Social History of Computing and Online Social Communities

Joseph M. Kizza and Li Yang

Department of Computer Science and Engineering

The University of Tennessee-Chattanooga, Chattanooga, Tennessee, USA

Joseph-Kizza@utc.edu and Li-Yang@utc.edu

Synonyms

Social Media, Social Networks, Privacy, Crime in Online Communities, Ethics

Glossary

OSNs: Online social networks (OSNs) are social networks with underlining electronic communication infrastructure links enabling the connection of the interdependencies between the network nodes.

mOSNs: Mobile OSNs (mOSNs) are newer OSNs that can be accessed via mobile devices and can deal with the new mobile context.

IMN: Instant Messaging Network (IMN) supports real time communication between two or more individuals.

SNS: Social Networking Services (SNS)

1. Definition

It is almost unimaginable that a modern person can live a meaningful life today without a mobile device as a conduit to an online social mesh of friends. These online social "gatherings" have slowly replaced the traditional face-to-face social gatherings that make us humans. While these online ecosystems are now packed with all sorts of interesting items that keep members coming back and new ones enrolling, the basic element of "presence" which transforms into "telepresence" in the virtual gatherings of any social gathering remains the same. The history of this amazing transformation of social gatherings mimics the history of social computing, the focus of this chapter. The development of the different media of social gatherings and communication is linked with computer technology developed. In fact the nature of these social media developed in line with the computing technology. The history of social computing cannot be discussed comprehensively without talking about these online media. And these online social media cannot be justifiably discussed without investigating individual rights and how these media affect participants' individual attributes. Therefore, ethical, privacy and security issues in these ecosystems are all involved in protecting personal privacy. On the central point of ethical implications of life in the social network, unlike in the traditional network, governance is not centralized, but community based with equally shared authority and responsibility by all users. But the mechanisms are not yet defined, and where they are being defined, it is still too early to say whether they are effective. The complexity, unpredictability, and lack of central authority are further enhanced by a virtual personality, anonymity and multiple personality. These three

characteristics are at the core of the social and ethical problems in online social networks in particular and cyberspace in general; the larger and more numerous these communities become, the more urgent the ethical concerns become.

2. Introduction

Social networks are at the core of social computing! In this discussion, therefore, the history of social computing is going to be discussed through the prism of social networks and their evolution into online social ecosystems, as we have them today. So a social network is a theoretical network where each node is an individual, a group or organization that independently generates, captures and disseminates information and also serves as a relay for other members of the network. This means that individual nodes must collaborate to propagate the information in the network. The links between nodes represent relationships and social interactions between individuals, groups, organizations, or even entire societies.

The concept of social networking is not new. Sociologists and psychologists have been dealing with and analyzing social networks for generations. In fact social networks have been in existence since the beginning of man. Prehistoric man formed social networks for different reasons including security, access to food and the social wellbeing.

As Joseph Kizza [1] observes, social networks begin with an individual reaching out to another individual or group for a social relationship of sorts and it snowballs into a mesh of social relationships connecting many individuals or/and groups. In general, social networks come in all sizes and are self-organizing, complex and agile depending on the nature of relationships in its links. As they grow in size, social networks tend to acquire specific elements and traits that make them different. These traits become more apparent as the network size increases. The type of social interactions, beliefs and other traits usually limit the size of the social network. It is important to note that as the social network grows big, it tends to lose the nuances of a local system, hence if certain qualities of the network properties are needed, it is better to keep the size under control.

3. Online Social Networks (OSNs)

As computing technology developed, social networks stated evolving into online social networks. **Online social networks** (OSNs) are social networks with underlining electronic communication infrastructure links enabling the connection of the interdependencies between the network nodes. The discussion in this chapter will focus on these OSNs. In particular we will focus on two types of online social networks [1]:

- The traditional OSNs such as Facebook and MySpace. Many of these can be accessed via mobile devices without the capability of dealing with mobile content, and
- The Mobile OSNs (mOSNs) which are newer OSNs that can be accessed via mobile devices and can deal with the new mobile context.

The interdependency between nodes in the OSNs supports social network services among people as nodes. These interdependencies as relations among people participating in the network services define the type of OSNs.

