The Newest Way to Screen Job Applicants: A Social Networker's Nightmare

Carly Brandenburg*

* J.D., 2007, Indiana University School of Law—Bloomington. B.A. DePauw University.

I. SOCIAL NETWORKING: THINK TWICE

Web sites designed to promote shared information—like blogs, Facebook, Friendster, Xanga, and MySpace—may provide more than the opportunity to share stories and details of a college student's or graduate's life. To many students and graduates who are "nurtured in open, collegial situations, blogging and personal Internet postings on social networking Internet sites such as MySpace, Facebook, and Friendster . . . blur the line between personal and public."[1] Students and graduates today are getting more than they bargain for as they attempt to enter the workforce and realize their blogging and social networking ways can come back to bite them.

This Note discusses the potential ramifications of using shared information sites, focusing on the Facebook social network and its users. Employers who hire graduating students are steadily discovering that social networking sites allow them to learn more than they ever could from reading an applicant's resume and cover letter. This Note explores some of the legal issues raised when employers conduct social network background checks. Its primary focus is to determine what kinds of privacy expectations, if any, social networkers can anticipate.

A. Social Networks and Their Dangers

Social networks on the Internet have become increasingly popular among the general population, but these networking sites are still used most frequently by college students and recent graduates.[2] Most social networks merely require a user to register by providing basic information and a valid email address. Social network users can then post anything they wish on that particular Internet social Web site. Users can post their comments, upload photographs, join and form groups with other networkers, and share their personal information. They can also freely search other users' profiles in order to find and interact with other social networkers throughout the world.

---

1. *Is Your Company's Work Blogging Down?*, 4 No. 1 FED. EMP. L. INSIDER (McGuire Woods LLP, Fortney Scott LLC), Sept. 2006, at 2 [hereinafter *Blogging Down?*].

2. *What You Won't See on a Resume*, 18 No. 12 GA. EMP. L. LETTER (Ford, Harrison LLP), July 2006, at 5 [hereinafter *What You Won't See*].

1. The Messages Social Networkers Communicate

On Facebook, as is the case with many social networks, users create profiles to share basic information that will allow others to search for, find, and connect with them. However, some users provide information about themselves that "go[es] to the very edges of decency and legality."[3] For instance, a Facebook user can find more than 500 groups and more than 500 events that contain the search term "sex" using a basic Facebook search.[4] Some of the groups that can be located using this search term on Facebook are fairly tame, like the group referring to the popular television series with the title, "Alright . . . I admit it . . . I'm a Sex in the City addict." On the other hand, the vast majority of Facebook groups containing the word "sex" are far less innocuous with titles like "Casual Sex at IU," "Chances are I'm currently having Sex," "Girls who Love Sex," "I Actually HAVE had Sex on Campus," and other similar groups.[5] By simply clicking on a group title and following its link to the group's members, Facebook users can find friends with similar interests, and employers can find potential hires with frighteningly questionable interests (and the propensity to share their feelings and interests with others). Similar results are yielded when searching for terms like "drugs," "porn," and "alcohol."

Beyond the groups social networkers can join and create, Facebook users can post anything they wish about themselves on their personal profiles. These profiles often contain pictures and also document Facebook users' interests and activities, political views, sexual orientations and proclivities, relationship status, religious beliefs, and any number of other bits of personal information that employers may find interesting or useful to their decision-making process.[6]

---

3. *Id.*

4. *See* Welcome to Facebook, http://www.facebook.com/ (last visited Mar. 21, 2008). Once one creates a profile and gains access to Facebook through the main webpage, simply click on "search" and then select "all networks" under the "basic search" portion of the network. Then input the desired search term—in this instance, "sex"—to see how many names, profiles, groups, or events are yielded. Once a user begins searching, he or she can limit the search to his or her own social network or to all networks (including other universities, companies, geographic regions, etc.).

5. The titles of these groups were all found through the basic search on Facebook described *supra*, note 4. All are actual and current groups formed by Indiana University Bloomington students. Facebook users can find similar groups formed on many different college campuses by Facebook users at other universities.

6. Many social networkers use Facebook or other similar sites to share the "idiosyncratic odds and ends of their lives, intended for viewing by other students . . . [but] the unintended consequences of overly comprehensive, brutally frank, or mischievous entries are surfacing." *See* Sarah Schweitzer, *Universities Ponder Facebook Etiquette*, THE TECH, Sept. 27, 2005, *available at* http://www-tech.mit.edu/V125/N42/facebook.html.

2. Employers Are Discovering Their Options

According to a National Association of Colleges and Employers ("NACE") study, approximately one in ten employers report they plan to review potential hires' profiles and information posted on social networks.[7] In addition, employers who admit to reviewing social networkers' profiles as they screen job applicants say the information available on these profiles has at least some influence on their hiring decisions. The NACE study does point out, on the other hand, that many employers say they do *not* review social networkers' online postings in order to evaluate potential hires; around forty percent of surveyed employers are still undecided regarding whether to use this sort of information as they seek the best candidates for jobs.[8]

Another study conducted by CareerBuilder.com yielded similar findings.[9] The study included 1,150 hiring managers nationwide, and about twelve percent of those managers surveyed said they have screened job candidates by searching for the potential hires' profiles on social networking sites. Of the employers electing to research candidates on social networking sites, sixty-three percent did not hire a prospective employee based on the information uncovered about the candidate online.[10] Beyond those managers surveyed who admitted to searching for social networkers' information, an additional twenty-six percent of the managers reported they have used Internet search engines like Google to research prospective hires.[11]

Some sources recommend that employers search social networks and play it safe—why not check a potential candidate out using every resource available before making that critical hire?

> Online social networks provide you with a screening tool for job applicants. It's unlikely that a job applicant would ever attach provocative photos, detailed descriptions of sexual escapades, or a list of hobbies that includes funneling beer and recreational drug use on her resume. But with just a few clicks of the mouse, you can find out all sorts of revealing information about potential candidates.[12]

---

7. *See New "Background" Check*, 23 No. 21 EMP. ALERT (National Employment Law Institute), Oct. 12, 2006, at 11 (highlighting the results from the NACE study).

