The Impact of Online Social Networking: Facebook and the Publicization of Users' Private Lives

by Aspasia Tsaoussi

Lecturer in Sociology of Law, Faculty of Law (AUTh)

Abstract

Online social networking services such as Facebook, Twitter and LinkedIn have proliferated in recent years. In this paper, we will focus on the impact of Facebook, which is the network with the most users worldwide (as of March 2011 Facebook had more than 640 million registered users). Facebook has multiple uses: it is potentially and concurrently a dating site, a friend locator, and a public relations tool. We examine both the positive and the negative repercussions of the Facebook phenomenon. We then look more closely at one of its main effects: the fact that it serves to efface the boundaries in the traditional public/private dichotomy. Supposedly Facebook protects its users through privacy settings. Yet users add personal details (like email addresses, cell phone numbers, and photos). If something goes wrong, questions arise as to the legal relationship that users have agreed to. Who has access to their personal information? What is the meaning of the Facebook disclaimer in its "Terms of Service" (the online equivalent of "fine print" in contracts of adhesion)? Perhaps only lawyers know that under Facebook's ToS, users give up copyright control of any material posted. As a result, laypersons at best remain partially protected. Privacy issues and data protection concerns (esp. protecting users who cannot protect themselves, such as minors under 18 who regularly use the medium) clash with freedom of expression/freedom of speech/freedom of information. The legislator concerned with efficiently regulating the use of online social networks needs to accommodate these conflicts, devising wise and balanced solutions.

1. Introduction

Online social networking services such as Facebook, Twitter and LinkedIn have proliferated in recent years. In this paper, we will focus on the impact of Facebook, which is the network with the most users worldwide. As of March 2011, Facebook had more than 640 million registered users. The typical user spends about 20 minutes a day on the site, and two-thirds of users log in at least once a day (Cassidy 2006). What started in early 2004 as a Harvard-only service (intended originally for the elite online communities of Harvard, Stanford and Yale) has become a global phenomenon unprecedented in magnitude and popularity.

Three of the features that explain Facebook's popularity are the following:

(a) Users can exchange messages, including automatic notifications when they update their profile,

(b) They can join common interest user groups (organized by workplace, school, or college, or other characteristics)

(c) Build "Applications" which allow users to personalize their profiles and perform other tasks (compare movie preferences, etc).

If we tried to answer the question "what is Facebook?", we would come up with a number of different replies that all fittingly describe what Facebook *is* and what Facebook *does*:

- ❖ Social network
- ❖ A social utility
- ❖ Mega social-media site
- ❖ Dating service[1]
- ❖ Professional network
- ❖ Generator of social norms (*cf* Netiquette)
- ❖ Agent of socialization
- ❖ A phenomenon (the "Facebook effect")

According to Mark Zuckerberg, its co-founder and chief executive, Facebook was designed and intended to be a social utility. In David Kirkpatrick's best-selling book about *The Facebook Effect*, Mark Zuckerberg and his comrades are quoted repeated as believing that Facebook is different because it is a social utility. Facebook never wanted to be a social network site; it wanted to be a social utility. Thus, it shouldn't surprise anyone that Facebook functions as a utility.[2]

At its basis, Facebook (like other social networking sites, such as Twitter), reflects the tendency of many individuals to communicate with other persons they do not know. Through hobby descriptions, funny wall posts and photographs, Facebook and other Social Networking Sites have tapped into a common human desire, attention (Rosen 2007). A virtual playground for sociable extroverts, Facebook also hosts introverted personalities, former classmates, current colleagues, acquaintances, sexual partners, fans and collectors. Everyone that a person wants to connect with is baptised "a friend".

Online Social Networks are teaching their users new social norms. In the offline world social norms of general etiquette and privacy are enforced; in the online world the social barriers have changed (Rosen 2007). People can view other people's profiles privately and a new form of etiquette is created. What does it mean socially and culturally to decline a friend request? What if this friend request was addressed to us by a colleague we are not particularly fond of? In this case, by declining the friend request we are reinforcing our dislike and (more importantly) signaling this dislike to the person who extended the invitation. It is clear that our behavior in the virtual online world has an impact on the offline real world…

For many professionals, Facebook has become a medium that enables connections. In recent years, it has been used interchangeably with more strictly professional online services such as LinkedIn. Many users open accounts to expand their social networks, locate old classmates, college room mates, army buddies, etc. It is a glorification of Mark Granovetter's observation that it is "the strength of weak ties" that holds together a social network (Granovetter 1973).[3]

---

[1] Facebook hosts several dating services like Zoosk, successfully replacing previous dating websites of the past, e.g. SixDegrees.com, an unsuccessful site that operated from 1997-2000. Zoosk is the largest online dating service designed for social networks such as Facebook. Today over 20 million members use the Zoosk dating application on Facebook. It is also characteristic that Early Social Networking was mainly focused on dating.

[2] http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html

[3] Mark Granovetter, an American sociologist at Stanford University, was a pioneer in social network analysis and revived the virtually defunct interdisciplinary field of Economic Sociology in the late 1970s to mid-1980s. "The Strength of Weak Ties" was among his most influential works. In it, he argues that most intuitive notions of the "strength" of an interpersonal tie should be satisfied by the following definition: the strength of a tie is a (probably

Other users give emphasis to political deliberations online, struggling to raise their friends' awareness on a number of social, cultural, health and political issues: joining various "causes" on Facebook serves precisely this purpose. Facebook allows users to disseminate information, promote awareness and create online communities that share common goals.

The Internet has produced revolutions in many kinds of behavior, such as greatly reducing the advantages from reading newspapers, but one of the most important is in providing easy access to various kinds of social interactions. It is fairest to say that users of online social networking are pursuing a variety of interests online. At the same time, "Facebook offers a socially compelling platform that also facilitates peer-to-peer privacy violations: users harming each others' privacy interests" (Grimmelman 2009: 1137).

