Curating the Social Graph, or What Your Friends Say About You

Brook Ellingwood

Mary Janisch

Ian Porter

Kenneth Rufo

Inge Scheve

Daniel Thornton

John Yeager

Brook Ellingwood, Mary Janisch, Ian Porter, Kenneth Rufo, Inge Scheve, Daniel Thornton, & John Yeager, "Curating the Social Graph: or What Your Friends Say About You," The Four Peaks Review 2.1 (2012) 68-86,.

INTRODUCTION

The concept of "curating" comes from the Middle Latin term *curatus*, which refers to the responsibility of caring for souls. The curator was a priest, a spiritual guide, a shepherd. The term entered common use in the 16th century to describe the duty Christian priests had to their congregation. Over time, the "curing" of souls gave way to the care-taking of things, and to curate came to signify the assembly, display, and preservation of artifacts, typically in a museum or as part of a personal collection. Today, the term has taken on new meaning in the age of digital media, when one's persona now enjoys a digital projection, a blending of the soul and of things. Now what is curated are one's social connections, those set of relations that have always been managed, but not always under our control.

Friendships and acquaintances have traditionally been the product of no small amount of coincidence. Wrought from accidents of geography and class cohort, from the necessities of the labor market and the whims of employers, from the shared enjoyment of certain leisure activities and the serendipity of a chance encounter, friendships were managed with only marginal amounts of agency, or put differently, we chose our friends, but our choices were not always purely ours to make.

The transition to and explosion of relations made possible by social media platforms like Twitter and Facebook alter that equation in any number of significant ways. Our ability to grow our friends and acquaintances now comes with unsurpassed and unparalleled ease. Our ability to subtract or "unfriend" those contacts is just as easy, though certain social media norms and some very minor procedural steps often mitigate our desire to do so. But perhaps more profoundly, the ability to map the web of relationships that comprise our social networks is now actionable in a manner never known before. This ability, unlike the abilities of adding and subtracting friends, is not, strictly speaking, *ours*. Because of the socio-public nature of the platforms through which contacts are acquired, third parties have a similar ability to map our personal network of social relations. These maps, these social graphs, hold significant consequences for human interactions, our sense of self, and our practical ability to present ourselves to others.

As such, we must ask today what it means to curate our social graphs. And we must determine the

extent and locus of responsibility for their curation and publication.

This white paper explores the current state of data, both personal and social, in the context of the social graph. We will begin, as we must, with the question of privacy, but we wish to underscore that while privacy provides a necessary starting point to this discussion, privacy typically delimits a particular question about how much data about yourself is known to others. Our concern here is both related and distinct, in that we are concerned with the wealth of data being collected about semi-public interactions between social agents, even if those agents are themselves tightly curtailing who has access to their personal, "private" data.

THE STATE OF PRIVACY IN THE AGE OF SOCIAL MEDIA

Social networking is one of the most popular activities online. Forty-seven percent of adults who go online used social networking sites in 2010, up from 37 percent in 2008 (Lenhart et al, 2010). Facebook, with more than 500 million active users, was by far the most popular social networking site, followed by Windows Live Profile, Twitter, and Myspace (Efrati, 2010). (Because of its reach, Facebook will be the focus of much of this section.)

Many social networking sites allow users to decide who can view their profile --and what parts of it-- through privacy settings, though a certain minimum of information is always publicly available. On Facebook, for instance, at a minimum a user's name, profile picture, gender, username, and networks are visible to anyone on the Internet (Facebook, 2011). On Myspace, the basic displayed information is profile picture, numerical friend ID, stated location, gender and age, and display name (Myspace, 2011).