8. *See id.*

9. *See* CareerBuilder.com, One-in-Four Hiring Managers Have Used Internet Search Engines to Screen Job Candidates; One-in-Ten Have Used Social Networking Sites, CareerBuilder.com Survey Finds (Oct. 26, 2006), http://www.careerbuilder.com/share/aboutus/pressreleases.aspx (follow "2006" hyperlink; then follow "10/26/2006" hyperlink).

10. *Id.*

11. *Id.*

12. *What You Won't See*, *supra* note 2, at 5.

Employers are increasingly realizing that they have a choice when it comes to their hiring decisions. They may be more limited with disciplinary actions once employees are actually hired, and this makes an employer's decision to hire the right people particularly important.[13]

With the power and responsibilities many new employees can have in the workplace, many employers believe it is important that their hires possess a sense of propriety and an ability to separate their work life and behavior from their personal life. "[N]ew employees have access to a wide range of sensitive materials and information via the rise of the information economy and flattened workplace structures. Given the powerful communication tools in employees' hands, judgment or discretion are increasingly important characteristics for [employees to have]."[14]

B. Protecting Social Networkers' Privacy: An Impossible Task?

As employers discover the availability of social networkers' online information, can social network users protect themselves and their posted information? Users of Facebook may harbor the incorrect belief that other students and intended viewers are the only people able to view their profiles. Facebook's privacy settings state you can "control exactly who can see what by including or excluding certain friends or friend lists," as well as "[c]ontrol who can search for you, and how you can be contacted."[15]

According to Mark Zuckerberg, the man who created Facebook in 2004 while a sophomore student at Harvard University, "[T]he problem Facebook is solving is this one paradox. People want access to all the information around them, but they also want complete control over their own information. Those two things are at odds with each other."[16] Zuckerberg believes that Facebook is able to adequately address this problem because it lets its users activate privacy settings. Users can attempt to prevent strangers from viewing the profiles, pictures, and personal information they post on Facebook by enabling blocking techniques designed to limit outsiders' access to the information. College students, for

---

13. *Blogging Down?*, *supra* note 1, at 2 (stating that "[o]nce employees are hired . . . it's usually better to address the problem by establishing specific guidelines and training them in the importance of observing the rules and exercising discretion and judgment").

14. *Id.*

15. Having created a Facebook profile, one may access privacy settings by clicking "Privacy." After accessing this section, users can choose whether everyone or only limited groups of people can access their profiles and information. *See* Welcome to Facebook, *supra* note 4.

16. John Cassidy, *ME Media: How Hanging Out on the Internet Became Big Business,* NEW YORKER, at 56 (May 15, 2006), *available at* http://www.newyorker.com/archive /2006/05/15/060515fa_fact_cassidy.

example, can choose to block all persons not affiliated with their college or university. Those who use Facebook could also enable privacy settings that limit those who can view their profiles to people they accept as their friends or those connected to them through friends (friends of their friends).[17]

1. Facebook's Privacy Settings and Their Shortcomings

Despite the available technology that can potentially limit or block unwanted social network users from viewing students' and graduates' Facebook profiles, many Facebook users simply do not activate their privacy settings. Other social networkers enable their privacy settings, but fail to realize that employers nonetheless may be able to gain access to profiles seemingly protected by privacy settings.

Hiring companies can access potential hires' social networking profiles in a variety of ways. Not long ago, some of the employees now involved in making hiring decisions for their companies were students with their own Facebook profiles. Graduates can keep their profiles and maintain connections to their colleges' social networks, thereby maintaining connections to the college students who make up the next wave of employment hopefuls. This phenomenon may not be pervasive yet since Facebook and other social networking sites have only existed for a few years.[18] However, as Facebook and other social networking sites gain popularity among college students and as more student Facebook users graduate and join the world of employment, this trend may become increasingly prevalent. Even if employees never had Facebook profiles during their college years, many employees still retain their college email addresses or a valid alumni email address.[19] With a college or alumni email address, employees can create profiles and become affiliated with their undergraduate universities' networks, thereby acquiring access to current students. To those students, these employees will simply appear to be other students and alumni similarly interested in using Facebook as a social networking tool rather than as an employment screening tool.

Some companies also hire current students who can access their peers' social networking profiles and effectively circumvent any privacy settings a potential hire may have put in place to attempt to restrict unwanted persons from accessing their profile.[20] For instance, an Indiana

---

17. *See* Welcome to Facebook, *supra* note 4.

18. A sophomore student at Harvard created Facebook in 2004. *See* Cassidy, *supra* note 16, at 50.

19. *See* Alan Finder, *Online Persona Can Ruin Your Shot at That Job*, SEATTLE TIMES, June 11, 2006, *available at* http://seattletimes.nwsource.com/html/nationworld /2003054004_recruit11.html.

20. *See id*.

University ("IU") student seeking interviews may take extra precautions to keep his or her information safe by setting online privacy measures allowing only other IU students to access and view his or her Facebook profile. Not only would that student's information not be safe from a recent IU graduate who retains an IU student or alumni email address and now uses that address to aid his or her employer in seeking out the next wave of new employees, but the student also would not be shielded from a current peer instructed to research prospective employees for a particular company.

Many students discover their social networking profile or other information posted on the Internet has cost them a job opportunity after it is too late.[21] Others take a preemptive stance, attempting to keep their profiles clean and "Googling" themselves occasionally to ensure that unwanted material does not show up online for anyone to view.[22] Is self-censorship the only option available for social networkers hoping to keep their information restricted to intended recipients only?

