Facebook: Surveillance and Changing Notions of Privacy in the Social Networking Era

Vanessa Keen

Over the past several years the social networking site Facebook.com has surged exponentially in popularity. From its humble beginnings as a university student network created by a college sophomore, the site has grown into a global phenomenon, including people from all demographics and walks of life. Facebook now has more than 350 million active users (Facebook Statistics, 2009) and is transforming the concept of privacy for about as many people. These people spend an average of 55 minutes a day on the site, sharing a total of 3.5 billion blog posts and status updates a week, and uploading 2.5 billion photos a month (Facebook Statistics). As users voluntarily post information about their favorite books, movies and TV shows, educational history, job records, current location, daily schedules, sexual orientation, political affiliations, and moment-to-moment thoughts, more and more of what once was considered private is now widely available to others. And these others are often not just the handful of friends or members of a closed network one might imagine they're sharing with. As Facebook grows, so does its prevalence as a subject of surveillance. Today, Facebook users are of interest to not just fellow Facebookers, but to companies, advertisers, and the government.

In evaluating Facebook as a subject of surveillance, it is helpful to look at it from a panoptic perspective. The panopticon, originally an 18th century prison prototype designed by Jeremy Bentham, developed into a metaphor of surveillance whereby the many may at anytime be watched by the few. Recognized by French sociologist Michael Foucault as a function of power, the panopticon serves as a system of control driven by visibility. Foucault found this

setup put those being watched into "a state of conscious and permanent visibility that assures the automatic functioning of power" (1977, p. 17). In a journalistic article called "Friend Me if You Facebook: Generation Y and Performative Surveillance," author Westlake considers how the panopticon model can be applied to Facebook (2008). Westlake believes that the Internet as a whole falls under the "panoptic gaze," and that the idea of the United States government secretly patrolling user activity puts them in the metaphorical position of the guard tower of Bentham's original prison design.

However, Westlake goes on to say that the real power the panopticon has on Facebook is that just about anyone can also go up and sit in the guard tower. From that vantage point, users know that at any given time another user may be checking their recent wall posts, their status updates, or their uploaded photos, and as a result he or she engages in a form of self-policing. Citing the work of sociologist Erving Goffman (1959), the article notes that "when the individual presents himself before others, his performance will tend to incorporate and exemplify the officially accredited values of the society, more so, in fact, than does his behavior as a whole" (Westlake, 2008, p. 35). This means that since Facebook users know their activity can and likely will be watched, they strive to fit the social roles they have set out for themselves, and hence agree with society's accepted norms. As a result, Facebook becomes a "forum for the policing and establishing of normative behavior, more than the imagined forum of deviant exhibitionism" (p. 35). In a more outward perspective, users can also play the prison guard, and if they don't like what they see in others' profiles in the form of offensive postings or fake accounts, they can report the infractions to Facebook, the head warden of sorts. They can also more passively punish other users themselves. Westlake explains that a Facebook user who has a noticeably low

number of friends may be considered a socially incompetent loser who does not understand Facebook or is just not "with it." On the other hand, if a user has friends numbering into the thousands, they may be denounced as a "Facebook whore" who is desperate for virtual popularity.

What sets Facebook apart from previous social networking sites is its ability to coerce nearly all users to identify with their true names and their actual school or region. This turn towards authenticity is exactly what makes Facebook feel safer than most other online networks (Myspace for example gained a notorious reputation for attracting pedophiles and sex offenders). It also sets the tone for the type of social exchange that emerges. Since users realize that their full name and affiliations are broadcast for the world to see, there is no opportunity for disgruntled Facebook denizens to hide behind anonymous postings, lessening the opportunity for cyber bullying or faceless trolling (the posting of inflammatory or disruptive content). A user's Facebook "friends" are predominately real life companions or acquaintances. Studies confirm that there is more "Facebook use involving people with whom [users] share an offline connection—either an existing friend, a classmate, someone living near them, or someone they met socially than use involving meeting new people" (Ellison & Lampe, 2007, Abstract section). This trend helps establish the illusion of a gated community, comfortable and relatively close knit, but guarded from unknown visitors.