Nearly half of Facebook's users log into the site every day (Facebook, 2011a), doing things like posting status updates, uploading and sharing photos, becoming a fan of products, and commenting on their friends' posts. When a user registers for Facebook, Facebook recommends making much of their data – including posts and likes and lists of friends--public, though users can override these recommendations. In recent years, social networking data has become a virtual goldmine to a host of different companies. Marketers and advertisers use the data to target their products. Data brokers use social networking data along with other information aggregated about a person on the Web to build and sell profiles of Internet users. Hiring managers have used social networking sites to screen job candidates, and college admission officers have done the same for prospective students. Recently, companies also began exploring how to use a user's social graph—the friends in his or her network—to help make predictions about things like his or her creditworthiness (more on this below).

FACEBOOK'S DEFAULT PRIVACY SETTINGS: EVOLVING FROM PRIVATE TO PUBLIC

Initially, when Facebook was launched in 2004, a user's personal information could only be viewed by someone if that person belonged to a group specified by the user in the privacy settings. Over time, Facebook revised its privacy policies bit by bit to make a user's data more public by default (Opsahl, 2010). When Facebook became a development platform on which companies could create games and other applications, users who chose to use those apps gave companies access to their data, as well as their friend's data. In December of 2009, Facebook prompted its users to review new privacy settings, which by default were set to make most information public. Facebook reported that about 35 percent of its users who had never edited their settings did so at this time, though it was unclear whether some users accepted the defaults without knowing what they entailed (boyd & Hargittai, 2010).

In an interview in January 2010, Mark Zuckerberg, Facebook's CEO, said the company's latest privacy defaults reflected changes in social norms around the sharing of information, brought about my blogging and other social media:

Doing a privacy change for 350 million users is…not the type of thing that a lot of companies would do…We view that as a really important thing… to always keep a beginner's mind and think, "What would we do if we were starting…the site now?" We decided these would be the social norms now, and we just went for it. (zennie62, 2010)

To manage their privacy settings on Facebook, users must click through multiple options over several pages. In addition to the main Privacy Settings page, which controls what a user shares on Facebook, there is a page for managing how people can contact a user on Facebook (what Facebook calls "connecting"), one for managing privacy settings for third-party apps and websites (including whether a user appears in public search listings), and another that manages whether a user appears in social ads on friends' pages.

In 2011, these were Facebook's default recommended privacy settings for sharing and connecting. If a user takes no action on their privacy settings after signing up, this is what will be shared and with whom. (At a minimum, a user's basic information--name, profile picture, gender, and networks --is always available and cannot be hidden through privacy settings.)

Everyone	**Friends of Friends**	**Friends**
Name, gender, and profile pic	>	>
Status and posts	>	>
Photos and videos	>	>
Networks	>	>
Bio and favorite quotations	>	>
Family and relationships	>	>
Current city and hometown	>	>
Likes and activities	>	>
Education and work	>	>
Search for you on Facebook	>	>
Send you friend requests	>	>
Send you messages	>	>
See your friends list	>	>

	Photos/videos you're tagged in	>
	Religious and political views	>
	Birthday	>
		Comment on posts
		See places you check into
		Contact info

Facebook has historically faced a storm of criticism that its privacy policies are needlessly long, complicated, confusing, hard to find, full of legalese, and generally difficult for the average person to follow (Bilton, 2010). In March 2011 Facebook announced that it was at work on a simpler privacy policy (Richmond, 2011), one that would be clearer about the scope of users' actual privacy protection. The subsequent profile redesign, Timeline, opened up new complications regarding user privacy and their history of activity on the network (Burnham, 2011).

DATA SHARED THROUGH THIRD-PARTY APPS AND GAMES

Facebook is a platform for tens of thousands of apps, including such popular games as Farmville (Steel & Fowler, 2010). These apps and games are huge moneymakers for Facebook, promising to bring in somewhere between $1.3 and $2.5 billion of revenue a year (Diana, 2011). When a user chooses to use an app, he or she gives consent for the app developer to access basic information from his or her profile, as well as his or her friends list and whatever else he or she has made publicly available (Facebook, 2010b).

The apps on Facebook are designed to be social, and Facebook gives apps access to a user's friends list so that a user can invite other friends to play, too. In this way, a person's friend list is a back door by which third-party apps can have access to a whole range of data. Users can restrict what kind of information is available through friends, or block platform apps altogether, but they must go into their privacy settings to do this.