2. The Benefits of Facebook

A social scientist's rough first listing of the manifested benefits of Facebook could ;ppl something like this:

- ❖ Social connectivity
- ❖ It builds bridging social capital
- ❖ Networking
- ❖ Entertainment and pastime[4]
- ❖ Exchange of information
- ❖ Increased social awareness
- ❖ Engagement in "causes"

Among these benefits, we should single out its potential to connect people. Social connectivity has been extensively explored in the past ten years. The most influential precursor theory was the "small world" thesis of sociologist Stanley Milgram. In 1967, Milgram conducted conducted experiments examining the average path length for social networks of people in the United States. The research was groundbreaking in that it suggested that human society is a small world type network characterized by short path lengths. The experiments are often associated with the phrase "six degrees of separation", although Milgram did not use this term himself.

Social networking websites such as Friendster, MySpace, XING, Orkut, Cyworld, Bebo and of course Facebook, have greatly increased the connectivity of the online space through the application of social networking concepts. In 1998, Duncan J. Watts and Steven Strogatz from Cornell University published the first network model on the small-world phenomenon. They showed that networks from both the natural and man-made world, such as the neural network of C. elegans and power grids, exhibit the small-world phenomenon. Generally, their model demonstrated the truth in Mark Granovetter's pioneering work on the spread of information in social networks. Watts combined his own research in network theory with summaries of the work of others to examine networks from a new perspective (Watts 2004).

---

linear) combination of the amount of time, the emotional intensity, the intimacy (mutual confiding), and the reciprocal services which characterize the tie.

[4] By posting, sharing or reading humorous quotes, watching funny videos, etc. Some one-liners gleaned from friends' recent wall posts include: "I used to be schizophrenic, but we're all right now" and in response to an **"OMG, I'm getting married!!"** status update, "Bigamy: one wife too many. Monogamy: same thing**".**

Today with the use of online networks, the foremost expert in the new science of networks, theorist Albert-László Barabási believes that "the number of social links an individual can actively maintain has increased dramatically" bringing down the six degrees down to about three (Barabási 2003).[5] According to the recently published insightful book *Connected,* authored by Nicholas Christakis and James Fowler, five basic rules describe the relationship between individuals and their networks, including mutual adaptation, the influence of friends and friends' friends, the network's "life of its own". Networks do more than promote the good of the group: they also spread contagions; create "epidemics" of obesity, smoking and substance abuse; disseminate fads and markets; alter voting patterns, and more (Christakis and Fowler 2011).

But how strong are the ties between Facebook "friends"? Recent Facebook statistics reveals that the average Facebook user has 150 friends, who are actually acquaintances. The average user (regardless of number of friends) has only five close friends on Facebook. A user actively follows only 8 percent of his/her Facebook friends, regularly communicates with 4 percent and keeps in close touch with about 2 percent. Most Facebook users just don't have the time and/or the desire to follow 86 percent of his/her virtual friends.

Users may be quick to forge ties and send friend requests, but they have been proven just as quick in "defriending" their virtual online friends. Once a Facebook friend becomes oppressive, harassing, vindictive, or just plain annoying, there is always the "remove friend" option that aims to remedy the damage that is done. The "defriending phenomenon" is quite interesting from a social-psychological point of view, but it is not within the scope of this paper to explore it. For the purposes of our analysis, we will concur with Schoenberger (2009) that the defriending phenomenon shows how very little the word "friend" means in the context of social media.[6]

Nevertheless, Ellison et al. (2007) have found a strong association between use of Facebook and bridging, not bonding, social capital. Bonding social capital is between individuals in tight relationships, such as family and close friends-- bridging is "weak ties," which are loose connections between individuals who may provide useful information or new perspectives for one another but typically not emotional support. According to Robert Putnam, bridging social capital is considered to be better-suited for linking to external assets and for information diffusion (Putnam 2000). As Ellison et al. point out, members of weak-tie networks are thought to be outward looking and to include people from a broad range of backgrounds (*id*). The social capital created by these networks generates broader identities and generalized reciprocity.

3. Publicizing the Private: Facebook's privacy concerns

Despite the benefits of connectivity, there are dangers connected with Facebook use. With their daily wall posts, Facebook users are daily and to a great extent subconsciously engaged in the process of *publicizing their private sphere*. This may have dire and unanticipated consequences for their lives. They may find themselves losing their job or spouse or circle of friends. Employees who have called in to work declaring they're ill and are going to take the day off to

---

[5] Barabási's book shows that networks (social network of friends, the web's five billion websites, the biological food chain, business and commerce, the growth of cities, intra-cellular proteins, and so on) can be quantified and described with the same type of mathematical laws. These different types of networks share the same properties. By understanding how networks function and grow, one can develop strategies to take advantage of that growth (http://www.andreas.com/faq-barabasi.html).

[6] In her words, "if you can willy nilly defriend someone – they probably were never a friend at all".

recuperate then go on to post lovely photos from their day trip to the nearest beach or zoo or fun spot of their choice. As a result, they are discharged.[7] Teachers who post racist comments are dismissed from their posts. Students are sent to the principal's office for derogatory information they posted on Facebook about the school or their teachers. Philandering boyfriends or girlfriends are caught red-handed as a well-meaning Facebook "friend" posts something relevant to their weekend activity. Couples break up, spouses divorce, friends are distanced. Declaring their Relationship status has imposed tremendous amounts of pressure on users of all ages, has given rise to misunderstandings and has made personal relationships even more fragile to maintain.

Many Facebook users have profiles about themselves, some with more detailed information than others. Who protects the privacy of Facebook users' data? Who owns our online personas? If we post information on a social networking site or write a blog post, who owns the data? Before we discuss further the privacy issues that arise from the use of Facebook, some definitions of basic terminology are necessary. Users post personal information on their Facebook pages. But what exactly is *"personal data"*? It is information which can be used, either alone or when combined with other information that is linkable to a specific individual, in order to distinguish or trace that individual's identity. A person's name, photograph, signature or tax registry number are some characteristic examples of such data, which are linked to a specific person.

