lifestyle of individuals actively participating in UCC. Participators in this phenomenon are reveling for everybody to see their names, hobbies, political and religious beliefs and other socializing intended information, which is undoubtedly not something that was done before. Unfortunately, along with recognized benefits individuals and the community can have with the growth of the UCC phenomenon, this kind of user participation and behavior is at the same time producing different privacy concerns.

According to [1] Internet privacy can in general be defined as a seclusion and freedom from unauthorized intrusion. The key word in the definition is "unauthorized" as it marks the beginning of privacy infringement. The Internet enables different means for privacy infringement. Personal user data can be collected for different mal-purposes like creating false identity, performing targeted web advertising, or sending spam e-mail, to name just some of them. With mass user media content creation and publishing, the amount of personal and impersonal data that is accessible on the Internet is increasing and user privacy on the Internet is even at bigger risk than before.

However, privacy issues concerning UCC are somehow different than the common Internet related privacy concerns. As UCC services are built on the idea of sharing information and different self-created media content, the content that is publicly available is published by individual's free will. UCC participators are deliberately publishing their personal information, their pictures, videos and other content in order to attract as many people as possible. Implementing different access constraints would extinguish the UCC purpose and benefits. Because of the UCC nature, the amount and way this content is being published, the known Privacy Enhancing Techniques (PET) are typically neither useful nor adequate.

To examine the exposed privacy issues, we observed three services that represent a specific content category: video-sharing, photo-sharing, and social networking services. We also observed what kind of content users are voluntarily publishing and what kind of data they are unknowingly and thus involuntarily providing.

It is of great concern to whom user content and data are accessible and for what purpose. UCC service deployments provide the use of identifiable information which a user provides to one entity for one purpose on to another entity for another purpose. Other purposes include compositions of digital dossiers, search and sales. Possible privacy attacks include user manipulation, blackmailing, stalking and identity theft. Some accessible technologies retrieve information from pictures alone (Face Recognition and Content-based Image Retrieval) and in that way the possibilities of potential privacy intrusions are increased.

The prevalence of monitoring and profiling practices – regardless of their intentions – is indicative of a surveillance society in which institutions gain power over individuals. In such a context, privacy is highly valued as an expression and a safeguard of personal dignity. Privacy is among the highest of privileged individual rights.

The main questions of interest are:

- What are the actual problems of sharing too much information?
- If user privacy is becoming more at risk with UCC participation, who and how can benefit from UCC services?
- How informed and concerned are the users about the possible negative consequences?

What we do is influenced by who else knows what we're doing. Our concern comes from the following question: would UCC users behave differently if they knew who else knows what they are doing?

The paper is organized as follows. Section 2 provides for the general presentation of UCC, the belonging services and the ways user can participate. Section 3 deals with the problem of user privacy that is associated with UCC. Section 4 presents the content that users are making available while Section 5 summarizes the privacy policies of the three representative UCC services that were taken into consideration. Privacy policies of UCC services give an insight into how providers of these services can use the content provided by their users. Special attention is given to privacy risks that can arise from these policies. Finally, Section 6 presents who and how can collect data from UCC services and web sites.

During our research, we especially considered previously accomplished research reported in [2], [3], [4], and [5]. The discussed issues partially involve the social impacts and drivers, and therefore we considered studies [6], [7] and [8], which approach the topic from the social science perspective. Additional technical aspects of UCC privacy intrusions will be attended in our further research.

2 User-Created Content

User-created content (UCC) definition provided by the Organization for Economic Co-operation and Development (OECD) understands media content to be justifiably named UCC, if it can be characterized by all of the following three criteria: a publication requirement, creative effort, and creation outside of professional routines and practices [2]. Media content that is considered to fulfill the OECD's three criteria can be any of the following expression formats: text, still picture, audio or video. Created content of different formats can be diffused as one of the following: blogging, multimedia sharing, podcasting, news, reviews, wikis, social networking and virtual worlds.