In 2010, *The Wall Street Journal* published a story on how some developers of popular Facebook apps were selling Facebook user ids – which can be used to access public user profiles -- to data brokers. Facebook said this behavior violated its terms of service, declared "zero tolerance" for data brokers, and took steps to correct the situation (Vernal, 2010). But Facebook also states, in its privacy policy, that it cannot guarantee that third-party developers will follow its rules. The incident highlighted the challenges facing Facebook when it comes to supervising what application developers do with user data.

DATA OBTAINED THROUGH DATA SCRAPING

Facebook requires written permission from data brokers wanting to "scrape" or collect information its users have made publicly available by editing (or perhaps failing to edit) their privacy settings. But data miners have gotten around that, operating from the mentality that if it's on the Web, it's up for grabs. Using automated software, or bots, brokers scrape up public social networking data and aggregate it with other information found about users on the Web, including email addresses, aliases used in blogging, and posts in password-protected online forums (Angwin & Steckler, 2010). The brokers build and sell user profiles for everything from advertising to background checks. Some, like Rapleaf, have been banned by Facebook, while others continue to fly under the radar (Goldman, 2010). In 2010 Ron Bowes, a security consultant, created a torrent of 100 million public Facebook profiles of users who hadn't edited the privacy settings that allow them to show up in public search listings (Tsotsis, 2010). While not a "scraper," Bowes was trying to show how much personally identifiable information is out there for anyone to grab.

THE "SOCIAL GRAPH" AND A COLLECTIVE ABDICATION OF PRIVACY

The phenomenon of online socializing is not new. Epistolary forms of social communication have existed online since the advent of email in the 1970s. More sophisticated forms of online socializing have exploded recently with the growth of so-called "Web 2.0" utilities like Facebook and MySpace. These sites have garnered millions of users into approximations of social sharing that are troubling to privacy advocates. Despite these

concerns, individuals often post sensitive personal information on their profiles that can be found by entities outside of their chosen social networks (Rambam, 2008). Legal scholar Daniel Solove has pointed out that the unintentional release of personal information can lead to unwanted scrutiny that can quickly spiral out of reach of the person posting the information. Solove also points out that once information escapes the control of the user, that information is nearly impossible to delete. This becomes an indelible part of the user's digital identity and can have catastrophic consequences for the user's personal and professional reputation (Solove, 2007).

The lack of anonymity is the biggest challenge to privacy in the social graph. Facebook, Twitter and LinkedIn require personally identifiable registrations. A person could elect to create a pseudonym for their Facebook or Twitter profile, but the actual anonymity afforded by such a strategy are limited. Curating your friends or followers makes it fairly easy to establish your actual identity.

There are two types of anonymity that are lost in social media--technical anonymity and social anonymity. Technical anonymity allows someone to control personally identifiable information like phone numbers, social security numbers, addresses etc...and separate that information from behavior. Social anonymity is when an individual perceives themselves to be anonymous even when they are engaged in socializing (Christopherson, 2007). Social media encourages us to be as identifiable as possible. We volunteer our technical anonymity based in the promise that being more transparent online increases the value of the social transactions we engage in. LinkedIn would be pointless if we weren't identifiable in our networks. It just wouldn't work.

While we have some control of what we share and who we share with in social media, we can't guarantee that social sense of anonymity that allows us to act in innovative and socially unpredictable ways. We can choose who we share information with but we can't control who they might share information with.

While sites like Facebook attempt to control third party access to personal data by giving users some control over how their information is shared within the site, the lucrative business of application based utilities using the site as a registration platform de-incentivize broader privacy protections. When a site like Facebook allows a third party to collect and then aggregates personal data, the original protection offered by Facebook's terms of service no longer apply. In an effort to maximize the convenience offered by the third

party application, users often sign up for these services without fully researching the privacy terms of the new application. Facebook has no economic interest in warning the user of the third party's policy because the third party is a customer of Facebook (Thurm &Kane, 2010). Once a user's data is out of the Facebook box, it is potentially open to all possible privacy harms. Indeed, recent studies indicate that half of all Facebook applications can actually post in your name without your knowledge (Taylor, 2012).