However this community might not be as protected as many would like to think. Ever since Facebook emerged as a widely used network, warnings have abounded about companies and employers monitoring and screening their applicants or employees. Many may have heard a

story of a potential hire being given the boot after managers came across more heavy drinking and drug references on their profile than they would care to see. So how much are companies really surveilling Facebook users, and is there reason for concern? In an in-depth review of such methods and their legal legitimacy, "The Newest Way to Screen Job Applicants: A Social Networker's Nightmare," author Brandenburg explores how students and recent graduates are "getting more than they bargain for as they attempt to enter the workforce and realize that their blogging and social networking ways can come back to bite them" (2008, p. 598). Brandenburg cites a study done by the popular job-finding site CareerBuilder.com which found that 12% of hiring managers admitted to having screened job applicants by searching their Facebook profile. Of those, 63% have chosen not to hire a candidate based on off-putting information found in their profile (p. 600). In one instance, city administrators in Bozeman Montana required that job candidates give them their username and password to any social networking sites they were on, as part of a background check (Kaste, 2009, para. 7). This caused so much outrage that the employers eventually had to issue a public apology and rescind their new application requirements. Still, such a case does go to show just how aggressive employers are willing to be with online background checks. In defending their actions, managers say that new employees are increasingly given access to sensitive company information and that "given the powerful communication tools in [their] hands, judgment or discretion are increasingly important characteristics for the employees to have" (Brandenburg p. 601).

Even once safely past the hurdles of the hiring process, Facebook accounts can still be surveilled by the employee's company. Like the die-by-the-clock factory foreman of yesteryear, today's employers are prone to close monitoring of their employees' activities, constantly on the

lookout for weakened productivity. In a short article in the April 2008 edition of *Employers Law*, it was reported that an in-depth study of such practices was done by law firm Charles Russell in conjunction with human resource website *Personnel Today*. The study surveyed 220 senior Human Resource professionals about their thoughts on employee Internet and Facebook usage. It found that employers were fearful of "abuse of the system during working hours, inappropriate messaging and breach of the company's code of conduct" (Peacock, p.4), and as a result 69% of employers planned to start monitoring or limiting Internet access, and 70% said they would consider disciplinary action if they found inappropriate Facebook photos identifying the company on an employee's profile (p. 4).

Although many companies are indeed wary of employee Facebook usage, others are more accepting of this new "connected generation" (Warren, 2008, para. 6) and allow, if not encourage, Facebook in the workplace. A study done at the University of Melbourne found that moderate amounts of workplace Internet leisure browsing actually lead to increased productivity (Fahmy, 2009). According to the results, employees who go on Facebook, among other sites, for less than 20% of their total time in the office are actually about 9% more productive than those that don't. "Short and unobtrusive breaks, such as a quick surf of the Internet, enables the mind to rest itself, leading to a higher total net concentration for a days' work, and as a result, increased productivity" (Fahmy, para. 9) explains Brent Coker, the study's director. Perhaps in light of these discoveries, combined with the inevitability of Facebook work breaks (the study also found that 70% of people who use the Internet at work engage in social network browsing), many companies are deciding to work *with* Facebook rather than against it. Currently, over 20,000 companies have signed up on the site (Inside Facebook, 2009), creating their own group

or page (similar to an individual user profile but consists of 'fans' instead of 'friends'). These company pages serve two functions: to connect employees to one and other for business networking, and to promote their company to other Facebook users. Perhaps lured by the fact that it's free and highly hyped more and more companies are actually encouraging their workers to join Facebook; not just so they can monitor them, but also so that they can coordinate and distribute information in new and advanced ways. Company groups serve as a forum where members, mostly employees, can organize and respond to planned events like meetings, conferences, or holiday parties. Discussion board threads about relevant topics can be posted and shared. While many of these tasks could be performed similarly by email or more traditional forms of office communication, social networking sites like Facebook seem to hold new appeal in that they demonstrate "part of the collaborative workplace that is replacing the top-down autocratic style of management of the previous century" (Warren, para. 6). Requiring less pressure on administrators to oversee organization, Facebook company groups democratize the workplace and position everyone on a similar plane of communication and accessibility.