Until 2005, the only indications of UCC activities were chat rooms, rating sites, blogs, newsgroups and forums. Since 2005, when the first concrete UCC services such as YouTube were launched [9] and the first UCC pilot projects such as the BBC (The British Broadcasting Corporation) user-created news pilot started [10], UCC has gained surprisingly extensive popularity and a large number of individual and collective devotees [2], [3].

The observed UCC services include YouTube, Flickr, and Facebook. YouTube and Flickr are the most popular service that host user-created videos and photos respectively. YouTube, which is now operated as a subsidiary of Google, is also the world's largest UCC website. All YouTube content is publicly available while for Flickr 20% of content is publicly unavailable [2]. As users of these services do not only share content with friends, family and like-minded people, social motivators for expressing oneself and actively participating in society, such as connecting with peers to make social bonds with other people, can therefore be overbalanced by the desire to attract attention and in some cases even to achieve a certain level of fame, notoriety or prestige. Talented individuals, such as the author who created and posted an authentic commercial for i-Pod on YouTube, can be discovered [11].

Facebook is a social networking site (SNS), primarily founded for social interaction among college students that now allows the wider public to be members and integrates multiple functions. Members are provided with tools for sharing pictures, personal information and participating in numerous Facebook-specific applications. Facebook members can join different groups and also make social connections with (in real life known or unknown) individuals who, after confirmation, become their Facebook friends.

In principle, members of all three observed UCC services are able to establish social relations with other users. These relations represent, on average, weaker ties than in offline social networks. Social studies such as [6] emphasize the strength of weak social ties: "… individuals with few weak ties will be deprived of information from distance parts of the social system and will be confined to the provincial news and views of their close friends." This is also applicable to UCC social bonds, where users tend to attain a vast number of such weak ties.

Practicability of user-created content services depends upon the number of the involved participants: more users are participating in a particular service, the more valuable and useful the service is to each participant. For this reason services are not financially restricting publishing of user-created media content. The fragile business models lead different critics of UCC services to thinking that there is more to these services than it is apparent and revealed: "What is providing for sustenance of UCC services if most if not all of them are provided to users without any charge?"

3 User Privacy

With providing enriched means of communication, UCC services enable users to express themselves in various ways. However, releasing UCC services into society also has some other, broader implications. Freedom of individual expression and the potential for unlimited participation in producing UCC content is leading to an immense user information flow and data-collection. Along with personal information, photos, and videos, UCC users are publicly sharing their thoughts, preferences, experiences, and feelings in the form of up-to-date online user profiles and journals of their lives.

The large amount of freely accessible user information provides foundations for peer-to-peer monitoring, a form of surveillance performed by individuals, rather than by agents of public or private institutions. This kind of monitoring does not have the same negative connotation as the conventional understanding of surveillance, because UCC users are willingly providing such information with the intent of availability to other people. Discussion reported in [7] argues that "…individuals are increasingly adopting practices associated with marketing and law-enforcement to gain information about friends, family members and prospective love interests" and emphasizes that "…in an age in which everyone is to be considered potentially suspect, all are simultaneously urged to become spies."

Users participating in UCC sites and services typically do not mind that they can be under surveillance and monitored as long as this is performed by other members of the online community, which are similarly participating in personal information disclosure. When this kind of monitoring is performed by SNS members, and is accompanied by user mutuality, empowering, and sharing, it is considered to be useful, as it is fundamentally social, and can be part of the building of subjectivity, as reported in [8].

Exposing oneself to the public therefore "by itself" does not inherently imply privacy violation. However,

when peer monitoring lacks the voluntary engagement of each participant, it becomes surveillance in Orwellian sense and is undesirable, since different privacy intrusions can arise. As UCC participators might not be fully aware who has access to their personal information, they might also not be aware that different data regarding what they do or say online can be collected and that records of their personal information along with their online behavior can be composed. In such cases, while UCC users desire social connections and interaction, they are also naively and innocently inviting unknown and unverified individuals into relative intimacy.

Additional privacy violations arise because UCC users are making publicly available content that does not regard them alone, but represents some acquainted or unacquainted individuals who do not have to be aware of the public availability of such content, and may not wish to make it publicly available. This can lead to various unpleasantness, inconvenience or annoyance.