3.1 Types of Online Social Networks

The growth of the OSNs over the years since the beginning of digital communication, saw them evolving through several types. Let us look at the most popular types using a historical chronology [1]:

Chat Network. The chat network was born out of the digital chatting anchored on a *chat room*. The chat room was and still is a virtual room online where people "gather" just to chat. Most chat rooms have open access policies meaning that anyone interested in chatting or just reading others' chats may enter the chat room. People can "enter" and "exit" any time during the chats. At any one time several threads of the public chats may be going on. Each individual in the chat room is given a small window on his or her communication device to enter a few lines of chat contributing to one or more of the discussion threads. This communication occurs in real time and whatever every one submits to the chat room can be seen by anyone in the chat room. Chat rooms also have a feature where a participating individual can invite another individual currently in the public chat room into a private chat room where the two can continue with limited "privacy". To be a member of the chat room you must create a user name and members of the chat room will know you by that. Frequent chatters will normally become acquaintances based on user names. Some chat room software allows users to create and upload their profiles so that users can know you more via your profile.

Although chat rooms by their own nature are public and free for all, some are monitored for specific compliance based usually on attributes like topics under discussion.

With the coming of more graphical based online services, the use of chat room is becoming less popular especially to youth.

Blog Network. Another online social network is the bloggers network. "Blogs" are nothing more than people's online journals. Avid bloggers keep diaries of daily activities. These diaries sometimes are specific on one thread of interest to the blogger or a series of random logs of events during a specific activity. Some blogs are comment on specific topics. Some bloggers have a devoted following depending on the issues.

Instant Messaging Network (IMN). The IMN support real time communication between two or more individuals. Like chat rooms, each participant in the IM must have a user name. To IM an individual, one must know that individual's username or screen name. The initiator of the IM is provided with a small window to type the message and the recipient is also provided with a similar window to reply to the message. The transcript of the interchange is kept scrolling up both users' screens. Unlike the chat room however, these exchanges of short messages are private. Like in Chat Networks, some IMN allow users to keep profiles of themselves.

Online Social Networks (OSNs). These are a combination of all the network types we have discussed above and other highly advanced online features with advanced graphics. There are several of these social networks including Facebook, Twitter, Myspace, Friendster, YouTube, Flickr, and LinkedIn. Since these networks grew out of those we have seen before, many of the features of these networks are those we have discussed in the above networks. For example, users in these networks can create profiles that include their graphics and other enclosures and upload them to their network accounts. They must have a username or screen name. Also communication, if desired, can occur in real time as if one is using chat or IM capabilities. In additional to real time, these networks also give the user the delayed and archiving features so that the users can store and search for information. Because of these additional archival and search capabilities, network administrators have fought with the issues of privacy and security of

users as we will see later in this chapter. As a way to keep users data safe, profiles can be set to a private setting, thus limiting access to private information by authorized users.

3.2 Online Social Networking Services

An online social networking service is an online service accessible via any internet enabled device with the goal of facilitating computer-mediated interaction among people who share interests, activities, backgrounds, or real-life connections. Social Networking Services (SNS) offer users functionalities for identity management (i.e. the representation of the own person e.g. in form of a profile) and enable furthermore to keep in touch with other users (and thus the administration of own contacts) [19].

Most online social network services consist of:

- User Profile management: People construct user profile in social networks for a particular group of audience or a particular task. The profile is used and managed as a social identity that they used to present to each other and analyze each other.
- Social or business links of interests: Users of social networks can search experts or peers based on difference criteria such as interest, company, or name. They can also proactively receive recommendations for contacts of interests from social networks.
- Context awareness: This helps to identify common backgrounds of users in social networks. For example, users could have common contacts, common interests, the same university, or the same company. Context awareness helps to build trust among users, which are essential for a successfully collaboration [20].
- Contact management: This combines all functionalities that manage and maintain users' personal network. Examples include tagging people, access restrictions to profile in social networks.
- Network awareness: This includes any change or update of users in one's personal network. This includes awareness of indirect communication, new feeds, and user notification.
- Exchange: This enables information sharing directly (e.g. messages) or indirectly (e.g. photos or messages via bulletin boards). Examples of exchange in social networks include messages, photo albums, etc.