HOW THE "SOCIAL GRAPH" IS BEING USED

Despite the serious privacy issues addressed above, the social graph is open for those data miners who wish to map it and those users who wish to clarify and enrich the map through new connections.

It is open in the sense that it is available for data miners to gather information across vast swaths of these social networks. The tools and techniques are available, says Murat Kantarcioglu, Assistant Professor of Computer Science at the University of Texas at Dallas. Drawing inferences about people not just based on their data within Facebook, for example, but across Facebook, Twitter, and LinkedIn and any number of other online social networks is already possible, he says. Although social network analysts continue to fine tune their tools and techniques - that is, the Web crawlers that gather the data and the algorithms that find meaningful relationships - they will remain qualitatively similar to previous techniques, says Kantarcioglu. "What is changing is the quantity of data... now, you have a lot more data," he says, contrasting current social network analysis with those efforts of the first social network analysts who, in the middle part of the 20th century, had to undertake ethnographic surveys to gather their analog data. Digital networks make data gathering easy, hence the amount of data gathered has jumped substantially.

Yet, with such a substantial jump in the magnitude of data collection, the work of social network analysis begins to shift towards qualitatively new ventures. For example, Kantarcioglu sees the future of network analysis in computing huge amounts of data in "real time" as the data is being produced, particularly location-based and time-stamped data. Using the data associated with mobile computing devices, which often carry location information produced by the device's global positioning system (GPS) and time stamps that correspond to the GPS data, Kantarcioglu sees the possibility of connecting these data

points to more traditional online social network data to infer conclusions about individuals with greater specificity and reliability.

Concomitant with the increase in computing power following Moore's law and the increased sophistication of data mining techniques, the production of huge quantities of data based on one's routine daily behaviors with a mobile computing device means that what can be known about an individual is truly astonishing. The image of that person, which is produced by drawing connections between these data, achieves higher orders of resolution that make the Orwellian panopticon in *1984* look quaint. Indeed, the panopticon can only see the now. The "eye" of social graph analysis can take the long view, drawing conclusions about an individual based on their behavior over time and across platforms (i.e., mobile computing behavior, online social network behavior, and search engine query behavior) and, thereby, enabling increasingly accurate models for predicting future behavior. That sounds pretty enticing to stakeholders who could use that information for power and profit. More on that in a minute.

If that picture seems grim, it presents only the first level of social graph analysis. The second level cares less about your data and more about the data produced by the people you associate with. As mentioned earlier, the ability to hide your data through privacy settings in social networks is tenuous at best. But, let's say for the sake of argument that Facebook's privacy settings actually worked. Perhaps that means that these data mining techniques won't affect those people who are diligent in managing their privacy settings. Think again.

A graduate student at the time, Behram Mistree worked with fellow Massachusetts Institute of Technology student Carter Jernigan back in 2007 on a project they called "Gaydar." Playing off the notion of "gaydar," that is, one's ability to intuitively know if someone else is gay, Mistree and Jernigan used social network analysis on Facebook accounts of students at MIT to determine if they could reliably predict if someone was gay or straight, even when that person hadn't explicitly revealed their sexual preference on their Facebook profile page.

How did they do this? Using what Mistree calls the "birds of a feather" analysis (that is, people with similar interests, socioeconomic backgrounds, cultural backgrounds, etc. will exhibit similar behaviors - it is alternatively called the "homophily principle" in network

analysis) they were able to determine a given person's sexuality based on their Facebook "friends." Even if the person in question had set his privacy settings high and had not revealed publicly information that would indicate his sexuality, Mistree and Jernigan were able to determine his sexuality by using a Web crawler to look at all of his friends' data. Because gay students were statistically more likely to have a higher ratio of gay friends, Mistree and Jernigan were able to use statistical analysis to make strong predictions about a student's sexuality based on his friends' data that did reveal sexual preferences.