The greatest danger inherent in posting personal data is *leakage* (also known as *Data Mining*), defined as the capability of third parties to link Personal Data obtained from Social Networking Sites with user actions both within and outside those Sites. Leakage of information occurs in many ways. For example, Facebook's "friend of a friend" feature potentially exposes personal data to third parties. One pernicious use of this type of data is by unscrupulous marketers who mine their friends' networks for business prospects.

3.1.
Advertisements, Games and Applications

Facebook's 2010 profit was estimated at $600 million (with the fourth quarter net at $250 million and still rising (Carlson 2011). Facebook makes most of its money off brand advertising, ads that send users to virtual games like CityVille and group-buying sites, and a 30 percent tax on Facebook credits.

Advertisements
Internet marketing specialists and online advertisers can pinpoint potential customers through specific details. The ads correspond to the interests that a user states in his/her profile. Facebook advertising is so successful because of the many ways in which audiences are targeted: by location, age, gender, education, place of employment, type of employment, relationship status, interests, languages and the purchasing preferences and habits of friends.

There were over 176 billion display ads in Facebook in 2010. Facebook derives its revenues from advertisements (e.g. banner advertisements from Microsoft), games, credits[8] and

---

[7] http://www.fastcompany.com/1723915/six-ways-your-online-privacy-is-at-risk

[8] Credits are an online currency unique to Facebook users. Members purchase 10 credits a dollar and can use this virtual money to purchase goods and play games. Facebook receives 30% of all credit transactions. Some claim that credits have the potential to be one of the strongest standardized debit systems in the world. If credits expand beyond Facebook apps and this proves to be successful, then they may become a global mobile payment platform.

gifts.[9] The revenues are not disclosed—they have to be estimated (some place the figure from $1 to $1.1 billion in 2010). Facebook itself has stated that its advertisers have quadrupled since 2009.[10] In this era where the world wide web reigns supreme, social networks are mega-profit generators. The title of a recent book is characteristic: *The Facebook Era: Tapping Online Social Networks to Build Better Products, Reach New Audiences, and Sell More Stuff* (Shih 2009).

There are companies that have vast databases because they collect as much information about users as possible. The value of these databases is huge. For example, if a data aggregator knows that I like chess, that small nugget of information is very valuable to advertisers. When Facebook basically lays the path for data aggregators to access this information about me, a number of potential privacy issues arise. This is possible through the use of tracking cookies,[11] widely used by advertisers to monitor who clicks on their ads.

Third party applications

Quizzes, games and all sorts of applications created by third users or companies, provided as add-ons. They are hosted by the website and they are not restricted by their host's Privacy Policy. Capitalizing on this freedom, they openly state that in order to function, the user must accept that they will have full access to all of the data on his page, often on his friends' pages as well.[12]

There are currently over 550,000 applications on Facebook. According to recent statistics, 70 percent of users engage with applications each month. There are one million application developers. The profit generating potential attracts them. It is characteristic that Zynga, the top application developer, made $250 million in 2009 --and $80 to $150 million of that was estimated to be profit, more net profit than Facebook itself made.

3.2. Facebook's privacy policy

Facebook has a privacy policy. It clearly states that it will not sell its users' information to advertisers without consent, and arguably has not violated that promise. However, in the same Privacy Policy, users are told that application providers will be supplied with users' names and other information that the user makes public.

The breakdown is that the application makers (e.g. Farmville) allow the user information to get to advertisers, which is apparently a breach of Facebook's terms with its application providers. Facebook responded by shutting down the violating application makers in 2010. This was hailed as a great first step. Facebook also announced that it was unaware of the UID transmission and that most application makers probably had no idea the UIDs were transmitted.

Despite this gesture of good faith, Facebook has progressively shrunk its privacy policy to fit its business interests, narrowly conceived. At best, Facebook's privacy policy in the past two years can be described as eroding, as demonstrated below:

---

[9] Facebook owns a virtual gift shop, where virtual goods can be purchased by users, using the credit payment system.

[10] http://www.msnbc.msn.com/id/41521349/ns/business-us_business/

[11] A tracking cookie is a piece of text stored by a user's web browser. A cookie can be used for authentication, storing site preferences, shopping cart contents, the identifier for a server based session, or anything else that can be accomplished through storing text data.

[12] The problem is spreading, as Android and iPhone applications have been reported to function in a similar manner.

In early 2009:

> …Information *may be accessed by everyone on the Internet* (including people not logged into Facebook ,…*and may be imported and exported by us and others without privacy limitations…*

In December of 2009:

> …your name, profile photo, list of friends and *pages you are a fan of*, gender, geographic region, and networks you belong to *are considered publicly available to everyone ….*

In 2010:

> ……*If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection…*

The Wall Street Journal wrote a series of articles in October 2010 about Facebook and other social media sites passing User Identifications (UIDs) to its advertisers. Also, the New York Times in a May 25, 2010 op-ed wondered "Should Government Take on Facebook?"[13] One fairly straightforward answer to the aforementioned question is that the government "can force Facebook to switch its defaults on its new Instant Personalization program" (Scoble 2010). The program is already being used for example by several websites like Yelp and Pandora, which Facebook calls "partner sites".[14] And it certainly is not in the financial interest of Facebook to have this opt-in, but it definitely is in the interest of the consumers.