Currently, the most popular online social network services fall in categories that range from friends-based, music and movie, religion, business and many other interests. In each of these categories, let us give a sample of the current services:

- General and Friends-based Social Networks
    - Facebook
    - MySpace
    - Hi4
- Movie and Music Social Networks
    - LastFM
    - Flixster
    - iLike

- Mobile Social Networks
    - Dodgeball
    - Loopt
    - Mozes
- Hobby and Special Interest Social Networks
    - ActionProfiles
    - FanIQ
- Business Social Networks
    - LinkedIn
    - XING
    - Konnects
- Reading and Books Social Networks
    - GoodReads
    - Shelfari
    - LibraryThing

3.3 The Growth of Online Social Networks

OSNs have blossomed as the internet exploded. The history and the growth of OSNs have mirrored and kept in tandem with the growth of the internet. At the infant age of the internet, computer-mediated communication services like Usenet, ARPANET, LISTSERV, bulletin board services (BBS) helped to start the growth of the current OSNs as we know them today. Let us now see how these contributed to the growth of OSNs.

BITNET was an early world leader in network communications for the research and education communities, and helped lay the groundwork for the subsequent introduction of the Internet, especially outside the US [2]. Both BITNET and Usenet, were invented around the same time in 1981 by Ira Fuchs and Greydon Freeman at the City University of New York (CUNY), were both "store-and-forward" networks were. BITNET was originally named for the phrase "Because It's There Net", later updated to "Because It's Time Net" [2]. It was originally based on IBM's VNET email system on the IBM Virtual Machine (VM) mainframe operating system. But it was later emulated on other popular operating systems like DEC VMS and Unix. What made BITNET so popular was its support of a variety of mailing lists supported by the LISTSERV software [3].

BITNET was updated in 1987 to BITNET II to provide a higher bandwidth network similar to the NSFNET. However, by 1996, it was clear that the Internet was providing a range of communication capabilities that fulfilled BITNET's roles, so CREN ended their support and the network slowly faded away[3].

Bulletin Board Services (BBS). A Bulletin Board System (BBS) is software running on a computer allowing users on computer terminals far away to login and access the system services

like uploading and downloading files and reading news and contribution of other members through emails or public bulletin boards. In "Electronic Bulletin Boards, A Case Study: The Columbia University Center for Computing Activities", Janet F. Asteroff [10] reports that the components of computer conferencing that include private conferencing facilities, electronic mail, and electronic bulletin boards started earlier than the electronic bulletin board (BBS). Asteroff writes that the concept of an electronic bulletin board began c. 1976 through ARPANET at schools such as the University of California at Berkeley, Carnegie-Mellon, and Stanford University. These electronic bulletin boards were first used in the same manner as physical bulletin boards, i.e., help wanted, items for sale, public announcements, and more. But electronic bulletin boards soon became, because of the ability of the computer to store and disseminate information to many people in text form, a forum for user debates on many subjects. In its early years, BBS connections were via telephone lines and modems. The cost of using them was high; hence they tended to be local. As the earlier form of the World Wide Web, BBS use receded as the World Wide Web grows.

LISTSERV. It started in 1986 as automatic mailing list server software which broadcast emails directed to it to all on the list. The first Listserv was conceived of by Ira Fuchs from *BITNET* and Dan Oberst from EDUCOM (later EDUCAUSE), and implemented by Ricky Hernandez also of EDUCOM, in order to support research mailing lists on the *BITNET* academic research network [4].

By the year 2000, Listserv ran on computers around the world managing more than 50 thousand lists, with more than 30 million subscribers, delivering more than 20 million messages a day over the Internet [4].

Other Online Services. As time went on and technology improved, other online services come along to supplement and always improve on the services of whatever was in use. Most of the new services were commercially driven. Most of them were moving towards and are currently on the web. These services including news, shopping, travel reservations and others were the beginning of the web-based services we are enjoying today. Since they were commercially driven, they were mostly offered by ISPs like AOL, Netscape, Microsoft and the like. As the Internet grew millions of people flocked onto it and the web and services started moving away from ISP to fully fledged online social network companies like Facebook, Flicker, Napster, Linked, Twitter and others.