What this means is that despite one's best efforts to make private their social graph data, data miners simply need to gather enough data about one's "friends," that is, one's social graph connections, to know more about a given person. While sexuality may seem like a relatively benign data point to draw a conclusion about, this type of data collection and inference drawing can be used for many other purposes as well, wrote Mistree in an email interview with the authors. When prompted to discuss the possibility of using these techniques to augment the process of determining a person's credit score, Mistree wrote:

"I would be many times more surprised if people were not already performing such analyses for credit scores (or credit score-like things) than if they weren't. I anticipate that another interesting-ish application on the horizon will be for health insurance. Especially with the upcoming healthcare law requiring insurers to take on people with pre-existing conditions, etc., it seems very likely that health insurers would like to focus their advertising on healthy individuals, and avoid advertising to unhealthy individuals. Talking to a couple of yahoo researchers, it appears that friends' dietary habits tend to overlap. Such information would be really useful for a health company trying to target healthy individuals.

Mistree makes clear that the implications for these types of analyses go way beyond predicting one's bedroom eyes. The social, political, legal and economic implications are much more profound, and the institutions that we've built around these spheres of society begin to crumble as their foundations shift beneath them. For example, Mistree highlights another area where this work could have an impact:

> "traditionally, when people think about web crawling it's within the context of pure commercial marketing. That ignores: 1) Foreign and domestic monitoring governments perform for "security". 2) Applications to politics: a political party's knowing which individuals to target with which message.

One need only look to the Middle East and northern Africa to see how these tools and techniques can be (and probably are being) used to wield state power and exert greater control over the populace.

POLITICS AND PROFILING

In July, 2009 shortly after the devastating defeat of Iranian protestors at the hands of their government, stories began to emerge about new immigration policies being practiced in Iran. It seemed the media hype, that had characterized these protests as the Twitter Revolution had been heard loud and clear by the Ahmadinejad regime. And as immigration resumed in the middle eastern country, many found it came along with a new question: "Do you have a Facebook profile?"

Foreign Policy columnist Evgeny Morozov was among the first to note this practice in a July 10, 2009 column entitled *Are Iranian Authorities More Sophisticated Than We Think?* (Morozov, 2009) But Iranian officials it seemed weren't as immediately interested in the content of users Facebook profiles, as they were in their connections. Reports of profile inspections at immigrations centered not around logging information like status updates, but from examining friends lists.

In an age of digitally mediated friendships, social networks can present governments with new ways to track associations between members of dissident movements. And using associational analysis like the "birds of a feather" types mentioned previously could help determine individuals likelihood of sharing political opinions.

Friends lists are unique amongst the features of Facebook in that anyone can access a users friend list, even without being their friend themselves. This allows researchers to draw connections based on real world knowledge without even having to access the richer data contained within a users profile. If immigration officials want to make sure that they don't allow anyone who is friends with a specific individual into the country, one way of confirming that relationship could be by checking their friends list on social networks.

The idea that friends often share political leanings is not new. A 1940's research study by Paul Lazarfeld at Columbia University presented strong evidence that behaviors and ideas such as politics can be "contagious" amongst groups of friends. (Thompson, 2009) What is

new is the ability for governments to trace these social connections and make use of them now that they are digitally archived.

The logging of Facebook friends by Iranian officials appears even more sinister in light of the recent events in Egypt and Tunisia. The Mubarak government made documented use of names found via social networks to arrest individuals once they left Tahrir Square. (Gallagher, 2011) And now that social tools like Facebook and Twitter are seen as platforms for planning protest, the penalties for not protecting your social graph can be increasingly dire.