Companies' use of Facebook extends beyond simple inter-office organization, but also helps businesses connect with their clientele and interact with their audience. Proponents of company Facebook pages claim it's not necessarily about selling, but rather about creating a "never-ending conversation with fans" (Pattison, 2009, *Not All About Selling* section para. 1). The same democratization of top-down communication that is seen within companies can also be witnessed in external company-to-client interaction. New York theatre marketing agency Art Meets Commerce is one firm that has found great success in bringing their company to Facebook (Pattison). Their Facebook page for Broadway show "Rock of Ages" has gained over 13,000

fans. Staff members at the firm constantly update the page with streams of photos, video clips, and interviews with the actors, which keep their fans coming back for more. Facebook users flood the page with responses to the content, creating the "never-ending conversation" previously mentioned. While most feedback is positive, users are also not afraid to voice their complaints. For example once Art Meets Commerce posted a video of Paris Hilton endorsing the show, which sent the fans (probably few of which overlap with the famous heiress's fan base) into a tirades of disapproval about how sick they were of seeing Ms. Hilton's face plastered everywhere. "You end up moving away from being an Internet marketer and go into almost customer service," says Jim Glaub, creative director at Art Meets Commerce. "A lot of times people use Facebook to ask questions: What's the student rush? How long is the show? Where's parking? You have to answer." (Pattison, *Not All About Selling* section para. 3)

As Glaub affirms, customer service is an integral component of why companies are entering into the social media world. As customers increasingly move away from traditional methods of complaint about unsatisfactory products or services, and start broadcasting their displeasure through YouTube videos, blogs, or Facebook status updates, companies are learning to respond in kind. This shift to online communication is especially prevalent since these types of complaints are often more damaging to the company's image than a strongly-worded letter or angry phone call. Information management firm Convergys found that "a negative review or comment by a frustrated customer on the Twitter, Facebook or YouTube web sites can lose companies as many as 30 other customers" (Jamieson, 2009, para. 2). Nevertheless, by engaging online with critics and fans alike, companies can often see encouraging results. One of Art Meets

Commerce's other Facebook pages, this one for the off-Broadway musical "Fela!," helped generate "18 million impressions, more than 5,700 clicks and $40,000 in ticket sales" (Pattison, *Not All About Selling* section para. 6).

Companies' surveillance and utilization of Facebook leads nicely into the next overlooked category of Facebook voyeurs: Advertisers. Facebook is a dream come true for these product promoters, who now have almost instant access to the sort of information that market researchers of earlier times could only fantasize of. Much of the material advertisers glean from Facebook accounts is retrieved in an underhanded and ethically questionable way, unbeknownst to all but the most diligent of users. In November 2007 for example, Facebook launched Beacon, a program that took information about Facebook users' online purchases from various other websites, and formatted them into a sort of testimonial advertisement that would appear on the side bar of their friends' home pages (Melber, 2008, p. 23). (For instance, if John Smith bought a ticket to see *The Notebook* on Fandango.com, an advertisement featuring John's profile picture and the words "John Smith just purchased one ticket for *The Notebook* at Fandango!" would be created and displayed.) The effect was a nonconsensual personal endorsement of a product a user may or may not (as is probable in the case of John Smith) want their entire friend network knowing they purchased. This mining of information drew the line for many Facebook users, and within days Beacon had incited a reaction that swept across (a relatively small portion) of Facebook. Moveon.org, a policy action group, created a Facebook group to protest Beacon's unethical methodology and demand restrictions on the advertisements generated. Although the group drew less than 0.2% of Facebook's users, the protest was effectual, and Facebook

eventually buckled and agreed to make the advertisements "opt-in" only—users had to volunteer to have their online purchases announced (p. 23). Mark Zuckerman, creator of Facebook, is quoted as justifying the original Beacon decision behind the defense of creating a service that could be "lightweight [enough so that] it wouldn't get in people's way as they browsed the web, but also clear enough so people would be able to easily control what they shared" (p. 23). However, Ari Melber, expert on Facebook privacy issues, finds this controlled sense of privacy somewhat disconcerting and wonders

> why would people want to browse the web with "lightweight" surveillance broadcasting their pictures and supposed endorsements of products they happen to buy? And why do people continue to give pictures and personal information to a company that reserves the right to use their photos—and their very identities—to sell more advertising, products and market targeting in the future? (p. 23)

His questions, although valid, did not seem to resonate in quite the same way for the majority of Facebook users, who continue to fall into new forms of marketing traps.