2. Should a Right to Privacy on Social Networking Sites Be Recognized?

Could an employer's unauthorized use of the information on a social networker's profile for hiring purposes constitute an invasion of privacy? In order for a person's privacy to be invaded, that person must have a reasonable expectation of privacy.[23] Facebook tells its users that, "[a]t Facebook, we believe you should have control over your information and who sees it. So in addition to the basic visibility rules – only your friends and people in your networks can see your profile – we also give you granular control over the information you post to the site."[24] The site also provides in its December 6, 2007, adopted privacy policy:

> We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want

---

21. *See* Nate Anderson, *Google + Facebook + Alcohol = Trouble*, ARS TECHNICA (Jan. 19, 2006), http://arstechnica.com/news.ars/post/20060119-6016.html. This source and others also highlight the fact that social networkers can get themselves into trouble due to information posted on the Internet with persons other than prospective employers. Many colleges and universities have been able to access pictures and information on Facebook that provide evidence of underage drinking or other violations of school rules that can cause students to face disciplinary procedures within their academic institutions. *See id.*

22. *See id.*; *see also,* Kate Bigam, *Employers May be Eying Students' Facebook Accounts*, DAILY KENT STATER, Nov. 3, 2006, *available at* http://media.www.kentnewsnet.com/media/storage/paper867/news/2006/11/03/News/Employers.May.Be.Eyeing.Students.Facebook.Accounts-2437174.shtml.

23. *See* Mitchell Waldman, Annotation, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5th 15 (2001).

24. Facebook Site Tour, http://www.facebook.com/sitetour/privacy.php (last visited Mar. 21, 2008).

> everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.[25]

From these statements, one can see why Facebook users may believe their information posted on the social networking site is secure. If one continues reading the Web site's privacy policy, he or she can also find this warning:

> You post User Content . . . on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.[26]

From the statements informing Facebook users of their ability to use privacy protection measures to warnings about the unavoidable flaws inherent in any privacy protection system, it is difficult to determine whether Facebook networkers can have any reasonable expectation that the materials they post on the site will be safe from unwanted viewers.

3. The Reasonable Expectation of Privacy Requirement: Being Seen by Some Does Not Mean One Should be Seen by All

No clear answer can yet be gleaned from legal precedent as to whether the Facebook users and other social networkers have a reasonable expectation of privacy in their profiles and posted materials. According to court decisions, there is uncertainty as to whether a person retains a limited right to privacy and a reasonable expectation of privacy when the information that person intended to keep private was intentionally shared with some but also fell into the hands of unintended recipients. For example, the California Supreme Court stated in *Sanders v. American Broadcasting Co.* that:

> There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law . . . . The mere fact that a person can be

---

25. Facebook Principles, http://www.facebook.com/policy.php (last visited Mar. 21, 2008).

26. *Id.*

> seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone.[27]

In *Sanders*, an ABC investigative journalist, Stacy Lescht, obtained employment as a telephone psychic and used a hidden video camera to record her conversations with her new co-workers. Sanders, an employee of the company, sued the undercover journalist after part of one of his conversations with her was broadcast on ABC's *PrimeTime Live* television program. The ABC journalist argued that because coworkers could overhear her conversations with Sanders, Sanders could have no reasonable expectation of privacy in the communication. The court disagreed, determining that Sanders retained a reasonable expectation of privacy during his workplace discussions with coworkers.[28]

Other cases also suggest that a plaintiff who reveals information about himself or herself to some people may have the right to keep that information private from other unintended persons for the purposes of privacy tort law.[29] This may be the case regardless of contractual or legal constraints placed upon those to whom the information is expressed.[30] In addition, a plaintiff may reasonably expect information to be kept private in a variety of situations involving different groups of people, such as persons close to the plaintiff,[31] coworkers,[32] or mere strangers.[33]

In *Y.G. v. Jewish Hospital of St. Louis*, the plaintiffs were a married couple who conceived twin children after their participation in an *in vitro* fertilization clinic. The couple's church condemned this form of conception, and the couple kept the information about their twins' conception limited to a few close friends and family members. The couple attended a party at the *in vitro* clinic for around forty people who were involved with the clinic, and a local news media crew covered the party and aired pictures of the couple on television. The media crew argued that the plaintiffs waived their expectation of privacy as to their involvement with the clinic when they attended the party, but the court disagreed. It held that by attending the party the couple "clearly chose to disclose their

---

27. *See* Sanders v. American Brdcst. Co., 978 P.2d 67, 72 (Cal. 1999).

28. *Id.* at 79.

29. *See id*. at 67. *See generally* Y.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488 (Mo. Ct. App. 1990); Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491 (Ga. Ct. App. 1994).

30. In other words, whether the information one shares is with a doctor or lawyer (legally protected and private relationships) or with friends or acquaintances who are under no specific legal obligation to maintain the confidences shared with them is not determinative of whether the person can have an expectation of privacy.

31. *See Kubach*, 443 S.E.2d at 491.

32. *See Sanders*, 978 P.2d at 67.

33. *See Y.G.*, 795 S.W.2d at 488.

participation to only the other *in vitro* couples. By so attending this limited gathering, they did not waive their right to keep their condition and the process of *in vitro* private, in respect to the general public."[34]

Similarly, in *Multimedia WMAZ, Inc. v. Kubach*, the court determined that an HIV positive man retained a reasonable expectation of privacy as to his condition when it was disclosed by a television station. Mr. Kubach agreed to appear as a guest for a report the television station aired, but he agreed to do so only if his identity was kept private and his image distorted to render it unrecognizable. The distortion did not work as Kubach expected and as the station had promised, and Kubach was recognized by television viewers throughout his community. The television station argued that the plaintiff had no reasonable expectation of privacy as to the fact that he was HIV positive because he had disclosed the information to friends, some family members, and members of support groups. Many people were aware of the fact that Kubach was HIV positive. The court disagreed with the station and sided with Kubach, stating that the plaintiff had expressed news of his condition to some "because they cared about him and/or because they also had AIDS."[35] In addition, although Kubach did not tell his friends and relatives to keep his medical condition confidential, "there was also testimony that they understood that plaintiff's condition was not something they would discuss indiscriminately."[36]