And these techniques aren't only being used by oppressive dictatorships. The United States Central Intelligence Agency have made significant investments in purchasing personal data sets from Social Media Monitoring (SMM) companies. (Hoover, 2009)

DETERMINING CREDIT REPORTS

But your online friends list needn't have anything as glaring as a political zealot or potential terrorist amongst it to impact your future in a negative way. Social Media Monitoring companies like Rapleaf and Trackur are using your virtual sphere of influence to help determine things as common as your credit score.

In these scenarios, risk associated with loans are determined partially by the company you keep: Users connected with individuals who have bad credit histories receive lower reports. Those whose profiles are connected with friends that have high credit ratings, receive higher scores. (Taylor, 2010)

These companies also monitor the conversations you have over social networks to make determinations about loan eligibility. Ken Clark, author of *The Complete Idiot's Guide to Boosting Your Financial IQ* describes it in the following way: "Social graphs can pre-emptively cut the amount of charge-offs by not giving high-risk people a card." (Sandberg, 2010)

But is such behavior really fair? And should factors such as economic risk really be determined by the company you keep online? Arguments about whether this kind of information should be used are really about what we consider public versus private

behavior. There is little doubt that if credit companies were tapping users phones and mining their conversations to determine economic solvency, the public would be outraged.

But social networks exist in a kind of no man's land, trapped between our collective idea public and private. Conversations on the subject often collapse into cynical conclusions that nothing you do online is private. And that may be true. But such conclusions are only true if we as a society allow it to be so. Which is why the way in which we respond to these new techniques and business models is so important. The decisions we make now as these new kinds of companies emerge, are likely to have vast implications on our futures. With that in mind we make the following suggestions for response.

POSSIBLE REMEDIES: LEGISLATION

Kantarcioglu suggests that the remedy to issues of privacy on social networks is going to have to come from legislative action. He argues that individuals who use social networks and corporations that operate them are not sufficiently incentivized to protect privacy to the extent that users want. "Government regulation is required because of the potential failure of free markets in this case," he said. "User ignorance... thinking like 'I'm normal, what behavior do I have to hide' lacks the incentive" to protect that user. In other words, corporations are only financially incentivized by profit, so the extent to which they protect your data corresponds to their desire to keep it private so as to sell it at some point. In addition, individuals are often unaware of the extent to which data mining can discover information about them that they thought was undiscoverable. The only recourse, then, is legislative.

Specifically, Kantarcioglu argues that "the default should be data should not be sold. It should be used for marketing purposes only if you opt in explicitly."

DATA PORTABILITY AND USER-CONTROLLED SOCIAL NETWORKS

Some people argue that data portability is the solution to online privacy issues – that people, and not large companies, should own their online data and decide who can see it and where.
Some of the major Web companies, including Facebook and Google, have recently implemented data portability features. Google, which began this initiative in 2007 with a group it calls The Data Liberation Front, allows users to export data from a number of products, including Picasa, Google

Blogger, and Gmail (Google, 2011). In October 2010 Facebook introduced an option to download everything from your profile into a zip file.

While these initiatives allow data, such as photos, to be exported and then imported to other sites, the data is still ultimately on those companies' servers, in the "cloud," where it is used to bring in lucrative advertising, among other uses. These projects don't meet users' desire to control their data themselves. In 2010, when Facebook was getting a lot of heat for its privacy issues, a group of college students decided to create an open-source alternative to the centralized Facebook model. The project, called Diaspora, allows people to set up their own servers ("seeds") and create "hubs" for sharing information with friends (Singel, 2010). The founders describe Diaspora as a "privacy-aware, personally controlled, do-it-all open source social network."

SELF-DESTRUCTING DATA

"What goes on the web, stays on the web," the saying goes. But what if online data, instead of being permanent, could self-destruct, leaving no trail? Roxana Geambasu, a Ph.D student at the University of Washington, has developed a software prototype with some colleagues that causes data such as web mail or Facebook messages to self-destruct after a set period of time.