Even though Beacon was nixed, other furtive methods of ascertaining Facebook users' information have arrived in its place. One of the latest developments on this front is the Facebook quiz. The quiz is an application run by outside developers that users can choose to add, along with things like Honesty Box (an application where users can post anonymous feedback about a person) or Graffiti Wall (a Microsoft Paint-esque tool to draw pictures on a friend's profile), to their Facebook repertoire. It is touted as a light-hearted amusement, where users answer a series of multiple choice questions to ultimately identify some aspect of their personality or character. Through the online quizzes one can discover "where Kanye West will

next interrupt them" or "which *Sex in The City*" character they are most like. The results are then posted with an accompanying entertaining graphic on their profile and their friends' newsfeeds (Facebook homepages that display a real-time announcement of all friends' various updates). The quizzes are not considered serious evaluations or psychological indicators of any weight, but rather a fun procrastination tool. However, there is a serious side to even the most frivolous of quizzes; the creator of any particular quiz gains access to the entire profile of anyone who then takes it (Kaste, 2009, para. 5). The application essentially scrapes quiz takers' information, unbeknownst to them, and then relays it to the quiz developer. "You think that all you're doing is answering a few innocent questions," an American Civil Liberties Union representative says. "But in fact, you're opening up your entire profile and almost all your personal information to whoever wrote the quiz" (Kaste, para. 9). A large segment of quiz creators are actually companies and advertisers, who are looking to not only create a brand association with Facebook users, but also benefit from the focused and thorough information they can gain from individuals' profiles. In addition, these businesses often use the user's quiz responses to learn even more about them, their lifestyle, and spending habits. RealAge is one such detailed quiz that assigns you a "biological age" based on your family history and health habits. The quiz developers then "take your most sensitive answers—those about sexual difficulties, say, or signs of depression—and sell them to drug companies looking to market medications" (Raphael, 2009, para. 7).

It's not only under-the-radar quiz applications that help marketers get to know their targets; Facebook marketing is verging on the mainstream and transforming the way companies

and advertisers do business. "You need to be where your customers are and your prospective customers are" says Clara Shih, author of marketing guide *The Facebook Era*. "And with 300 million people on Facebook, and still growing, that's increasingly where your audience is for a lot of products and services" (Pattison, 2009, para 3). Facebook can be especially useful for smaller businesses, who may not have the budget for larger scale, traditional forms of advertising, or the power of presence to be very effectual in those mediums. Chris Meyer, a wedding photographer in Woodbury Minnesota, certainly noted such difficulties. (Pattison, Aim at Potential Customers section para. 1) Investing in a full page ad in a wedding magazine was costly and ultimately fruitless, and renting a booth at a wedding industry convention supplied him with only four bookings. Feeling somewhat discouraged, Meyer half-heartedly tried his hand at advertising through Facebook. The results astounded him. Through Facebook's marketing program, he aimed his ads to women aged 22 to 28, located in the Minneapolis area, and who had their relationship status set as "engaged." Such a micro-targeted approach produced outstanding results: Meyers estimates he's spent around $300 on Facebook advertising over the past couple years and as a result has taken home $60,000 in revenue. Over three quarters of his clientele find him through Facebook or recommendations from other Facebook users. "I'd be out of business if I didn't have Facebook," Meyers claims. "Especially with this economy, I need to stretch each marketing dollar as much as I possibly can" (Pattison, Aim at Potential Customers section para. 4).