3.4 Gaining Knowledge from Social Networks

When more and more people are making their opinions available in social networks, it is possible to find out about the opinions and experiences of those in the vast pool of people that are neither our personal acquaintances nor well-known professional critics. Figuring out "What other people think" has always been an important piece of information for most of us during the decision-making process. Organizations are attempting to extract insights from opinions of their consumers for revenues increase and competitiveness improvement. The Twitter as an example of a social network consist of 40 million Twitter users, including billions of tweets, more than 1 billion relationships between users, millions of posts, hashtags, URLs, and emoticons. Through analyzing and exploiting the Twitter data, it is possible to formulate and answer a variety of interesting problems/questions, such as the trending topics, brands, pop culture to assess the sentiment or popularity around any area of interest, followers count, tweets counts by catalog, and more. For instance, the problems or questions related to Twitter may be "What's the twitter

traffic distribution by hours, days, weeks, months, and years?" "Sort all the URLs twitted in descend order," "What background color Twitter users like most?" "Who is the person who twitted the most in the three year period?" "Who is the Twitter user who has the most followers by month and year?" "Which geographic location has the most Twitter users?", and so forth.

4. Ethical and Privacy Issues in Online Social Networks

Privacy is a human value consisting of a set of rights including solitude, the right to be alone without disturbances; anonymity, the right to have no public personal identity; intimacy, the right not to be monitored; and reserve, the right to control one's personal information, including the dissemination methods of that information. As humans, we assign a lot of value to these four rights. In fact, these rights are part of our moral and ethical systems. With the advent of the Internet, privacy has gained even more value as information has gained value. The value of privacy comes from its guardianship of the individual's personal identity and autonomy.

Autonomy is important because humans need to feel that they are in control of their destiny. The less personal information people have about an individual, the more autonomous that individual can be, especially in decision making. However, other people will challenge one's autonomy depending on the quantity, quality, and value of information they have about that individual. People usually tend to establish relationships and associations with individuals and groups that will respect their personal autonomy, especially in decision making.

As information becomes more imperative and precious, it becomes more important for individuals to guard their personal identity. Personal identity is a valuable source of information. Unfortunately, with rapid advances in technology, especially computer and telecommunication technologies, it has become increasingly difficult to protect personal identity.

4.1 Privacy Issues in OSNs

Privacy can be violated, anywhere including in online social network communities, through intrusion, misuse of information, interception of information, and information matching [5]. In online communities, intrusion, as an invasion of privacy, is a wrongful entry, a seizing, or acquiring of information or data belonging to other members of the online social network community. Misuse of information is all too easy. While online, we inevitably give off our information to whoever asks for it in order to get services. There is nothing wrong with collecting personal information when it is authorized and is going to be used for a legitimate reason. Routinely information collected from online community members, however, is not always used as intended. It is quite often used for unauthorized purposes, hence an invasion of privacy. As commercial activities increase online, there is likely to be stiff competition for personal information collected online for commercial purposes. Companies offering services on the Internet may seek new customers by either legally buying customer information or illegally obtaining it through eavesdropping, intrusion, and surveillance. To counter this, companies running these online communities must find ways to enhance the security of personal data online.

As the number and membership in online social networks skyrocketed, the issues of privacy and security of users while online and the security of users' data while off-line have taken center stage. The problems of online social networking have been exhibited by the already high and still growing numbers especially of young people who pay little to no attention to privacy issues for themselves or others. Every passing day, there is news about and growing concerns over

breaches in privacy caused by social networking services. Many users are now worried that their personal data is being misused by the online service providers.

As the growth in Online Social Networks continues unabated, the coming in the mix of the smart mobile devices is making the already existing problems more complex. These new devices are increasing the number of accesses to OSNs and increasing the complexity of the privacy issues, including [6]:

- The presence of a user. Unlike in the most traditional OSNs where users were not automatically made aware of the presence of their friends, most mobile OSN (mOSN) now allow users to indicate their presence via a "check-in" mechanism, where a user establishes their location at a particular time. According to Krishnamurthy and Wills [6], the indication of presence allows their friends to expect quick response and this may lead to meeting new people who are members of the same mOSN. Although the feature of automatic locate by oneself is becoming popular, it allows leakage of personal private information along two tracks: the personal information that may be sent and the destination to which it could be sent.
- Location-based tracking system (LTS) technologies that are part of our mobile devices. This is a feature that is widespread in the mobile environment. However, users may not be aware that their location can be made known to friends and friends of friends who are currently online on this mOSN, their friends in other mOSNs and others may lead to leakage of personal information to third-parties.
- Interaction potential between mOSNs and traditional OSNs. According to Krishnamurthy and Wills [6], such connections are useful to users who, while interacting with a mOSN can expect some of their actions to show up on traditional OSNs and be visible to their friends there. However, a lot of their personal information can leak to unintended users of both the traditional OSNs and the mOSNs.