4. The Reasonable Expectation of Privacy Requirement: Once Information is Provided to Some, it is Open to All?

On the opposite end of the spectrum, there are also cases that reject a plaintiff's invocation of a limited right to privacy regarding particular facts or information that the plaintiff disclosed to third parties. In *Nader v. General Motors Corp.*, the New York Court of Appeals set a very different precedent from the cases discussed previously.[37] Just before consumer advocate Ralph Nader published his best seller, *Unsafe at Any Speed*, General Motors allegedly tried to intimidate Nader by digging into his personal information and past. The company allegedly interviewed Nader's friends and relatives regarding Nader's interests, habits, political and religious beliefs, sexual history, and other areas under the false pretense that it was researching Nader for prospective employment purposes. The court determined that information already known to others could hardly be considered private, and Nader therefore could not expect to maintain his

34. *Id.* at 502.
35. *Kubach*, 443 S.E.2d at 494.
36. *Id.*
37. *See* Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970).

privacy despite the fact that he had shared personal information with select persons only.[38] Essentially, Nader was deemed to have assumed the risk that persons to whom he disclosed his information would spread that information to others. As a matter of law, facts shared with others are no longer private.[39]

The case of *Duran v. Detroit News, Inc.* also follows a similar hard-line toward privacy in information disclosed to third parties.[40] In this case, Consuelo Sanchez Duran was a Colombian judge who had indicted the drug lord Pablo Escobar. As a result of her ruling, Duran and her family received death threats that caused her to resign, flee Colombia, and take a job as the Colombian consul in Detroit, Michigan. Duran used her real name when shopping and dining out, and told a few neighbors of her reason for fleeing Colombia; however, she also took precautions to ensure that her relocation to Detroit was not otherwise advertised or widely known publicly (for instance, she kept an unlisted phone number, did not join clubs or organizations, and did not attend concerts or other public events). Duran sued when, after living in Detroit for a few months, local reporters exposed her history and disclosed her address. At least one reporter also publicized the $1 million bounty the Colombian drug cartel had put on Duran's head. The Michigan Court of Appeals determined that Duran's actions and disclosures to Detroit residents had rendered her identity "open to the public eye,"[41] and Duran could enjoy no reasonable expectation of privacy as to her identity and background.

The final hard-line case of interest is *Fisher v. Ohio Department of Rehabilitation and Correction*.[42] In this case, the Ohio Court of Claims determined that a plaintiff who told four coworkers that some interactions between herself and her young son had "sexual overtones" could claim no reasonable expectation of privacy as to her statements.[43] The plaintiff's disclosure to the coworkers rendered the information nonprivate, and the plaintiff's employer was therefore free to disclose the information to the plaintiff's husband (who subsequently divorced her). The court stated that "the report merely recounts a conversation which the plaintiff publicly and openly conducted with her fellow employees. The plaintiff's discussion of her personal experiences was freely offered to the persons around her without concern of the impact it might have on her character."[44]

---

38. *Id.* at 770.
39. *See id.*
40. *See* Duran v. Detroit News, Inc., 504 N.W.2d 715 (Mich. Ct. App. 1993).
41. *Id.* at 720.
42. 578 N.E.2d 901 (Ohio Misc. 1988).
43. *Id.* at 902.
44. *Id.* at 903.

From the cases discussed in this section and the preceding section, it is clear that there is not a strong line of cases to direct a modern court's determination of whether a plaintiff has a reasonable expectation of privacy for the purposes of privacy tort law. The number of persons to whom a plaintiff voluntarily discloses information does not seem to be a determinative factor in deciding whether a plaintiff can claim an expectation of privacy. In *Kubach*, the plaintiff told around sixty people about his HIV positive condition, and the court determined that he could reasonably expect to maintain his privacy as to this fact;[45] on the other hand, the plaintiff in *Fisher* told only four coworkers of the "sexual undertones," but she could retain no expectation of privacy in her statements.[46] Why should particular disclosures waive privacy expectations while others do not?

5. Interpreting Precedent: The Future, Privacy Concerns, and the Stored Communications Act

It is difficult to know how a modern court might rule on a Facebook user's privacy claims against an employer (or another unintended viewer) who accesses the user's profile or online postings without permission. The fact that a Facebook user could permit hundreds, or even thousands, of people to view her profile may not be the only indication of whether the social networker has a reasonable expectation of privacy where unwelcome viewers are involved. It seems plausible that "if you are using privacy features that you believe restrict access to very few specific people completely within your control, and an employer somehow hacks past such a privacy barrier, you may have a strong privacy claim."[47] After all, a person who attempts to protect and secure their privacy and information is more deserving of that privacy than one who does not care about protecting privacy. In the end, however, it is difficult to say whether an attempt at protecting one's privacy will be enough to secure an expectation, and perhaps even a right, to that privacy.

In addition to the cases discussed previously that provide insight into a court's reasoning with regard to a plaintiff's expectation of privacy generally, other cases have dealt with the issue of whether a plaintiff can have an expectation of privacy with regard to his or her communications posted on an Internet Web site. In *Konop v. Hawaiian Airlines, Inc.*, Konop, a pilot with Hawaiian Airlines, configured and maintained a Web

45. Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 494 (Ga. Ct. App. 1994).

46. *Fisher*, 578 N.E. 2d at 902.