Facebook has grown so much in usage over the past few years that it's not just nosy companies and hungry advertisers that may be looking at users' Facebooks; the site is also

beginning to be surveilled by the government. There is significant concern that in this age of "war on terror"; when the government seems to need less and less reason to tap phone lines or intercept mail, social networking sites are a growing target for surveillance. Facebook's privacy policy offhandedly admits to potentially sharing user information with third parties and the government, without giving very clear guidelines as to when this could occur (Facebook's Privacy Policy, 2009). Such partnerships with the government may have been going on for much longer than many are aware of. A 2006 report by *New Scientist* magazine reported that the "Pentagon's National Security Agency is funding research into harvesting personal information posted on social networking sites in order to 'build extensive, all-embracing personal profiles of individuals'" (Cohen, 2008, p. 16). A common and perhaps not unfounded response to this is "so what? Sure it's a little weird that the government is looking at my site, but I've got nothing to hide." Addressing this sort of indifference, Melber (2007) suggests a few likely scenarios in which government surveillance could potentially make almost any Facebook user a target of interest. Your profile "might list a criminal suspect among your 700 'friends,' or place you at the scene of a crime" (Melber, p. 22), and suddenly you may find yourself in an interrogating room trying to deny any connection. In a national surveillance state, a condition Melber argues we currently live in, government surveillance restraints and norms are transforming rapidly. As the government circumvents the traditional criminal justice system, justifying the lack of procedure as a matter of national security and anti-terror measures, Melber believes that "soon, the Executive [will be] increasingly tempted to make use of that parallel system for everything from domestic misdemeanors to undemocratic abuses" (p. 23). This has been a trend in the past,

it's happening now in other forums, and Facebook surveilling could easily fall under this ever widening category.

Although much of the information about how the United States government is using Facebook remains hazy, not everyone is satisfied to simply leave their suspicion up to speculation. The Electronic Frontier Foundation, a public interest group dedicated to fighting for technology regulations, recently sued the CIA and Department of Defense, in order to find out exactly how the governmental agencies are using Facebook and other social networking sites in their investigations (Twitter Tapping, 2009, para. 5). Working under the Freedom of Information Act (legislation that guarantees the right to data held by the state), The Electronic Frontier Foundation was incited to action after a recent range of unsettling stories came to light. For example, *Wired* magazine reported that In-Q-Tel, the investment branch of the CIA, invested in a software firm called Visible Technologies which specializes in monitoring online social media (Shachtman, 2009). Visible Technologies offers a program that crawls through millions of websites, looking through blogs, online forums, and social networking profiles. It then rates and labels whether the content is positive or negative and how influential the posting or author is, in order for employees to go back and manually investigate anything that is marked as suspicious (Shachtman, para. 9). Meanwhile, the *Wall Street Journal* reported that state revenue agents have been searching for tax evaders by patrolling through Facebook and that the FBI had searched the home of man suspected of coordinating protests against the global finance organization Group of Twenty meeting via Twitter (Twitter Tapping, para. 2). These types of incidences, many of which probably never make it to the press, greatly concern the Electronic Frontier Foundation, who want the government to come clean about their cyber social

monitoring. Echoing the Foundation's concerns, Steven Aftergood, who tracks intelligence issues for the Federation of American Scientists explains

> even if information is openly gathered by intelligence agencies it would still be problematic if it were used for unauthorized domestic investigations or operations. Intelligence agencies or employees might be tempted to use the tools at their disposal to compile information on political figures, critics, journalists or others, and to exploit such information for political advantage. That is not permissible even if all of the information in question is technically 'open source.' (Shachtman, para. 11)

Until the Electronic Frontier Foundation's lawsuit goes through, it may be difficult to know exactly how the United States government is monitoring Facebook. However it has become clear that more localized governments and jurisdictions are certainly employing the advantages of ease and accessibility that Facebook provides them in surveying their citizens. There are countless examples of Facebook being used to deter crime or to decide the fate of the accused in a court of law. In Tilonsburgh, Ontario, police were tipped off to a Facebook event called the "Wabash Party," a festivity in the forest with 716 invitees confirming attendance (Niedzviecki, 2009, p. 247). The event's wall consisted of excited chatter about the upcoming celebration, with people boasting comments like "this party is gonna be a real mess!". The event's profile picture featured two people passed out on a pile of beer cans. The Ontario Provincial Police responded by issuing a public statement that anyone attending the party would be monitored for underage drinking, illegal drug use, and trespassing. The party was cancelled. In the coastal town of Torbay, England, police found a Facebook event broadcasting a beach