In addition to almost free access to a turn of personal data on OSNs, there is also a growing threat to personal data ownership. For example who owns the data that was altered or removed by the user which may in fact be retained and/or passed to third parties? Fortunately users are beginning to fight for their privacy to prevent their personal details from being circulated far widely than they intended it to be. For example, take Facebook's 2006 News Feed and Mini Feed features designed to change what Founder and CEO Mark Zuckerberg called Facebook's old "Encyclopedic interface," where pages mostly just list off information about people, to the current stream of fresh news and attention content about not only the user but also the user's friends and their activities [7] . The first, News Feed, brought to the user's home page all new activities on all friends and associate links including new photos posted by friends, relationship status changes, people joining groups, and many others, thus enabling the user to get an abundance of information from every friend's site every day. Although these features adhered to Facebook's privacy settings, meaning that only people a user allowed to view the data were able to see it, it still generated a firestone from users across the world. Over 700,000 users signed an online petition demanding the company discontinue the feature, stating that this compromised their privacy [7]. Much of the criticism of The News Feed was that it gave out too much individual information.

Since online social networks, just like their predecessor cyberspace communities are bringing people together with no physical presence to engage in all human acts that traditionally have

taken place in a physical environment that would naturally limit the size of the audience and the amount of information given at a time. As these cyber-communities are brought and bound together by a sense of belonging, worthiness, and the feeling that they are valued by members of the network, they create a mental family based on trust, the kind of trust you would find in a loving family. However, because these networks are borderless, international in nature, they are forming not along well-known and traditional identifiers such as nationalities, beliefs, authority, and the like, but by common purpose and need with no legal jurisdiction and no central power to enforce community standards and norms.

4.2 Strengthening Privacy in OSNs

As more and more people join OSNs and now the rapidly growing mOSNs, there is a growing need for more protection to users. Chew et al. suggest the following steps needed to be taken [8]:

- Both OSN and mOSN applications should be explicit about which user activities automatically generate events for their activity streams
- Users should have control over which events make it into their activity streams and be able to remove events from the streams after they have been added by an application
- Users should know who the audience of their activity streams is and should also have control over selecting the audience of their activity streams
- Both OSN and mOSN application should create activity stream events which are in sync with user expectation

Other suggestions that may help in this effort are:

- Use secure passwords.
- User awareness of the privacy policies and terms of use for their OSNs and mOSNs.
- Both OSNs and mOSNs providers should devise policies and enforce existing laws to allow some privacy protection for users while on their networks.

4.3 Ethical Issues in Online Social Communities

Online social communities including online social network are far from the traditional physical social communities with an epicenter of authority with every member paying alegency to the center with a shared sense of responsibility. This type of community governance with no central command, but an equally shared authority and responsibility, is new, and a mechanism needs to be in place and must be followed to safeguard every member of the community. But these mechanisms are not yet defined, and where they are being defined, it is still too early to say whether they are effective. The complexity, unpredictability, and lack of central authority is further enhanced by [1]:

- *Virtual personality*: You know their names, their likes and dislikes. You know them so well that you can even bet on what they are thinking, yet you do not know them at all. You cannot meet them and recognize them in a crowd.
- *Anonymity*: You work with them almost every day. They are even your friends; you are on a first-name basis, yet you will never know them. They will forever remain anonymous to you and you to them.

- *Multiple personality*: You think you know them, but you do not because they are capable of changing and mutating into other personalities. They can change into as many personalities as there are issues being discussed. You will never know which personality you are going to deal with next.

These three characteristics are at the core of the social and ethical problems in online social networks in particular and cyberspace in general; the larger and more numerous these communities become, the more urgent the ethical concerns become. With all these happening in online social networks, the crucial utilitarian question to ask is what is best way and how can we balance the potential harms and benefits that can befall members of these online social networks and how if possible to balance these possibilities. Of late, the news media has been awash with many of these online ills and abuses and the list is growing including potential for misuse, cyber-bullying, cyber-stalking and cyber-harassment, risk for child safety, psychological effects of online social networking, and free speech.