Today, Facebook shifts the burden to users to turn off UIDs on each of the partner sites they visit. The relevant Facebook message appears only to the knowledgeable, well-informed users. Once in your Facebook account, you need to visit "My Account", then click on "Privacy settings", then click on "Apps and Websites" at the lower left-hand side of the page. You then scroll down to "Instant personalization" and you click on the "Edit settings" button. What you see is this:

> Currently, we've partnered with a few websites to provide you with great, personalized experiences the moment you arrive, such as immediately playing the music you like or displaying friends' reviews. To tailor your experience, these partners only access public information (like your name and profile picture) and information available to everyone. When you first arrive at the following sites, you'll see a notification message and an option to turn off the personalized experience:
> - Bing - Social Search
> - Pandora - Personalized Music
> - Trip Advisor - Social Travel
> - Yelp - Friends' Local Reviews
> - Rotten Tomatoes - Friends' Movie Reviews
> - Clicker - Personalized TV Recommendations
> - Scribd - Social Reading
> - Docs - Document Collaboration

---

[13] http://roomfordebate.blogs.nytimes.com/2010/05/25/should-government-take-on-facebook/

[14] You can see which music I listen to, for instance, on Pandora, a feature which got turned on automatically. The government could force Facebook to turn that feature off by default and make me "opt in" for you to see my Pandora music.

At that point, the user must make sure that the "Enable instant personalization on partner websites" is unchecked. This is the only way the user can be certain that instant personalization on partner sites is turned off.

Users must be very careful and very cautious: the UID for users can be used to look up all of their public information. The UID does not allow access to information that the user has chosen to make private through privacy controls. Basically, if you are a Facebook user you cannot hide your name and gender, *but everything else can be hidden*.

This option to hide all personal information lies in the heart of the main counter-argument to all these privacy concerns: every single user of the service has the power to avoid privacy concerns by no longer using the service. In the words of Jim Harper, director of information policy studies at the Cato Institute, the webmaster of WashingtonWatch.com*,* "If consumers have privacy worries, they can simply decline to use social networks like Facebook, and many do".[15]

But is that really so? First of all, there is a generalized lack of knowledge on the part of users concerning Facebook's privacy policy and their exposure to potential web-related risks. Perhaps only lawyers know that under Facebook's "Terms of Service" (a disclaimer that is the online equivalent of "fine print" in contracts of adhesion), users give up copyright control of any material posted. As a result, laypersons at best remain partially protected. Secondly, Facebook owns the right to maintain users' information in its database, even after those users' profiles have been deleted. Users do not have the right to be forgotten! The European Union is actively defending users' "right to disappear" (Walsh 2011), what the French call *le droit à l'oubli* – literally, the right to oblivion. New European Union rules planned for later this year will put the EU on the leading edge of privacy laws. The moves could have a profound effect on companies like Facebook. The European Commission is under negotiations with Facebook in order for European users to have the right "to be forgotten" when they do not need their data any more or when they want to delete them and to be clearly informed regarding who will collect and use their personal data and for how long (Vivian Reding 2010, EU Commissioner of Justice).

In theory, many different policy interventions have been proposed when it comes to the law and policy of privacy on social network sites. James Grimmelmann's argument that we think about privacy as product safety seems to be quite convincing. There is an inevitable tension between privacy on the one hand and security on the other. The ensuing result is often increased surveillance, as after September 11, security concerns predominate in western societies. For example, the UK, once a bastion of freedom and civil liberties is now one of the most advanced surveillance societies in the world, ranked third after Russia and China. The average UK adult is now registered on more than 700 databases and is caught many times each day by nearly five million CCTV cameras (Flintoff 2010). Increasingly monitored, citizens are being turned into suspects.

On "The Early Show on Saturday Morning", Joan Goodchild spotlighted five dangers she says Facebook users expose themselves to,[16] probably without being aware of it:

- Your information is being shared with third parties
- Privacy settings revert to a less safe default mode after each redesign
- Facebook ads may contain malware[17]
- Your real friends unknowingly make you vulnerable

---

[15] http://roomfordebate.blogs.nytimes.com/2010/05/25/should-government-take-on-facebook/

[16] http://www.cbsnews.com/stories/2010/05/08/earlyshow/saturday/main6469373.shtml

[17] *Malware*, short for malicious software, is software designed to harm or secretly access a computer system without the owner's informed consent.

- Scammers are creating fake profiles

In April of 2011, security firm Sophos published an open letter to Facebook about its security and privacy measures on the popular social networking site, and the message is clear: It's time for some changes in order to better protect users (Goodchild 2011). In addition to privacy issues, Facebook users run an online risk of denigration. The negative representation of reputation online, which can be related to *distortion*-- being inaccurately characterized--and *appropriation*-- the use of one's identity or personality for the purposes and goals of another. Examples include incorrect tagging of photos, creating a phony profile of someone (with denigrating information), or posting negative information (like pornography, racial slurs, etc.) on someone's profile page (see Solove 2006).

4. The Protection of Minors

An issue of primary concern for Facebook regulators is the protection of minors from sexual predators, from pornographic sites, from pedophiles and cyber-bullying. The site was originally restricted to college and high-school students, but since it opened membership to the general public, Facebook has run into such issues more often. The site's operators have increasingly dealt with problems that plagued MySpace, another networking site that raised parental concerns about inappropriate sexual contact between adults and teenagers.

4.1. Facebook and sexual predators
At least three convicted sex offenders in the US had pages on Facebook. Facebook's chief privacy officer says the site takes down such profiles and pages within 72 hours of a complaint, and will do so in these instances. In the summer of 2007, the Connecticut state attorney general had said that his office is investigating at least three of these cases and had found inappropriate images as well (Fischman 2007). Many sexual predators have already faced charges for online solicitation of sex with young girls. According to reports that surfaced in 2009, MySpace revealed that 90,000 registered sex offenders had been kicked off its site in the past two years. But where did all of those sex offenders go? Some evidence suggests that a portion of them are now on Facebook (Schonfeld 2009).

In September of 2007, New York attorney general Andrew Cuomo subpoenaed Facebook because of what he says is the site's lack of controls to protect the safety of its users, despite Facebook's claims that it makes about the safety measures it has in place on the site. In recent weeks, investigators from the attorney general's office went undercover to conduct tests on Facebook's safety controls and procedures, according to a statement. Pretending to be underage users, the investigators were solicited by adult sexual predators on Facebook. In addition, investigators were able to access pornographic images and videos.