The software, called Vanish, was developed in response to how the rise of new technologies such as cloud computing have affected the security and privacy of people's data. And that includes social networks. "One of the problems is that … users cannot tell what happens to their data after they've uploaded to one of the online social networking services, like Facebook," said Geambasu in an email. "These services essentially take over ownership of our data and provide us with very little control back. For example, once you upload the data to Facebook, you can no longer ensure who accesses the data or how long the data will be retained."

Vanish works by encrypting data. The person who gets an encrypted message or document can decode it, but then the ability to decode it expires, and it turns to gibberish. No one can read the message or document again, not even the sender (Flatow, 2009). Geambusu says it's designed to "simulate the ephemeral nature of a phone call with online communications systems like web mail."

The idea of self-destructing data is to give control of one's data back to the user. If users could

decide what stays on the web and what doesn't, this has implications for the data brokers and other businesses that monetize that data.

REFERENCES

Angwin, J. & Stecklow, S. (2010, October 12). "'Scrapers' Dig Deep for Data on the Web," *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html

Bilton, J. (2010, May 12). "Price of Facebook policy? Start clicking. *The New York Times*. Retrieved from http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html

boyd, d. & Hargittai, E. (2010, August 2). Facebook privacy settings: Who cares? *First Monday*. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

Burnham, K. (2011, December 15). "Facebook's New Timeline: Important Privacy Settings to Adjust Now." CIO.com. Retrieved from http://www.cio.com/article/690742/Facebook_s_New_Timeline_Important_Privacy_Settings_to_Adjust_Now.

Christopherson, K. M. (2007). The positive and negative implications of anonymity in internet social interactions: "on the internet, nobody knows you're a dog". *Computers in Human Behavior., 23*(6), 3038.

Diana, A. (2011, Feburary 24). "Facebook cracks down on third-party apps." InformationWeek. Retrieved from http://www.informationweek.com/news/internet/social_network/showArticle.jhtml?articleID=229219361

Efrati, A. (2010, September 28). "Tweet this milestone: Twitter passes Myspace." *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/digits/2010/09/28/tweet-this-milestone-twitter-passes-myspace/

Facebook (2010a, April 15). Automated Data Collection Terms {web page]. Retrieved from http://www.facebook.com/apps/site_scraping_tos_terms.php

Facebook (2010b, December 21). Privacy Policy [web page]. Retrieved from http://www.developers.facebook.com/policy.php

Facebook (2011). Statistics [web page}. Retrieved from http://www.facebook.com/press/info.php?statistics

Flatow, I. (Host). (2009, July 31). :"Who really owns your digital data?" Washington DC: NPR. Transcript retrieved from http://m.npr.org/news/front/111421072?singlePage=true.

Gallagher, Ian. (February 6, 2011). *Egyptian Police Use Facebook and Twitter to Track Down Protesters' Names Before Rounding Them Up.* Daily Mail Online. Retrieved March 20, 2011 from http://www.dailymail.co.uk/news/article-1354096/Egypt-protests-Police-use-Facebook-Twitter-track-protesters.html

Geambasu, R. (personal communication, March 8, 2011).

Goldman, D. (2010, December 13). "Why your Facebook ID is marketer's Holy Grail." CNN. Retrieved from http://money.cnn.com/2010/12/13/technology/facebook_id_privacy/index.htm

Google (2011). Data Liberation Front FAQ {web page}. Retrieved from http://www.dataliberation.org/home/faq#TOC-Why-are-you-doing-this-What-s-the-cLenhart, A.,

Hoover, Nicholas (October 22, 2009). *CIA Invests in Social Media Monitoring Technology.* Information Week. Retrieved March 19, 2011 from http://www.informationweek.com/news/government/info-management/showArticle.jhtml?articleID=220900005

Madden, M. & Smith, A. (2010, May 26). Reputation management and social media. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf.