5 Security and Crimes in Online Social Communities

Online crimes, in tandem with the growth of computing and telecommunication technologies, are one of the fastest growing types of crimes and they pose the greatest danger to online communities, e–commerce, and the general public in general. An *online crime* is a crime like any other crime, except that in this case, the illegal act must involve either an internet-enabled electronic device or computing system either as an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime. Also online crimes are acts of unauthorized intervention into the working of the telecommunication networks and/ or the sanctioning of authorized access to the resources of the computing elements in a network that lead to a threat to the system's infrastructure or cause a significant property loss. The International Convention of Cyber Crimes and the European Convention on Cyber Crimes both list the following crimes as online crime [9]:

- Unlawful access to information
- Illegal interception of information
- Unlawful use of telecommunication equipment
- Forgery with use of computer measures
- Intrusions of the Public Switched and Packet Network
- Network integrity violations
- Privacy violations
- Industrial espionage
- Pirated computer software
- Fraud using a computing system
- Internet/e–mail abuse
- Using computers or computer technology to commit murder, terrorism, pornography, and hacking

As we discussed before, the online contents are accessible from different locations without noticeable delay. Because of the decentralized architecture of the Internet, personal publication through the Web becomes more feasible and affordable, while still maintaining a high exposure to the target audience. At the same time, the lack of regulations makes the online social community a pretty free realm where the geographical border dims in the online communities. Information can be spread anonymously with little interference from governments via the online community. Costs of the community are relatively low compared with other media. Various communities benefit from the online features of the community. We will analyse a dark web as a case study here to illustrate how terrorist/extremist organizations and their sympathizers exchange ideology, spread propaganda, recruit members, and plan attacks. The terrorists, extremists, and their sympathizers can benefit from Web techniques and online communities. They exchange ideology, spread propaganda, recruit members and even plan attacks through the online community. Especially, because of the ubiquity of the online community, the previously isolated terrorists/extremist cells are able to collaborate more efficient than any time before and to form a more compact community virtually. Dark webs contain rich information about the dark groups, such as ideologies, recent topics and news.

Several research works has been conducted to analyze web of terrorist cells or criminal activities. M. Sparrow [14] applied social network analysis to criminal activities and observed three problems associated with criminal network analysis. They are incompleteness of analyzing data as a result of missing nodes and links that the investigators will not uncover, fuzzy boundaries resulting from the difficulty in deciding who to include and who not to include, and the dynamic property of analyzed networks. V. E. Krebs [15] uses public information reported in major newspapers such as the New York Times, and the Wall Street journal to map networks of terrorist cells. Their research unrevealed a picture of a covert network after the tragic events of September 11th, 2001. P. Klerks [17] describes the development of criminal network analysis. The approaches start from manual analysis. An analyst constructs an association matrix by identifying criminal associations from raw data. Then a graphic-based approach is proposed to automatically generate graphical representation of criminal networks. Recently social network analysis has been used to provide more advanced analytical functionality to assist crime investigation. J. Xu and H. Chen [16, 19] use data mining techniques to reveal various structures and interactions within a network. Discovering topics from dark websites helps in developing effective combating strategies against terrorism or extremists. The latent or topics are buried in large scale web pages and hosted by dark websites. This work employs information retrieval (IR) techniques to discover hidden topics in a known dark web, such that the discovered latent topics can provide insights into social communities.

Modeling text corpora extracted from websites help find short description of a topic such that essential statistical relationships are preserved from for the basic tasks such as classification, summarization and similarity judgment [14]. In the field of information retrieval, a basic vocabulary of words or terms is chosen and each document in the corpus is reduced to a vector of

real numbers, each entry representing ratios of word counts. In the popular *tf-idf* scheme [15], term frequency (tf) count is compared to an inverse document frequency (idf) count, which measures the number of occurrences of a word in the entire dataset. The tf-idf scheme generates a term-by-document matrix X whose columns contain the tf-idf values for each of the documents in the corpus. Latent semantic indexing (LSI) [12] is proposed to further reduce description length and reveal more inter- or intra- document statistical structure. LSI uses a singular value decomposition of the X matrix to identify a linear subspace in the space of tf-idf features that capture most of the variance in the collection.

Hofmann [13] presented probabilistic LSI (pLSI) model to model each word in a document as a sample from a mixture model, where the mixture components are multinomial random variables that can be viewed as representations of topics. Thus each word is generated from a single topic, and different words in a document may be generated from different topics. While Hofmann's word is a useful step toward probabilistic modeling of text, it provides no probabilistic model at the level of documents. Yang et al. [18] discovered latent topics from the dark web by Latent Dirichlet Allocation (LDA) [11] which improves upon pLSI by placing a Dirichlet Prior on topic distribution to reduce overfitting and bias the topic weights from each document towards skewed distributions with few dominant topics.