"Disturbingly, Facebook often did not respond, and at other times was slow to respond, to complaints lodged by the investigators - posing as parents of underage users - asking the site to take action against predators who had harassed their children", the statement said (Rosencrance 2007). Perhaps most alarmingly, Facebook ignored several (and repeated) complaints from undercover investigators concerning persons who made inappropriate sexual advances to underage users (*id.*).

Lecturer Aspasia Tsaoussi   4th International Conference on International
Law
                                    Thessaloniki (20th and 21st May 2011)

4.2. Facebook and pornography

Child pornography and child sex trafficking don't just pop up occasionally on Facebook; criminals regularly use the site to systematically exploit children. Netizens Watch, an independent, multi-national online watchdog organization (which must maintain anonymity for their own protection) has discovered thousands of new false profiles featuring child pornography and code words used to connect with other pedophiles (Kloer 2011). In one day-long sweep alone, a Netizens Watch member found over 1,400 images of child pornography, from toddlers up to 14-year-olds. These images primarily manifest in closed groups created by pedophiles to share photos and videos of abused children and through profiles created by their pimps or abusers. Often, specific sex acts can be "ordered" on Facebook, and can include extreme violence and heinous brutality.

Facebook's policy is against pornography of any kind and requests members to report sites that contain it. Currently Facebook is full of pornography. However, there is a link at the bottom of Playboy, Hustler and The Bunny Ranch that says "Report Page". Once again, it is in the hands of the users to act.

However, despite frequent user reports of child sexual abuse being facilitated through Facebook, the company has failed to create a strategy to address this growing crime. Activists have launched the "Stop Child Porn on Facebook Campaign",[18] which serves as a call to action to both Facebook and its users to make fighting child exploitation a priority.

4.3. Facebook harassment: A new type of peer pressure

Researchers have shown interest in how narcissism is manifested on social networking Web sites. Social psychologists have identified three personality traits (extraversion, emotional intelligence and Machiavellianism) and two main personality types among Facebook users: "narcissistic" and "shy". Recent research conducted by Buffardi and Campbell (2008) collected narcissistic personality self-reports from Facebook page owners. The findings revealed that narcissism predicted (a) higher levels of social activity in the online community and (b) more self-promoting content in several aspects of the social networking Web pages.[19] Furthermore, strangers who viewed the Web pages judged more narcissistic Web page owners to be more narcissistic.

Facebook enhances narcissistic tendencies in young adolescents, who are more vulnerable to pressures resulting from the image they project to their peers. Facebook enables and enhances arbitrary divisions along the lines of outward appearance ("she's the best looking girl in class— her recently posted photo got 55 likes!!") or popularity ("he's the most popular boy—he has 700 friends!!!"). Young teens are separated into "in groups" and "out groups". The in-groups include all the good-looking, popular "cool" kids and the out-groups all the kids that don't fit this description. Stereotypes are solidified and the right to be different, look different, do things that are different from the rest, does not exist in this virtual world. Facebook fuels these divisions

---

[18] http://www.stopchildpornonfacebook.com./
[19] In 2010, Mehdizadeh collected self-esteem and narcissistic personality self-reports from 100 Facebook users at York University. Participant Web pages were also coded based on self-promotional content features. Correlation analyses revealed that individuals higher in narcissism and lower in self-esteem were related to greater online activity as well as some self-promotional content (Mehdizadeh 2010).

online and amplifies their meaning offline. The result is the rise in the number of teens who may suffer angst and clinical depression (Facebook outcasts).

There are also documented cases of teenagers who have committed suicide as the result of cyber-bullying.[20] Users in their mid- or late-teens may use Facebook to exchange disrespectful, cruel and hurtful messages. Although there is no easy and automatic way for Facebook and other social networking sites to become "safer" social venues for young people to socialize online, steps can be taken to increase surveillance.

In August of 2010, the Libertarian Party (LP) protested the decision by Facebook to refuse advertisements that advocate for the legalization of marijuana. The LP had been running a highly successful Facebook ad to express its support of marijuana legalization, but Facebook banned the ad about a week after accepting it. Wes Benedict, Executive Director of the LP, commented, "Whether or not the folks at Facebook like marijuana, we think they should end their ridiculous censorship of our ad, which expresses the Libertarian position on a political issue of interest to many people."[21] Benedict continued, "We recognize Facebook's right to control their content and censor whoever they want. But we're also exercising our First Amendment right to complain about their bad decision, and to alert other consumers to put pressure on them."

5. The Regulation of an Unregulated Medium

The issue of Facebook's regulation has raised concerns on both sides of the Atlantic. The United States prefers what it calls a "sectoral" approach to data protection legislation, which relies on a combination of legislation, regulation, and self-regulation, rather than governmental regulation alone. Privacy legislation in the United States tends to be adopted on an *ad hoc* basis, with legislation arising when certain sectors and circumstances require.[22] To date, the US has no single data protection law comparable to the EU's Data Protection Directive. Self-regulation has demonstrated its weaknesses: Industry self-regulation of privacy is a negotiation about "the rules of play" for the use of personal data. In deciding on these rules, industry is likely to be most interested in protecting its stream of revenues (Schwartz 1999). Therefore, it will benefit if it develops norms that preserve the current status quo of maximum information disclosure.

We will first look into US-based responses and then examine European Union legislation. In 2010, fifteen privacy groups in the US filed a complaint with the Federal Trade Commission seeking an investigation over possible deceptive trade practices. An increasing number of users are now calling for regulation. In the US, Senator Charles Schumer (D- N.Y.) says he wants the network to make it easier for users to understand how their personal information is being used. He has urged the Federal Trade Commission to provide guidelines for social networking sites, like Facebook, Myspace, and Twitter on how private information submitted by online users can be used and disseminated. Schumer has stated that if that doesn't work, he is prepared to craft legislation to achieve the same end.