47. Posting of George Lenard to CollegeRecruiter.com Blog, *Employers Using Facebook for Background Checking: Is it Legal?*, http://www.collegerecruiter.com/weblog/archives/2006/09/employers_using.php (Sept. 1, 2006, 6:52 EST).

site that allowed other employees of the airline to read news updates and often critical editorial comments related to the airline, its senior management staff, and the employees' union.[48] The plaintiff designed the Web page to allow particular personnel to enter and view the site (using a valid username and password) and to deny access to others. Much like Facebook, Konop also incorporated terms and conditions of use into his site. These terms expressly required that all permitted users keep the information on the Web site private and that all nonauthorized persons "simply find *something else* to do" rather than access the Web page.[49] Konop sued after a manager of Hawaiian Airlines, lacking Konop's express permission to enter the Web page, was able to gain access after two authorized employees permitted him to use their employee usernames (thereby allowing the manager to effectively assume the other employees' identities and pretend to access the site as an authorized viewer). The Ninth Circuit determined that the manager's unauthorized viewing of the secured Web site could afford Konop a cause of action under the Stored Communications Act ("SCA").[50]

The Ninth Circuit recognized its decision was a difficult one, particularly where the SCA "addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public,"[51] but at the same time where "[t]he nature of the Internet . . . is such that if a user enters the appropriate information . . . it is nearly impossible to verify the true identity of that user."[52] The court agreed with Konop's argument that the manager may have violated the SCA, which recognizes and punishes the offense of "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ing] . . . access to a wire or electronic communication while it is electronic storage in such system."[53]

The Ninth Circuit's recognition that a cause of action may be available to plaintiffs under the SCA seems encouraging to Facebook users attempting to protect their posted information from the eyes of unauthorized employers. However, these hopes may be short-lived, as the

---

48. Konop v. Hawiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

49. *Id.* at 875, n.3 (emphasis in original).

50. 18 U.S.C. §§ 2701-2711 (2000). Title II of the Electronic Communications Privacy Act ("ECPA") "address[es] access to stored wire and electronic communications and transactional records." S. Rep. No. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

51. *Konop,* 302 F.3d at 875 (internal quotations omitted).

52. *Konop,* 302 F.3d at 875.

53. 18 U.S.C. § 2701(a)(1).

SCA also exempts from liability "conduct authorized . . . by *a user* of that service with respect to a communication of or intended for that user."[54] In *Konop*, the court determined that this exception may not apply on account of the particular facts involved in the case. Specifically, the two authorized employees who granted the manager permission to appropriate their usernames and access Konop's Web page may not have ever used Konop's site themselves.[55] Since a question existed as to whether either authorized employee had actually accessed the Web page, the Ninth Circuit could not determine whether either employee had ever become "a user" under the SCA.[56]

If the employees were "users" of Konop's site, their actions in allowing an authorized third party to access the site with their usernames may well have afforded the unauthorized third party (the manager) the ability to access the Web page without violating the SCA (since the manager's actions might then be considered "conduct authorized . . . by a user of that service . . ."). [57] Similarly, if Facebook users permits other students from their university to access and view their profile, those students who are employed as "spies" for hiring companies will also likely be considered "users" of the Facebook service and of the particular Facebook user's stored information under the SCA's terms. Student or alumni "spies" who are not specifically blocked or prohibited through privacy settings from accessing their peers' profiles and information will likely be considered authorized viewers and users of the Facebook service. Facebook users who want to protect their privacy may not have the means to prevent these authorized "spies" from sharing the information they retrieve with unwanted and unauthorized third party employers. Since the *Konop* court never actually decided whether the exception under the SCA would render Konop's Web site unprotected, despite Konop's diligent efforts to protect his online postings, it is difficult to know for certain how a modern court might react to the Facebook users' privacy dilemmas.

6. The Internet: An Amazing and Unruly Medium

Because many courts have recognized how accessible the Internet is, how many people are able to effectively access the Internet, and how

54. 18 U.S.C. § 2701(c)(2) (emphasis added).

55. *See Konop*, 302 F.3d at 880.

56. *Id.*

57. 18 U.S.C. § 2701(c)(2). A "user" is defined as "any person or entity who (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13). While there is no question that the two employees who gave the manager their user names were duly authorized by the provider to engage in use of the service, the facts did not show that the employees had actually used the service as required under part (A) of the definition above.

difficult it is to keep track of who is involved in viewing particular Internet sites,[58] it is possible that a modern court faced with Facebook users' privacy dilemmas could determine that social networkers should not be able to reasonably claim an expectation of privacy in their Internet postings. While this may not be the correct response to the privacy problems online, it enjoys some precedential support.[59]

Just as the court in *Konop* tried to reconcile Congress's intent that the SCA protect electronically communicated materials from unauthorized viewers with the pervasiveness and easy accessibility of the Internet, a Pennsylvania court attempted to determine the privacy issues raised with regard to communication on an Internet Web site in *J.S. ex rel. H.S. v. Bethlehem Area School District*.[60] In this case the Commonwealth Court of Pennsylvania held that a middle school student could not have an expectation of privacy with regard to the materials he posted on his Web site. The student created a Web page at his home on his family's computer, and posted derogatory comments about his teachers and principal on this site. After discovering the site and deeming it to be threatening and harassing to a teacher and the principal, the school expelled the student.

In addressing the issue, the Pennsylvania court noted that the school district could not have violated the boy's right to privacy because "any user who happened upon the correct search terms could have stumbled upon [the] Student's web-site."[61] The court pointed out that the Web site in question was not a protected site—it was not the sort of site that could only be accessed by particular viewers with passwords or specific usernames. The court also compared the posting of a Web site to the sending of email messages or letters: once the message or letter is received, the sender can no longer control the information's ultimate destination or potential to spread to others. Similarly, a creator of a Web site controls the site until the time it is posted on the Internet. Once posting has occurred, the creator loses control of the Web site's final reach and audience, and that site becomes accessible to anyone on the Internet. "Without protecting the web-site, the creator takes the risk of other individuals accessing it once it is posted."[62] Accordingly, the court affirmed the trial court's decision that the

58. "The nature of the Internet, however, is such that if a user enters the appropriate information (password, social security number, etc.), it is nearly impossible to verify the true identity of that user." *Konop*, 302 F.3d at 875.

59. *Compare* Reno v. ACLU, 521 U.S. 844 (1997), *with* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001) (pointing to the fact that the Internet allows millions of people across the world to share and exchange information and to communicate through the computer connections).

60. 757 A.2d 412 (Pa. Commw. Ct. 2000).

61. *Id.* at 425.

62. *Id.*

student maintained no expectation of privacy in the comments he posted on his Web site.