party which 7,000 people had RSVP'd to (p. 247). As a response, law enforcement placed a 24 hour ban of any public alcohol consumption in the area. The next day the event creator posted this message to the anticipatory revel goers: "People attending beaches in Torbay this weekend will be asked to leave or be arrested. Do not travel to Torbay. There will be high police presence around the coast. No event whatsoever will taking place in Torbay, and we urge you to inform all others who are planning to attend that it is no longer going ahead" (p. 247).

Even if one does manage to commit an offense before the police grow wise to it, Facebook can still play a large role in deciding the perpetrator's fate. Joshua Lipton, a Rhode Island college student, went drunk driving one night, lost control of his vehicle, and caused a three car pileup, severely injuring one young woman (Niedzviecki, p. 248). The next week was Halloween, and Lipton thought it would be funny to hit the party circuit in a pin-striped Jail-Bird costume, an ironic means of owning his newfound criminal status. When it came time for his court date, the prosecuting lawyer pulled up a PowerPoint slideshow featuring photos of Lipton's Halloween night—all acquired from his public access Facebook. The judge was not amused, and elected to give Lipton the maximum two year jail sentence. In another drunk driving case, Jessica Binkerk of Santa Barbara California killed her crash victim (p. 248). Binkerd's lawyer advised her several times to take down her Facebook, which featured a slew of unflattering photos of her engaging in obvious drinking behavior. She refused, and at her trial the prosecutor touted evidence about her character by pulling up these exact photos of her. "In one, Binkerd is wearing a shirt advertising tequila. In another, she's sporting a belt lined with plastic

shotglasses" (p. 248). Swayed strongly by the visuals, the judge sentenced her to over five years of jail time.

Perhaps what best ties these three surveillance powers (companies, advertisers, and the government) together is Facebook's users' largely passive reaction to them. Yes, sometimes reactionary forums pop up from a small percentage of users who object to some component of their panoptic presence—as was the case with the Beacon development—but for the most part surveillance seems to be a matter of little concern. One survey concluded that 90% of Facebook users have never read the site's privacy policy, and 60% claimed they weren't at all worried about their privacy (Niedzviecki, p. 213). A very interesting study presented at the Security and Human Behavior Workshop in Boston found that this sort of apathy wasn't exclusive to Facebook (p. 214). The researchers surveyed college students via email, inquiring whether they had ever engaged in any sort of illegal or imprudent activities. Half the students were assured that the information they gave out would stay completely confidential and their privacy protected, while the other half received no word whatsoever about any sort of privacy measures. Ironically, the first group was more hesitant to admit their offences than the group that had no idea how their responses would be used. 25% of the privacy-assured group admitted to copying homework, while a doubling total of 50% of the group who received no privacy disclaimer admitted copying (p. 214). The same team did another experiment in which they again surveyed college students about illicit activity. This time one group completed a survey on an official looking college website, while the other group answered the same questions but on a jazzy, fun-looking website with a headline reading "How BAD are U???" (Niedzviecki, p. 214).

Respondents were far more likely to report misdemeanors and crimes, such as illegal drug use, on the more whimsical looking site—even though they had no idea with whom the site was affiliated with. From these studies, it can be concluded that Internet users do not naturally think about privacy. They are willing to divulge information to anonymous sources, which they liken more to "sharing" rather than "disclosing." Privacy only seems to even enter their minds when it is specifically pointed out to them or linked with some sort of bureaucracy or institution.