Major privacy issues concerning UCC services, possibly having severe consequences, regard minors. UCC services do not support any active privacy mechanisms for authentication of unknown members or their trustworthiness – checking their age, gender, interests or any other information they provide. Considering this as well as the fact that users publish personal information, photographs and videos, child molesters and sexual predators have discovered that UCC sites can also be exploited to find victims. Different cases have been presented in [12].

One of the most controversial privacy implications associated with false identities on SNS sites was the suicide death of 13 years old Megan Meier in 2006 [13]. The mother of the Megan Meier's neighbor that Megan was no longer friends with set up a fake MySpace account, representing herself as a 16 year old male. The neighbor mother used the fake MySpace account in order to send Megan hurtful messages and to humiliate and hound her. Because of this, Megan suicide was partially attributed to bullying through the social networking website MySpace.

UCC privacy issues can partially be attributed to a basic lack of understanding and consideration of social implications of the technology itself, and a lack of advanced planning as the popularity of the sites has rapidly grown. As UCC technologies are quite new, the full impacts of their effects on society are possibly not fully understood.

4 Content Availability

The extent of privacy risks concerning UCC sites depends on the amount and the nature of the information users are making available. All three observed services typically enable their users to create and maintain individual profiles which include different personal information. Manipulating this data, users manage the way other people perceive them.

User content such as pictures of individuals, their friends and relatives, and additional information provided in user profiles (names, daily activities, etc.) that are publicly available on Flickr can be accessed without any prior authentication or limitation of a particular interested individual; an interested individual does not even require a Flickr account to view this information.

Besides user created videos, YouTube enables public access to some user published personal information like age and country and his or her video-related comments. The date when a user joined YouTube, the date when he or she last signed-in, the number of videos he or she watched, are also publicly available

Facebook and other SNSs encourage members to reveal personal information in their profiles as well as through personal photos. Analysis [4] of Facebook users' awareness of privacy issues states the following: "…not only are Facebook profiles most often personally identified, but by default they show contact information and additional data rarely available on other networks…"

Research concerning social networking website topics and Internet privacy topics performed in the United States in 2007 [5] included 205 students. Participants were approached and asked to complete anonymous questionnaires. The approximate number of user social networking "friends" was 239.41. Participants who were members of some social networking site answered questions with a »yes« or a »no«. The responses obtained, like for example that 73.6% participants allow anyone to view their profile, and that almost 10% of users include their home address as well as their phone number, imply a low privacy concern among users.

According to Reuters [14], a survey performed by the British-based insurance company Legal & General, established that people used UCC sites to connect with people who were essentially strangers. The test performed involved sending out 100 'friend' or 'follow' requests to strangers selected at random. Without any checks, 13 percent were accepted on Facebook and 92 percent on Twitter. This kind of behavior could provide potential data collectors with vital, personal information.

Moreover, the Legal & General survey included 2,092 UCC users and found nearly four in ten, or 38 percent, of people using social networking sites like Facebook or Twitter post details about holiday plans and 33 percent details of a weekend away. Coupled with the findings that an alarmingly high proportion of users are prepared to be 'friends' online with people they don't really know, this kind of behavior of UCC participators presents a serious risk to the security of people's home and contents.

Besides publishing personal information in different profiles, with which users present themselves to the

online community, users also communicate with other users and with the public by posting different media content. Information that has been once posted on different web-sites can typically not be deleted or retrieved. Users in these posts usually reveal even more about themselves, their opinions and their habits than with publishing personal information in their profiles. Thus, user posts are also very valuable for different data collectors. Further problems arise because privacy policy and terms of service of the hosting companies are due to change over time. This way, it is possible that once provided removable information cannot be removed in the future. Some providers of UCC services also distinguish between inactivating an account and deleting it. For example Facebook retains user data indefinitely when a user deactivates his or her accounts but removes it within a couple of weeks when a user deletes his or her account.

5 UCC Privacy Policies

Considering the amount of user information provided, successful UCC services are likely to have large user databases of personalized and non-personalized information. Through extensive privacy policies UCC services inform the public and address the following questions:

- What information is collected by the service provider, is it considered personal and how long is it held for?
- With whom is the information published on UCC web sites shared and under what circumstances?
- Is information obtained by the UCC service provider and provided by users augmented with data from other sources?
- What internal protections exist, if any, to prevent personal information disclosures?