The court's focus on the student's failure to implement privacy protection or security measures highlights its willingness to consider this particularly important issue as it addresses Internet users' privacy. Future courts' reliance on cases like *Konop* and *J.S.*, which discuss privacy settings and security measures at length, may help to create a future test and recognizable standards for determining a plaintiff's privacy expectations.

A court should be concerned with these privacy settings and security measures as it determines whether an expectation of privacy can exist. A number of factors could be relevant to determining whether a social networker can have a reasonable expectation of privacy in his or her information posted online. These factors include: (1) whether privacy settings are available; (2) whether the social networker attempted to or did enable the privacy settings; (3) the level of privacy the networker attempted to or was able to set with an eye to the spectrum of privacy settings and measures available to the social networker; (4) the kinds of people and groups to whom that networker chose to disclose the information he or she later claims to be sensitive and private; and (5) whether the unwanted or unauthorized person who accessed the networker's information was able to happen upon the information or had to hack through security measures to find the information. While this list is by no means exhaustive, it builds on the principles established in some of the privacy cases discussed previously. A court facing this difficult question without the benefit of clear precedent and in the face of new technology will, no doubt, be faced with a daunting task.

C. Are Employers Violating Facebook's Terms of Service?

In addition to the privacy issues that may arise when an employer uses Facebook to screen a potential hire, other legal difficulties may also occur. When a user registers for Facebook and creates a profile on the social networking site, that user must agree to particular terms of use. Any employer who retains, creates, or employs another to use their Facebook access and searching capabilities to locate information about the employer's prospective hires would also be bound by these terms of use. The terms state, in relevant part:

> You understand that . . . programs offered by us on the Site (e.g., Facebook Flyers . . .), the Service and the Site are available *for your personal, non-commercial use only*. You represent, warrant and agree that *no materials of any kind submitted through your account or otherwise posted, transmitted, or shared* by you on or through the Service will violate or infringe upon the rights of any third party. . . ; or

> contain libelous, defamatory or otherwise unlawful material. . . . [Y]ou [further] agree not to use the Service or the Site to:
> *impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity;*
> *intimidate or harass another*;
> *use or attempt to use another's account*, service or system without authorization from the Company, or *create a false identity* on the Service or the Site.[63]

The first portion of the terms of use is selected to emphasize that Facebook is not intended for commercial use. When employers use Facebook or similar social networks as a tool to screen job applicants, are the employers using the networks for commercial purposes? Certainly, employers would not screen potential applicants unless they did so in order to seek out the best human capital for hire and to make their businesses more profitable and successful. Commercial motivation may be one possible interpretation of employers' actions, but it may not be the only reasonable interpretation.[64] Just after stating that Facebook is to be used for noncommercial purposes, the terms of use focus "on materials submitted through your account," not on what one does with information he or she learns about others.[65] For this reason, "'non-commercial use only' could be interpreted as addressing only a prohibition on posting information for commercial gain, such as advertisements."[66]

While noncommercial use may be open for interpretation and, therefore, more difficult to prove, some employers' means of accessing applicants' information on Facebook may violate the terms of use more blatantly. Some employers may be engaged in misrepresentation in direct violation of Facebook's terms of service.[67] This might be the case where an employer pretends they are affiliated with a college in order to gain access to that college's students' profiles (this may include the example of the employee who uses her alumni email address to join her alma mater's network and thereby access enrolled students' posted information). An employee that uses another's Facebook account on a company's behalf (the

---

63. Facebook Terms of Use, http://www.facebook.com/terms.php (last visited Mar. 21, 2008) (emphasis added). Scroll down to the heading titled "User Conduct". The portions of the terms that may affect an employer using Facebook as a background checking tool have been emphasized in italics. The "User Conduct" section of the Facebook Terms of Use are provided in full in Appendix B.

64. *See* Lenard, *supra* note 48.

65. *Id.*

66. *Id.* (emphasis omitted).

67. As provided in the text, the Terms of Use state that one shall not "impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity." Facebook Terms of Use, *supra* note 64.

example of the student "spy" hired by a company to research his or her peers) is also a clear violation of the terms of use policy.[68]

II. CONCLUSION: THINKING PRACTICALLY

As technology continues to advance and the Internet evolves, society can likely benefit from providing students, graduates, and the general population with the ability to access forums like Facebook and to interact in new and more meaningful ways with others in our communities. The Internet has the potential to break down geographic barriers and help people to feel connected to each other in ways they could not previously have imagined. It would be unfortunate indeed if we are all forced to mind our P's and Q's at every turn during our use of this promising medium.

Despite the potential promise of better connections, interactions, and open social communication forums, Facebook users and other social networkers cannot and should not ignore the current threat to their online privacy. Employers are free to use their best judgment as they choose their new employees.[69] Accessing Facebook or another social network to screen candidates is just one more tool the employers have discovered to help them learn as much as they can about the people who could become integral to the success or failure of their companies. Social networkers need to be realistic: their information is not, at the present time, safe from these unauthorized viewers. Privacy settings and blocking tools that limit other social networkers' access should be employed, at minimum, in order to attempt to protect a Facebook user's privacy. Beyond this imperfect attempt to protect information, the only sure way for a social networker to protect his or her private information is to ensure that he or she monitors postings and self-censors posted materials. Perhaps, with the development of technology and improved privacy measures, social networkers will be better able to enjoy the vibrancy and openness that social networks like Facebook can offer.

Perfect privacy settings may not be a realistic short term goal, however, and perfect privacy settings may prevent many of the social interactions that social networkers seek.[70] The solution to this privacy threat can best be resolved by the courts and the legislature. Should courts

---

68. *See id.*

69. Lenard, *supra* note 48 (pointing out that "like it or not, as a general proposition employers are free to make unfair, stupid, arbitrary, and wrongheaded hiring and termination decisions, even based on false information, as long as in doing so they do not violate some specific law.").