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy

---

[20] http://www.ktla.com/news/landing/ktla-facebook-suicide-bullies,0,133841.story

[21] http://www.lp.org/news/press-releases/libertarian-party-protests-facebook-censorship-of-its-marijuana-legalization-ad

[22] For example, the Video Privacy Protection Act of 1988, the Cable Television Protection and Competition Act of 1992, the Fair Credit Reporting Act, and the 2010 Massachusetts Data Privacy Regulations.

and Trans-Border Flows of Personal Data." The seven principles governing the OECD's recommendations for protection of personal data were:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability—data subjects should have a method available to them to hold data collector

The OECD Guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. It should be noted that the United States, while endorsing the OECD's recommendations, did nothing to implement them within the United States. However, all seven principles were incorporated into the EU Data Protection Directive.

5.1. The EU Data Protection Directive[23]

The EU Data Protection Directive specifies that user consent must be "freely given, specific and informed" (Article 2(h) of Directive 95/46/EC). Article 24 of the Data Protection Directive requires Member States to establish appropriate sanctions in case of infringements. According to Article 28, independent authorities must be charged with supervising implementation.

Commissioner Reding has asserted:

> *"European privacy rules are crystal clear: a person's information can only be used with their prior consent. We cannot give up this basic principle, and have all our exchanges monitored, surveyed and stored in exchange for a promise of 'more relevant' advertising! I will not shy away from taking action where an EU country falls short of this duty."*[24]

No matter how we label it, a social network, a social utility or a social phenomenon, Facebook is operating on an international scale. Therefore, it is obvious that any public dialogue concerning its regulation also needs to be developed on an international level. This will no longer be a local population of users conversing with the founders over a blog:[25]

> *When Facebook introduced the News Feed and received a backlash from its users, Zuckerberg's first blog post was to tell everyone to calm down. When they didn't, new features were introduced to help them navigate the system. Facebook was willing to talk to its users, to negotiate with them, to make a deal. Perhaps this was because they were all American college students, a population that early Facebook understood.*

---

[23] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[24] http://dataprivacy.foxrothschild.com/tags/facebook/
[25] http://www.futurelab.net/blogs/marketing-strategy-innovation/2010/05/facebook_utility_utilities_get.html

5.2. The EU Directive on privacy and electronic communications

Directive 2002/58 on Privacy and Electronic Communications, otherwise known as the *E-Privacy Directive*, is an EU directive on data protection and privacy in the digital age. The EU Directive on privacy and electronic communications requires EU Member States to ensure confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented (Article 5(1) of Directive 2002/58/EC). It represents a continuation of earlier efforts, most directly the aforementioned *EU Data Protection Directive*. The Directive complements the EU Data Protection Directive and applies to all matters which are not specifically covered by the latter. More specifically, it deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies (see also Edwards 2005). This Directive has been amended by Directive 2009/136, which introduces several changes, especially in what concerns cookies, that are now subject to prior consent.

Under article 5(3) of the Directive, the Member States must ensure that the use of electronic communications networks to store information is only allowed if the user is provided with "clear and comprehensive information", in accordance with the Data Protection Directive, about why the information is being processed and is offered the right to opt out. The regime so set-up can be described as "opt-out with an added information request". This effectively means that the consumer must be given the opportunity to opt out of receiving cookies. The Directive does not give any guidelines as to what may constitute an opt-out.

Viviane Reding (EU Commissioner for Information Society and Media) has indicated that social networking sites, like Facebook, MySpace and Friendster, must safeguard and reinforce privacy protection online:

> *Privacy must in my view be a high priority for social networking providers and their users. I firmly believe that at least the profiles of minors must be private by default and unavailable to internet search engines. The European Commission has already called on social networking sites to deal with minors' profiles carefully, by means of self-regulation. I am ready to follow this up with new rules if I have to.*

Picking up on the Commissioner's statement, it seems evident that new rules are urgently needed. Self-regulation is insufficient. The protection of minors is endangered on a daily basis. Parents seriously and systematically underestimate the risks connected with their children's online profiles. Minors in their early teens are daily providing false data to Facebook about their birth year in order to get an account. Some parents know about it, but these are usually the parents who are also Facebook users and will be able to monitor their child's activity more successfully. But most parents do not know. They are not bad or unfit parents who are incapable of taking care of their children. But they are *uninformed* or at best *poorly informed* about the dangers.

With Facebook use spreading like wild-fire across Europe, we argue that policymakers and legislators should take four measures without delay:
   (a) raise the current minimum age of users from the current 13 (thirteen) to 15 (fifteen) years of age and
   (b) make parental consent a *sine qua non* condition for opening an account.
   (c) pressure Facebook to set up an office for the "Protection of Minors"

(d) incite Facebook to employ a dedicated team to scan the photos posted and shared by minors (human scanning should be used in combination with the existing flagging system)

Age restriction may seem like a paternalistic measure; however, the protection of minors is weighed as a global public good of the highest order. Besides, some SNSs are already restricted by age.[26] As for parental consent, it is our contention that both parents (regardless of marital statues) should agree and consent that their child opens an account. Both parents should provide consent in writing, by completing online application forms where they provide full contact details, including place of employment, telephone numbers, current street address, etc. They should then complete a consent form that is sent to Facebook central headquarters, reviewed by Facebook that contacts the parents online and then authorizes.

Facebook should set up an office for the "Protection of Minors". This could be a virtual office (something like a control center), that receives emails and online reports/ complaints about the suspected or actual abuse and harassment of minors. Increased transparency and accountability should guide any regulatory action or initiative. It should also incur the additional cost of having a pair of human eyes looking at every photo uploaded to the site and shared by minors, like MySpace does. Facebook currently relies on users to flag any content they find inappropriate. A more effective system would be for Facebook to employ a dedicated team to scan through photos, or even better, a combination of flagging and human scanning (Kincaid 2009).