Privacy policies of the three observed UCC services are available in [15], [16], and [17]. The visibility of information between observed services is variable, but according to their common privacy policies and statements, collected personal information that is not displayed publicly is protected and not sold to third parties. UCC services reserve the right to transfer personal information in the event of a transfer of ownership or sale of assets.

According to the YouTube privacy policy [15], "any personal information ... that you voluntarily disclose online (on discussion boards, in messages and chat areas, within your playback or profile pages, etc.) becomes publicly available and can be collected and used by others." According to the Facebook privacy policy [16], Facebook can use and distribute members' personal information in a non-personalized manner. The company even claims that this benefits its members, as they can receive advertising that is more likely to be of interest. Moreover, Facebook "may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile."

6 Data Collection

Different business, governments and individuals are taking advantage of the increasing technical capability of information systems to gather, process, and store consumer and citizen data. Experiences have shown that the vast amount of data available through Internet can be used to acquire knowledge about consumer preferences and citizen behaviors. Built profiles can be used for commercial purposes, for the prevention and detection of security breaches, fraud and other crimes, and for different illegal activities.

With collecting data that is provided from different user created content web sites, businesses, governments and individuals have access to even more user information than before.

6.1 Targeted advertising

Through Internet businesses can sell to and communicate with potential customers. The Internet also allows businesses to identify and learn about their customer base. By collecting information about individual behavior and interests businesses can adjust a suitable commercial model for a particular user or a group of users. This is referred to as targeted advertising and it basically includes advertising products or services for which it has somehow been established that they might be of interest to a particular customer. For example, when buying a book, the site a user is buying from typically suggests other similar books that may be of interest. Some e-mail services scan incoming e-mail messages and accordingly place advertisements relevant to the message-content scan findings.

More sophisticated methods of targeted advertising include tracking and collecting individuals' online activities, interests, preferences, and communication over time in order to compile a user record. In such a way, advertisements that are shown to people are relevant to their interests, regardless of the sites they are visiting. In practice, this is typically invisible to users and allows businesses to align their advertisements more closely to the inferred interests of their audience and consequently, spend their advertising money more effectively.

According to the privacy policies of the three observed services, personal information that is not displayed publicly is protected and not sold to third parties. However, providers have no obligation to protect other collected information. This is referred to as "secondary data" and can include usage information, length of connections, other users' profiles visited and messages sent, user behavior and tastes, etc. This information is ano-

nymous and non-personalized. Therefore, the business models of UCC services may involve selling such data to market research and other firms.

Information revealed by UCC users, like their age, gender, and location is commercially very valuable. If this information is anonymous, it can therefore be distributed to advertisers. According to their privacy policies, all three observed UCC services can target advertisements to customers who have demonstrated an interest in content related to the advertisement even if the page has nothing to do with the advertiser's product. Using secondary information, advertisers can show advertisements "that may be related to textual information, such as metadata and notes, associated with the photo you are seeing, or the search term you entered" (reported on the Flickr web site at the time of the writing). YouTube reserves the right to record and afterwards distribute information about users' usage of YouTube (viewed YouTube channels, the contacts users communicate with, the videos they watch and when they watch them, the frequency and size of data transfers, etc.). For most UCC services, the practice is to keep a viewing history of users.

How extensive this secondary data can be was made evident in July 2008, when Viacom − an American media conglomerate − won a court ruling regarding Viacom's copyrighted material that was without Viacom's permission posted by users on YouTube web sites as reported in [18]. The court ruling required YouTube to hand over 12 terabytes of data detailing the viewing habits of every user who has ever watched videos on this site. This led to concerns that the viewing habits of users could be identified through a combination of their IP addresses and login names.