Myspace (2011). Privacy settings: What you need to know {web page}. Retrieved from http://www.myspace.com/pages/privacysettings

Morozov, Evegny. (July 10, 2009). *Are Iranian Authorities More Sophisticated Than We Think?* Foreign Policy. Retrieved March 19, 2011 from http://neteffect.foreignpolicy.com/posts/2009/07/10/are_iranian_authorities_more_sophisticated_than_we_think

Nixon, J. (2010, July 28). 100 million Facebook pages leaked on torrent site {blog post}. Retrieved from http://www.thinq.co.uk/2010/7/28/100-million-facebook-pages-leaked-torrent-site/

Opsahl, K. (2010, April 28). Facebook's eroding privacy policy: A timeline {blog post}. Retrieved from http://www.eff.org/deeplinks/2010/04/facebook-timeline/

Purcell, K., Smith, A., & Zickuhr, K. (2010, February 2). Social media and young adults. Retrieved from http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults/Summary-of-Findings.aspx

Rambom, S. (2008) Privacy is Dead, Get over It. Retrieved February 7th, 2011 from http://video.google.com/videoplay?docid=3079242748023143842#

Richmond, R. (2011, March 1). "Facebook facelifts its privacy policy." *The New York Times*. Retreived from http://gadgetwise.blogs.nytimes.com/2011/03/01/facebook-facelifts-its-privacy-policy/

Sandberg, Erica. (January 13, 2010). *Social Networking: Your Key to Easy Credit?* CreditCards.com. Retrieved March 20, 2011 from http://www.creditcards.com/credit-card-news/social-networking-social-graphs-credit-1282.php

Segall, L. (2012, March 23). "Facebook strips 'privacy' form new 'data use' policy examiner." Cnn Money Tech. Retrieved from: http://money.cnn.com/2012/03/22/technology/facebook-privacy-changes/index.htm.

Singel, R. (2010, August 26). "Open-Facebook Competitor Diaspora Sets Sept 15 Launch Date." *Wired.* Retrieved from http://www.wired.com/epicenter/2010/08/diaspora-luanch/

Steel, E. & Fowler, G. (2010, October 18). "Facebook in privacy breach." *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html

Solove, D. J. (2006). A TAXONOMY OF PRIVACY. *IUPA University of Pennsylvania Law Review, 154*(3), 477-564.

Taylor, C. (2012, September 4). "Most Facebook Apps can Post Behind Your Back." Mashable. Retrieved from: http://mashable.com/2012/09/04/most-facebook-apps-post-behind-your-back-exclusive/.

Taylor Jr., Joe. (January 21, 2010). *Facebook Friend Lists Could Impact Credit Card Interest Rates.* CreditRatings.com. Retrieved March 20, 2011 from http://www.cardratings.com/credit-card-interest-rates-facebook.html

Thompson, Clive (September 10, 2009). *Are Your Friends Making You Fat?* New York Times Magazine. Retrieved March 19, 2011 from http://www.nytimes.com/2009/09/13/magazine/13contagion-t.html?pagewanted=all

Thurm, S. and Kane, Y.I. Your apps are watching you, *Wall Street Journal* December 17th 2010 Retrieved on February 11th, 2011 from http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

Tsotis, A. (2010, July 28). "Hacker proves Facebook's public data is public." *TechCrunch*. Retrieved from http://techcrunch.com/2010/07/28/hacker-proves-facebooks-public-data-is-public/

Van Buskirk, E. (201, February 9). "What do we want? Our data! When do we want it? Now!" *Wired.* Retrieved from http://www.wired.com/epicenter/2010/02/what-do-we-want-our-data-when-do-we-want-it-now/

Vernal, M. (2010, October 17). An Update on Facebook UIDs [blog post]. Retrieved from

http://developers.facebook.com/blog/post/422

zennie62 (2010, January 10). Facebook CEO Mark Zuckerberg: TechCrunch Interview {video file}. Video posted to http://www.youtube.com/watch?v=LoWKGBloMsU

Zuckerberg, M. (2010, October 6). Giving you more control [blog post}. Retrieved from http://blog.facebook.com/blog.php?post=434691727130.