6. Conclusion

The growth of online social communities, emanating from the old social gatherings of days before computing has given us all a bonanza to and means to access information in amazing ways. Online communities have created opportunities for us unprecedented in the history of human where one individual can reach millions of others anywhere on the globe in seconds. The history and development of computing has made all this possible. However, with the easiness and abundance of resources at our disposal availed to us by online communities, there has also been evils that have been enabled by these large ecosystems. To be able to safeguard personal privacy, security and dignity, we must pay special attention and develop protocols and best practices that must make everyone in these communities safely enjoy the experiences presented in these ecosystems. The battle is not yet worn and the way forward is not clear yet just because the next move in new technologies is not predictable.

Cross-References

Evolution of Social Networks

Collaborations in Online Social Networks

User Behavior in Online Social Networks, Influencing Factors

Cybercrime and the Use of Online Social Networks

Topology of Online Social Networks

Privacy Preservation and Location-based Online Social Networking

Online Social Network Privacy Management

Performance Measurement and Analysis of Online Social Networks Systems

Consequences of Publishing Real Personal Information in Online Social Networks

Corporate Online Social Networks and Company Identity

Ethical Issues Surrounding Data Collection in Online Social Networks

References

1. Joseph M. Kizza. *Ethical and Social Issues in the Information Age*, 5th Edition, Springer, 2013.
2. Robert Fox. "News Track: Age and Sex." *Communications of the ACM,* Volume 43 (9), September 2000, p. 9.
3. "Bylaws for Internet Corporation for Assigned Names and Numbers." ICANN, April 8, 2005. www.icann.org/general/bylaws.htm, retrieved April 2013.
4. Joseph M. Kizza. Ethical and Social Issues in the Information Age. Springer, 1999.
5. "Web Surpasses One Billion Documents: Inktomi and NEC Research Institute Complete First Web Study," Inktomi News & Events, January 2000.
6. William Wresch, Disconnected: Haves and Have-Nots in the Information Age, "Information Age Haves and Have-Nots.", Rutgers University Press, ISBN-10: 0813523702, 1996.
7. Walsh, Mark, "Court Backs Student on Facebook Page Criticizing Teacher", NewsWeek, http://blogs.edweek.org/edweek/school_law/2010/02/court_backs_student_on_faceboo.html, retrieved April 2013.
8. Monica Chew, Dirk Balfanz and Ben Laurie "(Under)mining Privacy in Social Networks", Google Inc. URL: http://w2spconf.com/2008/papers/s3p2.pdf, retrieved April 2013.
9. Kizza, Joseph M. *Computer Network Security.* New York, NY: Springer, 2005.
10. "Evolving the High Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure—Executive Summary." http://www.nap.edu/openbook.php?record_id=4948, retrieved April 2013.
11. Blei, Ng and Jordan, Latent Dirichlet Allocation (2003), Journal of Machine Learning Research 3 993-1022
12. S. Deerwester S. Dumais, T. Landauer, G. Furnas, and R. Harshman. Indexing by latent semantic analysis. Journal of the American Society of Information Science, 41(6):39-407, 1990.
13. T. Hofmann. Probabilistic latent semantic indexing. Proceedings of the Twenty-Second Annual International SIGIR Conference, 1999.
14. M. K. Sparrow, The application of network analysis to criminal intelligence – an assessment of the prospects, Social Networks, Vol. 13, pp. 251-274, Sept. 1991.
15. V. E. Kerbs, Mapping networks of terrorist of cells, Connections, vol. 24, pp. 43-52, 2001.

16. J. Xu and H. Chen, Analyzing and Visulization, Communications of the ACM, vol. 48, pp. 100-107, Jun. 2005.
17. P. Klerks, The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. Connections 24, 3 (2001), 53-65.
18. Li Yang, Feiqiong Liu, Joseph M. Kizza, Raimund K. Ege. Discovering Latent Topics from Dark Websites, *IEEE Symposium on Computational Intelligence in Cyber Security*, IEEE Xplore, April 2009.
19. Koch, M.; Richter, A.; Schlosser, A.: Services and applications for IT-supported social networking in companies, Wirtschaftsinformatik, 6/49, 448—455, 2007.
20. ramer, R. M.: Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. In: Annual Reviews Psychology, 50, pp. 569—598, 1999.