Extensive polemics regarding Facebook privacy arisen in November 2007, when this UCC service launched a system called Beacon, where third-party websites could include a script enabled by Facebook on their sites, and use it to send information about the actions of Facebook users on their site to Facebook [19]. Beacon created considerable controversy soon after it was launched, due to privacy concerns [20]. Information such as purchases made and games played were published in the user's news feed, for all of his or her Facebook friends to see. Originally if no action was taken by the user, this information was automatically published. Beacon was later changed to require that any actions transmitted to the website would have to be approved by the Facebook user before being published. The controversial service, which became the target of a class action lawsuit, was finally shut down in 2009.

6.2 Official use

Willingly provided information about social relations, as well as personal information about political views, religious beliefs, sexual orientation, and preferences regarding everyday life activities is in different ways complementary to information included in different official records. As UCC services reserve the right to released personal information for law-enforcement purposes, all user-provided content and data available through UCC sites can be collected for such official use.

An insight into how misinformed users can be about the adequacy of their accounts privacy settings adjustments, can be obtained by considering the consequences the Facebook application "President Obama should be Killed" [21] had. The application itself is a demonstration of how poor privacy policies and government investigations can collide. An application survey asked whether the present USA president should be killed and offered several options for respondents. Many Facebook users were outraged, and contacted the company responsible for the application and the USA secret service. The survey was taken down, but not before several hundred people participated. The matter is still being investigated, but the issue may not just be about the person(s) who created the survey. An investigation could extend to the people who participated in the survey, as well as their Facebook network of contacts. In this case, how much information the secret service may collect and how much might be available for them to collect may leave a lot of people vulnerable to being caught up in a federal investigation related to a threat on the President's life.

6.3 Employers

Individuals who access the Internet from work should know that employers are increasingly monitoring the Internet sites that employees visit. According to the 2005 Electronic Monitoring & Surveillance Survey from the American Management Association and The ePolicy Institute [22]:

- 76% of employers monitor employees' Web site connections;
- 65% use technology to block connections to banned Web sites; and
- 55% monitor e-mail.

Considering this, saying something as obvious and seemingly innocent as "I'm bored" in a status update or a post during working hours can have dire consequences if the wrong people see it. Having in mind how users in user created content communities perceive "friends" and that they are trying to have as much friends as possible, this is very expectable and common.

Regarding employers, many companies and government offices throughout the world have disabled employees UCC access from work. According to a researched performed on 1400 USA companies having more than 100 employees [23], 54% of companies in the USA have prohibited access to Facebook and Twitter to their employees. It has been established, that with the usage of social networks, the individuals professional reputation is decreased. Using social networks, users are emphasizing their private aspects and lives while em-

ployees should have in mind that they represent the company for which they work for even outside working hours.

6.4 Illegal activities and frauds

Privacy infringements arise because identifiable information available from UCC sites is available not only to the hosting site and within the network itself but to third parties who access data without the site's direct collaboration as well. Consequently, encouraging publishing of personal information and friend identification particularity, UCC services are vulnerable to different illegal activities and frauds.

It has been shown that SNS services are especially vulnerable to "phishing" attacks. "Phishing" is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party [24]. For example, the "phisher" searches large amounts of reliable social network information for UCC user e-mail or instant messaging addresses. He then misrepresents himself to the user by sending a link to a fake website, which appears almost identical to the legitimate one and directs him to enter his sensitive information. This sensitive information can include usernames, passwords and credit card details. An experiment performed at Indiana University in 2005 [24] shows a success rate of over 70% for these attacks on social networks.

Aside from the profile information users choose to make available to their friends, friends of friends, or everyone on Facebook, the biggest security and privacy loophole could be in third-party applications. Applications like quizzes and games available to Facebook users are based on »cloud computing", which means that applications run somewhere in the "cloud" and not on the user's computer, where the "cloud" represents the unpredictable part of any network through which data passes between two end points. When users choose to access these applications, they are not only exposing all of their profile information to the third-party developer that created it, but are also surfacing their friends' profile data.

As user data and applications are stored on someone else's hardware, with »cloud computing«, users lose a degree of control over their sensitive information. The responsibility for protecting that sensitive personal information from hackers, internal breaches, and subpoenas falls into the hands of the hosting company. According to a paper concerning ethics in web development [25], increased interest in UCC applications, as well as the associated low entry costs, has created a widely distributed developer base in terms of age, education, and experience. Hence, it can no longer be assumed that innovators are classically trained, and therefore have exposure to ethical considerations involving technology. This can have many possible adverse consequences as the hosting company generally does not have the same motivation as the user to defend against disclosure of the user information.