Of course, when it comes to adults, self-restraint and common sense should dictate what is publicized on one's profile. We are after all the only vanguards of our own privacy. The ancient Greeks asserted that what belongs in the domestic sphere should not be made public (*«τα εν οίκω μη εν δήμω»*). User responsibility is likely to be a pivotal axis in every future regulative effort concerning Facebook and other social network sites. However, future users will be just as likely to use Facebook's "near obscurity" in order to communicate with their friends, sharing personal trivia, chatting and crossing many fine lines in their attempt to bridge the social distance. There is a tendency to over share and to be less cautious when caught in the contagious enthusiasm of belonging in a global community that is all about friendship. There is also an element of curiosity about what other friends have been up to: Facebook allows you to steal glances into your friends' lives. One of the reasons underlying Facebook's tremendous popularity is what we call its hidden function: the fact that it legitimizes gossip.

Lastly, it is interesting to see that Facebook itself is adjusting to users' demands and complaints. One example is how difficult it used to be three years ago to deactivate your account. Until February 2008, it was nearly impossible to delete one's Facebook account; the data associated with it would remain on Facebook's servers even after a user "deactivated" the account (Aspan 2008a). A year earlier, Facebook had informed a blogger that in order to close his account, he would need to delete each contact, Wall post, and so on by hand—all 2500 of them (Mansour 2007). Consequently, Facebook added a "delete" option (Aspan 2008b), although it was plagued by bugs at first: some "deleted" profiles were still visible, including contact lists and applications.

---

[26] See Wikipedia (April 2011). List of notable social networking websites, http://en.wikipedia.org/wiki/List_of_social_networking_websites

To quote Grimmelman, "deliberately staying off of Facebook has an unambiguous social meaning, and Facebook should respect the request" (Grimmelman 2009: 1200). This is why he proposes what he calls "a reliable opt-out rule". Facebook should proactively offer this sort of an opt-out to any non-user as soon as it acquires enough information about them to be able to contact them (e.g., an email address or IM screen name); it should also purge from its servers any other information linked with the email address whose owner has opted out.

6. Conclusion

In the past few years we have all witnessed an increasing socialization of the web. Facebook is a social medium with an unprecedented degree of "open access"— this fact alone calls into question many of our heretofore *traditional* understandings of information. The cultural, psychological and political dimensions that are conventionally linked with information laws are challenged in their foundations. The lack of monitoring mechanisms continuously poses new dilemmas and opens the gate to new problems. The boundaries between the public and the private sphere have been effaced. At the same time, many feel that what's at stake with Facebook today has little to do with privacy or publicity, and a lot to do with informed consent and choice.[27] Facebook speaks of itself as a utility while also telling people they have a choice.

If we take the optimistic view, then we will see Facebook use as an attempt on the part of users to recapture a long-lost sense of belonging to a community, a global community with indefinite and undefined boundaries but with more personal elements. This is an asynchronous and uncoordinated attempt, and perhaps a largely unconscious one, on the part of users to try and reclaim a sense of *Gemeinschaft*, a spontaneously arising organic social relationship, as identified by German sociologist Ferdinand Tönnies in 1887.[28] In its expanded understanding, *Gemeinschaft* is possible in globally dispersed communities; thus, we could see Facebook as a patchwork of local and virtual communities.[29]

If we adopt a pessimist's view, we will have to conclude that Facebook is a social networking website with the potential to ruin people's lives. In an earlier article, Paul Schwartz had argued that the widespread, silent collection of personal information in cyberspace degrades the health of a deliberative democracy, cloaking in dark uncertainty the transmutation of Internet activity into personal information that will follow one into other areas and discourage civic participation (Schwartz 1999). He predicted that this situation will also have a negative impact on individual self-determination by deterring individuals from engaging in the necessary thinking out loud and deliberation with others upon which choice-making depends. As noted by Bruce Mann, "the situation is serious – serious because the user-generated content (UGC) that is

---

[27] http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html

[28] "Gemeinschaft" (often translated as *community*) is an association in which individuals are oriented to the large association as much if not more than to their own self interest. Furthermore, individuals in Gemeinschaft are regulated by common mores, or beliefs about the appropriate behavior and responsibility of members of the association, to each other and to the association at large; associations marked by "unity of will" (Tönnies, 22).

[29] In his recent book, *The Church of Facebook: How the Hyperconnected Are Redefining Community*, Jesse Rice (2009) propounds the idea that the Wi-Fi, worldwide movement that is currently under way is changing how we interact with others. It represents what he sees as "a seismic shift that is redefining the idea of community". The author adopts a theological perspective, positing that this phenomenon subtly reflects a God who longs to connect to us.

displayed on-screen is destroying users' lives; serious too, because of the volume of users at risk from posting their content, without intervention by the SNI" (Mann 2008: 1).

We take the middle ground and believe that Facebook is neither a curse nor a boon. We adopt a pragmatic view rooted in the classic sociological tradition that our need to connect with other people is deeply and inherently social in nature. Facebook is a modern manifestation of the age-old longing for intimacy, friendship and connection that was described by Aristotle as the attribute of humans as social animals. It is indubitable that a lot is at stake: technology runs faster than the legal rules and social norms that shape our democratic self-governance. Legislation must be enacted to protect the rights of minors who will choose to use Facebook. In the context of the proper regulatory framework, Facebook users will be able to achieve a plurality of purposes and transform Facebook into a safe, lively global forum for the exchange of ideas and the formation of networks. Individual users will be able to pursue personal goals (such as self-determination and self-actualization), social goals (such as political collaboration) or both.

We should not forget that privacy protection law is closely interconnected with human rights law. We as social actors are the creators of norms that will allow us to co-exist harmoniously, each one of us endowed with fundamental and inalienable human rights. The legal rules we will enact are but the formal expression of these norms, which often arise spontaneously, out of a collective awareness that a better system is possible. More effective legal rules can enable a more prudent use of technology, providing a safe virtual environment to all users in present and future generations. Our defense of democracy and its gifts must be vigorous and unequivocal. Freedom of speech and freedom of expression are the hallmarks of healthy democracies. At the same time, they are the guarantors that open societies, in the Popperian sense, will be possible in the future.