70. Query: How can a social networker find strangers with similar interests with whom they can interact if their privacy settings effectively limit those who may view their information to those people they have expressly permitted to access that information (the people they already know)?

acknowledge that Internet users who attempt to limit others' access to their online information have an expectation of privacy in their information, the courts may be able to effectively discourage unauthorized snooping and prying by employers (and other unwanted viewers). If Congress clarifies that it is a priority to protect Internet communication from unauthorized viewers in acts like the Stored Communications Act, this may also create a clear standard of privacy protection.[71] Protecting social networkers' rights to privacy in their information could be the first step toward fostering and encouraging open communication on Internet public forums.

III. APPENDIX A: FACEBOOK'S PRIVACY POLICY

This policy is effective as of October 23, 2006.

Facebook Principles

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

1. You should have control over your personal information. Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control with whom you share that information through the privacy settings on the My Privacy page.

2. You should have access to the information others want to share.

There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that

71. For instance, if Congress removed the exception to the SCA that creates uncertainty as to whether an authorized user can share information with an unauthorized user, this would likely indicate to courts that the legislature's goal and priority is to protect stored communications from unauthorized viewers. Or, Congress could clarify this intention in the SCA by adding a requirement that a Web site's terms of use should govern where a plaintiff's expectation of privacy is concerned. This would likely resolve issues, such as the one in *Konop*, where the terms of use clearly prohibited the manager from accessing the plaintiff's Web page.

information. If you have questions or ideas, please send them to privacy@facebook.com.

Safe Use of Facebook

For information for users and parents about staying safe on Facebook, click here.

Facebook's Privacy Policy

Facebook's Privacy Policy is designed to help you understand how we collect and use the personal information you decide to share, and help you make informed decisions when using Facebook located at www.facebook.com ("Facebook" or "Web Site").

By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.

Facebook is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. This privacy statement covers the site www.facebook.com. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

If you have questions or concerns regarding this statement, you should first contact our privacy staff at privacy@facebook.com. If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily address, you should contact TRUSTe Watchdog at http://www.truste.org/consumers/watchdog_complaint.php. TRUSTe will then serve as a liaison with us to resolve your concerns.

The Information We Collect

When you visit Facebook you provide us with two types of information: personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site.

When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us.

When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies." A cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a

persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature.

When you use Facebook, you may form relationships, send messages, perform searches and queries, form groups, set up events, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information.

You post User Content (as defined in the Facebook Terms of Use) on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.

Any improper collection or misuse of information provided on Facebook is a violation of the Facebook Terms of Service and should be reported to privacy@facebook.com.

If you choose to use our invitation service to tell a friend about our site, we will ask you for your friend's email address. We will automatically send your friend a one-time email inviting him or her to visit the site. Facebook stores this information to send this one-time email, to register a friend connection if your invitation is accepted, and to track the success of our referral program. Your friend may contact us at info@facebook.com to request that we remove this information from our database.

Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.

By using Facebook, you are consenting to have your personal data transferred to and processed in the United States.

Children Under Age 13

Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 is allowed to provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us at info@facebook.com.

Children Between the Ages of 13 and 18

We recommend that minors over the age of 13 ask their parents for permission before sending any information about themselves to anyone over the Internet.

Use of Information Obtained by Facebook

When you register with Facebook, you create your own profile and privacy settings. Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook. We may occasionally use your name and email address to send you notifications regarding new services offered by Facebook that we think you may find valuable.

Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings. In some cases where your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile.

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, network names, and profile picture thumbnail will be available in search results across the Facebook network and those limited pieces of information may be made available to third party search engines. This is primarily so your friends can find you and send a friend request. People who see your name in searches, however, will not be able to access your profile information unless they have a relationship to you (friend, friend of friend, member of your networks, etc.) that allows such access based on your privacy settings.

Facebook will send you only service-related announcements from time to time through the general operation of the service. For instance, if a friend sends you a new message or poke, or someone posts on your wall, you may receive an email alerting you to that fact.

Generally, you may not opt-out of these communications, which are not promotional in nature. If you do not wish to receive them, you have the option to deactivate your account.

Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

We 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 and other users of Facebook, to supplement your profile. Where such information is used, we generally allow you to specify in your privacy settings that you do not want this to be done or to take other actions that limit the connection of this information to your profile (e.g., removing photo tag links).

Sharing Your Information with Third Parties

Facebook is about sharing information with others — friends and people in your networks — while providing you with controls that restrict other third parties from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you. For example: Your news feed and mini-feed may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your news feed and mini-feed here.

Unlike most sites on the Web, Facebook limits access to site information by third party search engine "crawlers" (e.g. Google, Yahoo, MSN, Ask). Facebook blocks access by these engines to personal information beyond your name, profile picture, and limited aggregated data about your profile (e.g. number of wall postings).

We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our

business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Facebook-specified purposes.

In conjunction with the use of the Facebook Development Platform, third parties who agree to abide by the Facebook Development Platform Terms of Service, including restrictions on access, storage and use of such data, may have limited access to your personal information. We have undertaken contractual and technical steps to restrict possible misuse of such information by such third parties, but of course cannot and do not guarantee that all third parties will abide by such agreements. Please report any suspected misuse of information through the Facebook Development Platform here and we will investigate any such claim and take appropriate action against the third party. You may opt-out of any sharing of information through the Facebook Development Platform on the My Privacy page.

We occasionally provide demonstration accounts that allow non-users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.

We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.

We let you choose to share information with marketers or electronic commerce providers through sponsored groups or other on-site offers.

We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service.

If the ownership of all or substantially all of the Facebook business, or individual business units owned by Facebook, Inc., were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in any pre-existing Privacy Policy.

Links

Facebook may contain links to other websites. We are of course not responsible for the privacy practices of other web sites. We encourage our users to be aware when they leave our site to read the privacy statements of each and every web site that collects personally identifiable information. This Privacy Policy applies solely to information collected by Facebook.

Third Party Advertising

Advertisements that appear on Facebook are sometimes delivered (or "served") directly to users by third party advertisers. They automatically receive your IP address when this happens. These third party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer each time they send you an advertisement in order to measure the effectiveness of their ads and to personalize advertising content. In this way, they may compile information about where individuals using your computer or browser saw their advertisements and determine which advertisements are clicked. Facebook does not have access to or control of the cookies that may be placed by the third party advertisers. Third party advertisers have no access to your contact information stored on Facebook unless you choose to share it with them.