Some companies could even willingly share sensitive data with marketing firms. Problems arise because legislation has not yet approached this matter in detail. The main question that remains unanswered is who actually owns the data, the user who provided the data or the company which is hosting it?

In 2007 Virgin Mobile (Australia) used pictures obtained from Flickr websites in their advertisement campaign. Amateur photographers licensed their work uploaded on Flickr in such a way, that it could be used by any other entity, as long as the original creator was attributed credit. Virgin Mobile upheld this restriction by printing the source, leading to the photographer's Flickr page on each of their ads. The models from the photos were not informed about the ongoing campaign, so different lawsuits like [26] are still pending at the time of writing.

7 Conclusion

With UCC, the creation, collection and processing of data has become a ubiquitous phenomenon. By collecting data that is provided from different UCC web sites, governments, businesses, and individuals have access to immense user information. The prevalence of monitoring and profiling practices, regardless of their intentions, is indicative of a surveillance society and in such a context, privacy is highly valued as an expression and a safeguard of personal dignity.

UCC services in general reserve the right to all released information provided by their users, which includes personal data as well as all other self-created and once published content for law-enforcement purposes and other official use.

According to the privacy policies of the three observed services, personal information that is not displayed publicly is protected and not sold to third parties. However, providers have no obligation to protect other collected information. Business models of UCC services may involve selling anonymous and non-personalized data to market research and other firms. UCC services are thus very useful to businesses for marketing purposes.

Extensive privacy intrusions arise because identifiable information is available not only to the UCC hosting site and within the network itself but to third parties who also access data without the site direct collaboration as well. For this reason, UCC services are also very useful to organizations or individuals involved in illegal activities and frauds.

As the users are taking advantage of the openness and decentralized nature of the UCC, they are evidently not aware of the risks. Users are deliberately publishing their personal information, their pictures, videos and other content to attract as many people as possible. An

alarmingly high proportion of users are prepared to be 'friends' online with people they don't really know. The possible dangers of sharing too much information are not greatly recognized by or are not of concern to users.

In our further research we will experimentally approach the problem of UCC privacy. We will also give attention to additional technical aspects of UCC privacy intrusions.

8 References

[1] Khosrow-Pour M., Advanced Topics in Information Resource Management; Vol. 2, Idea Group Inc, 2003 Mar., last accessed 2009 Sep. http://www.google.com/books?hl=sl&lr=&id=8eEy2ZKvlWkC&oi=fnd&pg=PA52&dq=internet+privacy+issues&ots=dX8K2s6tiy&sig=O6iLA0ZxVIk4DxMAMC8HqGpkI0I#v=onepage&q=internet%20privacy%20issues&f=false

[2] Wunsch-Vincent S., Vickery G., Participative web and user-created content: web 2.0, wikis and social networking, Organization for Economic Co-operation and Development, 2007 Apr.

[3] Cha M., Kwak H., Rodriguez P., Ahn Y., and Moon S., I Tube, You Tube, Everybody Tubes: Analyzing the World's Largest User Generated Content Video System, IMC 2007: Proceedings of Internet Measurement Conference, San Diego, California, USA, 2007.

[4] Acquisti A., Gross R., Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Lecture Notes in Computer Science, Berlin, 2006.

[5] Fogel J., Nehmad E., Internet social network communities: Risk taking, trust, and privacy concerns, Computers in human behavior; Vol. 25; Issue 1, 2009 Jan.

[6] Granovetter M.S., The strength of weak ties: A network theory revisited, Social Structure and Network Analysis, Sage, Beverly Hills, CA. 1982.

[7] Andrejevic M., The Work of Watching One Another: Lateral Surveillance, Risk, and Governance, Surveillance & Society; Vol. 2; Number 4, 2005.

[8] Albrechtslund A., Online Social Networking as Participatory Surveillance, First Monday [serial on the Internet]; Vol. 13; Number 3. 2008 Mar.