BIBLIOGRAPHY

Aspan, Maria (2008a), "How Sticky Is Membership on Facebook? Just Try Breaking Free", *New York Times*, Feb. 11, 2008, at C1.

Aspan, Maria (2008b), "Quitting Facebook Gets Easier", *New York Times*, Feb. 13, 2008, at C1.

Barabási, Albert-László (2003), *Linked: How Everything Is Connected to Everything Else and What It Means*. Plume.

Boyd, Danah M. and Nicole B. Ellison (2007), "Social Network Sites: Definition, History, and Scholarship", http://mimosa.pntic.mec.es/mvera1/textos/redessociales.pdf

Buffardi, Laura E. and Keith W. Campbell (2008), "Narcissism and Social Networking Web Sites", *Personality and Social Psychology Bulletin* 34: 1303-1314.

Carlson, Nicholas (2011), "Facebook 2010 profit? Try $600 million", *Business Insider*, 2/10/2011, http://www.msnbc.msn.com/id/41521349/ns/business-us_business/

Cassidy, John (2006), "Me media." *The New Yorker*, 50-59 (May 15). http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy

Christakis, Nicholas A. and James H. Fowler (2011), *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives -- How Your Friends' Friends' Friends Affect Everything You Feel, Think, and Do*. Reprint edition. Back Bay Books.

Edwards, Lilian (2005), "Articles 6-7, ECD; Privacy and Electronics Communications Directive 2002 (Canning the Spam and Cutting the Cookies: Consumer Privacy On-line and EU Regulation", in Lilian Edwards (ed.), *The New Legal Framework for E-Commerce in Europe*, pp. 31-66. Hart.

Ellison, Nicole B., Charles Steinfield and Cliff Lampe (2007), "The Benefits of Facebook 'Friends': Social Capital and College Students' Use of Online Social Network Sites", *Journal of Computer-Mediated Communication* 12(4): 1143-1168.

Fischman, Josh (2007), "Sexual Predators on Facebook", *The Chronicle of Higher Education*, July 30, 2007, http://chronicle.com/blogs/wiredcampus/sexual-predators-on-facebook/3216

Flintoff, Jean Paul (2010), "Can you disappear in surveillance Britain?", *The Sunday Times*, April 17, 2010,
http://women.timesonline.co.uk/tol/life_and_style/women/the_way_we_live/article7096105.ece

Goodchild, Joan (2011), "Security Firm to Facebook: Clean Up Your Act", April 18, 2011, http://www.cio.com/article/679823/Security_Firm_to_Facebook_Clean_Up_Your_Act?source=rss_security

Granovetter, Mark S. (1973), "The Strength of Weak Ties", *American Journal of Sociology* 78 (6): 1360-1380.

Grimmelman, James (2009), "Saving Facebook", *Iowa Law Review* 94: 1137-1206.

Kincaid, Jason (2009), "Wake Up Call: Facebook Isn't a Safe Haven", http://techcrunch.com/2009/02/08/wake-up-call-facebook-isnt-a-safe-haven/

Kirkpatrick, David (2010), *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. Simon and Schuster.

Kloer, Amanda (2011), "Online Activists Fight Child Pornography on Facebook", March 16, 2011, http://news.change.org/stories/online-activists-fight-child-pornography-on-facebook

Mann, Bruce L. (2008), "Social Networking Websites – A Concatenation of Impersonation, Denigration, Sexual Aggressive Solicitation, Cyber-Bullying or Happy Slapping Videos", *International Journal of Law and Information Technology* 17(3): 252-267.

Steven Mansour (2007), "2504 Steps to Closing Your Facebook Account", http://www.stevenmansour.com/writings/2007/jul/23/2342/2504_steps_to_closing_your_facebook_account

Mehdizadeh, Soraya (2010), "Self-presentation 2.0: Narcissism and Self-esteem on Facebook." *Cyberpsychology, Behavior and Social Networking* 13(4): 357-364.

Putnam, Robert D. (2000), *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

Rice, Jesse (2009), *The Church of Facebook: How the Hyperconnected Are Redefining Community*. David C. Cook.

Rosen, Christine (2007), "Virtual Friendship and the New Narcissism", *The New Atlantis*, 17: 15-31.

Rosencrance, Linda (2007), "Facebook failing to combat sexual predators: New York subpoenas Facebook over user safety", *Computerworld US*, September 25, 2007, http://www.pcadvisor.co.uk/news/default/10827/facebook-failing-to-combat-sexual-predators/

Schonfeld, Eric (2009), "Thousands of MySpace Sex Offender Refugees Found on Facebook", http://techcrunch.com/2009/02/03/thousands-of-myspace-sex-offender-refugees-found-on-facebook/

Schwartz, Paul M. (1999), "Privacy and Democracy in Cyberspace", *Vanderbilt Law Review* 52: 1609-1701.

Scoble, Robert (2010), "Why it is too late to regulate Facebook", http://scobleizer.com/2010/04/30/why-it-is-too-late-to-regulate-facebook/ (accessed on April 18, 2011)

Shih, Clara (2009), *The Facebook Era: Tapping Online Social Networks to Build Better Products, Reach New Audiences, and Sell More Stuff* (Shih 2009)

Shoenberger, Heather (2009), "Defriending: A laughing matter?", *National Examiner*, September 22, 2009, http://www.examiner.com/social-media-in-national/defriending-a-laughing-matter

Solove, Daniel (2006), "A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154(3): 477-560.

Tönnies, Ferdinand (ed. Jose Harris), (2001), *Community and Civil Society*, Cambridge University Press.

Walsh, Jason (2011), "When it comes to Facebook, EU defends the 'right to disappear'", *The Christian Science Monitor*, April 6, 2011, http://www.csmonitor.com/World/Europe/2011/0406/When-it-comes-to-Facebook-EU-defends-the-right-to-disappear

Watts, Duncan J. (2004), *Six Degrees: The Science of a Connected Age*. W.W. Norton & Company.