This privacy policy covers the use of cookies by Facebook and does not cover the use of cookies or other tracking technologies by any of its advertisers.

Changing or Removing Information

Access and control over most personal information on Facebook is readily available through the profile editing tools. Facebook users may modify or remove any of their profile information at any time by logging into their account. Information will be updated immediately. Individuals who wish to deactivate their Facebook account may do so on the My Account page. Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g., posting on someone else's Wall) you generally cannot remove such communications.

Security

Facebook takes appropriate precautions to protect our users' information. Your account information is located on a secured server behind a firewall. Because email and instant messaging are not recognized as secure communications, we request that you not send private information to us by email or instant messaging services. If you have any questions about the security of Facebook Web Site, please contact us at privacy@facebook.com.

Terms of Use, Notices and Revisions

If you choose to visit Facebook, your visit and any dispute over privacy is subject to this Privacy Policy and our Terms of Use, including limitations on damages, arbitration of, and application of law of the state of California. We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy's effective date. We therefore encourage you to refer to this policy on an ongoing basis so that you understand our current privacy policy. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account.

Contacting the Web Site

If you have any questions about this privacy policy, please contact us at privacy@facebook.com. You may also contact us by mail at 156 University Avenue, Palo Alto, CA 94301.

IV. APPENDIX B: FACEBOOK'S TERMS OF SERVICE

PLEASE READ THESE TERMS OF USE CAREFULLY AS THEY CONTAIN IMPORTANT INFORMATION REGARDING YOUR LEGAL RIGHTS, REMEDIES AND OBLIGATIONS AND SET FORTH VARIOUS LIMITATIONS AND EXCLUSIONS THERETO, INCLUDING WITHOUT LIMITATION A DISPUTE RESOLUTION CLAUSE THAT GOVERNS HOW DISPUTES WILL BE RESOLVED.

Welcome to Facebook, a social utility that connects you with the people around you. The Facebook service and network (collectively, "Facebook" or "the Service") are operated by Facebook, Inc. and its corporate affiliates (collectively, "us", "we" or "the Company"). By accessing or using our web site at www.facebook.com or the mobile version thereof (together the "Site") or by posting a Share Button on your site, you (the "User") signify that you have read, understand and agree to be bound by these Terms of Use ("Terms of Use" or "Agreement"), whether or not you are a registered member of Facebook. We reserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice. If we do this, we will post the changes to these Terms of Use on this page and will indicate at the top of this page the date these terms were last revised. Your continued use of the Service or the Site after any such changes constitutes your acceptance of the new Terms of Use. If you do not agree to abide by these or any future Terms of Use, do not use or access (or continue to use or access) the Service or the Site. It is your responsibility to regularly check the Site to determine if there have been changes to these Terms of Use and to review such changes.

User Conduct

You understand that except for self-service advertising programs offered by us on the Site (e.g., Facebook Flyers), the Service and the Site are available for your personal, non-commercial use only. You represent, warrant and agree that no materials of any kind submitted through your account or otherwise posted or shared by you through the Service will violate or infringe upon the rights of any third party, including copyright, trademark, privacy, publicity or other personal or proprietary rights; or contain libelous, defamatory or otherwise unlawful material. You further agree not to harvest or collect email addresses or other contact information of Users from the Service or the Site by electronic or other means for the purposes of sending unsolicited emails or other unsolicited communications. Additionally, you agree not to use automated scripts to collect information from the Service or the Site or for any other purpose.

You further agree that you may not use the Service or the Site in any unlawful manner or in any other manner that could damage, disable, overburden or impair the Site. In addition, you agree not to use the Service or the Site to:

upload, post, transmit, share, store or otherwise make available any content that we deem to be harmful, threatening, unlawful, defamatory, infringing, abusive, inflammatory, harassing, vulgar, obscene, fraudulent, invasive of privacy or publicity rights, hateful, or racially, ethnically or otherwise objectionable;

register for more than one User account, register for a User account on behalf of an individual other than yourself, or register for a User account on behalf of any group or entity;

impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity;

upload, post, transmit, share or otherwise make available any unsolicited or unauthorized advertising, solicitations, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation;

upload, post, transmit, share, store or otherwise make publicly available on the Site any private information of any third party, including, without limitation, addresses, phone numbers, email addresses, Social Security numbers and credit card numbers;

solicit personal information from anyone under 18 or solicit passwords or personally identifying information for commercial or unlawful purposes;

upload, post, transmit, share or otherwise make available any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

intimidate or harass another;

upload, post, transmit, share, store or otherwise make available content that would constitute, encourage or provide instructions for a criminal offense, violate the rights of any party, or that would otherwise create liability or violate any local, state, national or international law;

use or attempt to use another's account, service or system without authorization from the Company, or create a false identity on the Service or the Site.

upload, post, transmit, share, store or otherwise make available content that, in the sole judgment of Company, is objectionable or which restricts or inhibits any other person from using or enjoying the Site, or

which may expose Company or its Users to any harm or liability of any type.

The Facebook Website lists the following section under its terms of service. However, only the "User Conduct" section (emphasized below) has been provided in this Appendix.

Eligibility, Registration Data, Account Security, Proprietary Rights in Site Content, Limited License, Trademarks, *User Conduct*, User Content Posted on the Site, Facebook Mobile Services, Copyright Complaints, Repeat Infringer Policy, Links to Other Websites and Content, Share Service, Use of Share Links by Online Content Providers, User Disputes, Privacy, Disclaimers, Limitation on Liability, Governing Law; Venue and Jurisdiction, Arbitration, Indemnity, Submissions, Other Questions.

V. APPENDIX C: THE STORED COMMUNICATIONS ACT

§ 2701. Unlawful access to stored communications

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.--The punishment for an offense under subsection (a) of this section is--

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case--

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized-

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.