[9] Lanchester J., A bigger bang, The Guardian, 2006 Nov., last accessed 2009 Nov. http://www.guardian.co.uk/technology/2006/nov/04/news.weekendmagazine1

[10] BBC News, Coming together as a city, 2005, last accessed 2009 Nov. http://news.bbc.co.uk/2/hi/uk_news/4670099.stm

[11] The New York Times, Student's Ad Gets a Remake, and Makes the Big Time, last accessed 2009 Oct. http://www.nytimes.com/2007/10/26/business/media/26appleweb.html?_r=1

[12] CBS, MySpace: You Kids' Danger? Popular Social Networking Site Can Be Grounds For Sexual Predators, last accessed 2009 Oct. http://www.cbsnews.com/stories/2006/02/06/eveningnews/main1286130.shtml

[13] The New York Times, Vague Cyberbullying Law, 2009 Sep., last accessed 2009 Nov http://www.nytimes.com/2009/09/08/opinion/08tue2.html

[14] Reuters, Burglars using Facebook, Twitter to find targets: report, 2009 Aug., last accessed 2009 Sep. http://www.reuters.com/article/lifestyleMolt/idUSTRE57R0EC20090828

[15] YouTube Privacy Policy, 2009, last accessed 2009 Nov. http://www.youtube-nocookie.com/t/privacy

[16] Facebook Privacy Policy, 2009, last accessed 2009 Nov. http://www.facebook.com/policy.php

[17] Flickr Privacy Policy, 2009, last accessed 2009 Nov. http://info.yahoo.com/privacy/us/yahoo/flickr/details.html

[18] BBC News, Google must divulge YouTube log, 2008 Jul., last accessed 2009 Nov. http:// news.bbc.co.uk/2/hi/technology/7488009.stm

[19] The New York Times, Facebook Retreats on Online Tracking, 2007 Nov., last accessed 2009 Nov. http://www.nytimes.com/2007/11/30/technology/30face.html?_r=!

[20] Cnet news, Facebook Beacon has poked its last, 2009 Sep., last accessed 2009 Nov. http:// news.cnet.com/8301-13577_3-10357107-36.html

[21] CNN Politics, Secret Services investigating Facebook pool on Obama, 2009 Sep., last accessed 2009 Nov. http://www.nytimes.com/2007/10/26/business/media/26appleweb.html?_r=1

[22] 2005 Electronic Monitoring & Surveillance survey: Many Companies Monitoring, Recording, Videotaping and Firing Employees, Business Wire, last accessed 2009 Oct. http://findarticles.com/p/articles/mi_m0EIN/is_2005_May_18/ai_n13726103

[23] Robert Half Technology, Whistle-But don't tweet-while you work; A Majority of Companies Prohibit Social Networking on the Job, CIO Survey Reveals 2009 Oct., last accessed 2009 Oct. http://www.roberthalftechnology.com/PressRoom?id=2531

[24] Jagatic T., Johnson N., Jakobsson M., and Menczer F., Social Phishing. Communications of the ACM; Vol. 50; Issue 10, 2007 Oct.

[25] Miller S., Ethical Challenges with Web 2.0 Design, Proceedings of the Third International Conference on Internet Technologies and Applications (ITA 09), Centre for Applied Internet Research, Glyndŵr University, Wales, UK, 2009 Sep.

[26] Chang et al v. Virgin Mobile USA LLC et al. 2007 Oct., last accessed 2009 Oct. http://news.justia.com/cases/featured/texas/txndce/3:2007cv01767/171558/

Sara Stančin graduated from the Faculty of Electrical Engineering of the University of Ljubljana, Slovenia, in 2007. She is currently employed as a researcher of the National Young Researcher Scheme in the Laboratory of Communication Devices at the same faculty. Her research focuses on mobile communication systems.

Sašo Tomažič is a Full professor at the Faculty of Electrical Engineering of the University of Ljubljana. He is the Head of the Laboratory of Communication Devices and the Chair of Telecommunication Department. His work includes research in the field of signal processing, security in telecommunications, electronic commerce and information systems.