Facebook plays a significant role in the changing principals of personal information distribution and new conceptions of privacy. The majority of Facebook users have grown up in a different sort of society, one where reality TV shows and celebrity gossip are cultural mainstays and where standards of what is private and what is not have drastically departed from previous eras'. These users will rarely think twice about posting intimate information such as sexual orientation, personal photos, and provocative status updates for hundreds, if not thousands of people to see. Even if they aren't particularly keen on mass broadcasting their Facebook updates, it can almost feel counterintuitive not to. "Interestingly, the defaults [for Facebook] are set to increase social awareness" points out Clay Shirkey, professor of new media at New York University. "It's not that they're defaulting to private and letting us make it public, they're defaulting to public and letting us make it private" ("SwitchedShow", 2007). The situation of private-going-public is augmented by the fact that a relatively small percentage of users explore settings beyond the default ones dictated by Facebook, as well as the belief that "giving out information is social" (Siegal, 2009)—or so concludes Bryan Listen, a 22 year old and typical Facebook user, on a National Public Radio interview about privacy.

And that's exactly what Facebook is about—being social. Some traditionalists may turn their nose up at the idea of human sociability being enacted across screens, but the Department of Telecommunication, Information Studies, and Media at Michigan State University doesn't find the concept so far-fetched. After surveying and analyzing the Facebook patterns of hundreds of college students, they found that there is "a positive relationship between certain kinds of Facebook use and the maintenance and creation of social capital" (Ellison & Lampe, 2007, Discussion section). Social capital refers broadly to the resources gained through relationships with others. This can include anything from job opportunities, useful information, or companionship. Social capital is linked to epic civil improvement, such as a healthier economy and lower crime rates. Most importantly, it relates directly to psychological wellbeing in the form of satisfaction with life and self-esteem. The Michigan State researchers questioned students on the quality of various other aspects of their life, such as their attitudes toward themselves and their college experience. They found that "less intense Facebook users, students who reported low satisfaction with college life, also reported having much lower bridging social capital than those who used Facebook more intensely. The same was true for self-esteem" (Ellison & Lampe, Discussion section). Whether they are aware of it or not, this positive correlation between Facebook and general sense of wellbeing is an important motivating factor as to why people continue to immerse themselves in the site. When comparing these motivations to importance of security of personal information, it becomes clear that "many of us don't value our privacy nearly as much as the possibility of meaningful connection, convenience, and rewards like attention and even remuneration" (Niedzviecki, 2009, p. 232).

This is not to say that Facebook users have no appreciation of privacy, but rather implies that their ideas of what privacy *means* are changing. Privacy is no longer an absolute ("some things are just private") but instead, a function of control. Facebook users do value their privacy to a certain extent, but consider it something which they can exert control over ("I'll let some people see my profile, but not everyone"). This control, which leads to a perceived audience of people whom a user shares real life connections with, is one of the defining features of Facebook and ultimately what makes it so popular. However, more often than not, Facebook users, who believe they are exerting at least some control over their profile content, are unaware of just how many people really do have access to their personal information.

It is unlikely that we will revert back to prior notions of privacy anytime soon. This is in part due to the fact that our loss of privacy extends beyond social networking sites, and into almost all aspects of life. Credit card transactions are carefully monitored, toll booths remember our license plates, social security numbers are demanded indiscriminately, and everywhere we go cameras seem to be filming our trail. There is a type of technological determinism at work, driven by will, that seems to dictate that we continue handing over personal information and creating technology that will be able to categorize, track, and tattle on us. With this wide-spread theme of omnipresent surveillance and information accessibility reigning over us, people are unlikely to find Facebook voyeurism especially offensive. Users deleting their Facebook accounts en masse, and renouncing all wall posts, photos uploaded, and comments shared with friends probably won't happen any time soon. For now at least, the rewards of social-networking and sharing of self are too great to pull the plug on just yet.

What does need to happen however, is an honest appraisal of our new privacy values and a reexamination of how our society—including the scopophilic forces of companies, advertisers, and government agencies, work within these. The age of social media is still new, so new that old privacy laws fail to reflect the changing digital landscape, and that new laws have yet to be created to keep up with the change. In this transitional period from absolute privacy to controlled privacy, from face-to-face interactions to online sociability, it is essential that a discourse, or at least awareness, about these issues is raised. The meaning of privacy may be shifting, but the core value behind it still exists. So log on Facebook—take a quiz, find out which Disney Princess you are, maybe even post a comment or two—but just remember, what you do in your private time may not be so private after all.

References

Brandenburg, C. (2008). The newest way to screen job applicants*:* a social networker's nightmare. *Federal Communications Law Journal, 60* (3), 597-627. Retrieved from http://www.law.indiana.edu/fclj/pubs/v60/no3/11-Brandenburg.pdf

Cohen, N. (2008). The valorization of surveillance: towards a political economy of facebook. *Democratic Communiqué, 22* (1), 5-22.

Ellison, N. & Lampe, C. (July 2007). The benefits of facebook ‘‘friends:’’ social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4). Retrieved from http://jcmc.indiana.edu/vol12/issue4/ellison.html

Facebook’s privacy policy. (2009). Retrieved from http://www.facebook.com/policy.php

Facebook statistics. (2009). Retrieved from http://www.facebook.com/press/info.php?statistics

Fahmy, M. (2009, April 2). Facebook, youtube at work make better employees: study. *Reuters*. Retrieved from http://uk.reuters.com/article/idUKTRE5313G220090402?pageNumber=2&virtualBrandChannel=0

Foucault, M. (1977). *Discipline and punish*: *The birth of the prison*. New York: Vantage.

Inside facebook. (2009). Retrieved from http://www.insidefacebook.com/complete-list-of-21655-companies-on-facebook

Jamieson, A. (2009, December 13). Silent majority risk worse customer service as companies monitor twitter, facebook. *Telegraph*. Retrieved from http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/6802019/Silent-majority-risk-worse-customer-service-as-companies-monitor-Twitter-Facebook.html

Kaste, M. (2009). *Is your facebook profile as private as you think.* Retrieved from http://www.npr.org/templates/story/story.php?storyId=114187478

Melber, A. (2007, December 27). Facebook and the national surveillance state. *Huffington Post.* Retrieved from http://www.huffingtonpost.com/ari-melber/facebook-the-national-sur_b_78376.html

Melber, A. (2008). About facebook. *The Nation, 286* (1), 22-24. Retrieved from http://www.thenation.com/doc/20080107/melber

Niedzviecki, H. (2009). *The peep diaries: How we're learning to love watching ourselves and our neighbors.* San Francisco: City Light Books.

Pattison, K. (2009, November 11). How to market your business with facebook. *The New York Times.* Retrieved from http://www.nytimes.com/2009/11/12/business/smallbusiness/12guide.html?scp=1&sq=companies+use+facebook&st=nyt

Peacock, L. (2008). Employers watch facebook usage. *Employers Law,* 4. Retrieved from http://www.personneltoday.com/articles/2008/04/14/45172/employers-watch-facebook-usage.html

Raphael, J. R. (2009, May 13). Facebook quizzes: beware the hidden dangers. *CIO*. Retrieved from http://www.cio.com/article/492617/Facebook_Quizzes_Beware_the_Hidden_Dangers?page=1&taxonomyId=3089

Shachtman, N. (2009, October 19). Exclusive: US spies buy stake in firm that monitors blogs, tweets. *Wired*. Retrieved from http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/

Siegal, R. & Block, M. (2009, October 27). Is your facebook profile as private as you think. *All Things Considered Podcast*. Podcast retrieved from http://www.npr.org/templates/player/mediaPlayer.html?action=1&t=1&islist=false&id=114187478&m=114216186

SwitchedShow. (2007, November 6). Facebook killed the private life [Video File]. Video posted to http://www.youtube.com/watch?v=azIW1xjSTCo

Twitter tapping. (2009, December 12). *The New York Times.* Retrieved from http://www.nytimes.com/2009/12/13/opinion/13sun2.html?_r=1&scp=2&sq=facebook+government&st=nyt

Warren, B. (2008). *Facebook as a business tool: using social networking to communicate, campaign, and connect*. Retrieved from http://socialtagging.suite101.com/article.cfm/facebook_at_work#ixzz0ZgNJooXK

Westlake, E. J. (2008). Friend me if you facebook: generation y and performative surveillance. *TDR: The Drama Review, 52* (4), 21-41. Retrieved from http://muse.jhu.edu/journals/the_drama_review/v052/52.4.westlake.html