Kurt Medley

Ethics and Technology

February 10, 2012

Policy Vacuums within Social Networking Services

As Social Networking Services (SNS) become heavily intertwined into contemporary life within the U.S. and elsewhere, the deliberation for correct ethical standards regarding privacy policies and the transparent notion of data mining is forced into action. The clear inability to classify personal information within a forum type context as public or private has lead to ethical questions regarding online personal privacy. These conceptual muddles have recently been addressed by major SNS's like Facebook, Twitter, and MySpace but not clarified.

Theoretically speaking, there is no way of guaranteeing the security of one's personal information if it is first initialized within a database. The ability of third party, unaffiliated, entities absorbing information about potential clientele remains a prominent drawback in the struggle for online personal privacy. As part of a research project, two MIT students, using an automated script, were able to data mine over 70,000 Facebook profiles from four schools (MIT, NYU, the University of Oklahoma, and Harvard University) [1]. This was in 2005, and since then, Facebook has implemented dramatic changes in its security protection for users. It remains uncertain, though, how efficient such alterations really are. For standard users and technically savvy users alike, the issue remains shrouded with uncertainty and the resolution totally ambiguous.

Private information becomes disseminated within SNSs more so than in data pools of other businesses because of the manner by which SNSs operate and generate reve-

nue. A SNS is usually a free service, which means it must cater to third party companies and marketing strategies implemented by these companies in corroboration with its own standards. This usually means advertisement. For the same reason a Internet user may receive unwanted mail - or "spam" - as its appropriately referred to, is the same reason a Facebook user might receive unwanted messages or be subjected to more malicious actions. The clause concerning Facebook's right to sell users' data to private companies was addressed: "We may share your information with third parties, including responsible companies with which we have a relationship." This statement was eventually removed from the Facebook privacy policy and dismissed, in essence, without any sort of reprimand of the company [2].

Interestingly, these sort of problems carry more weight than they seem to. A Facebook representative who cannot vouch for an affiliated company's intent to store or sell personal information seems unethical, especially when personal information is distributed to these companies. Facebook (and similar SNS) cannot guarantee that stored personal information won't be distributed to unwanted affiliates of affiliates and thereby nullifies an argument that only "companies with good standing" have access to any personal information.

"Terms of Use" contracts present a separate conceptual muddle entirely but contribute directly to hidden data mine efforts. It would not be unreasonable to consider the fact that within "Terms of Use" contracts, lay hidden embedded "acknowledgements" to publicize personal information to (but not limited to) selective third parties by which have the ability to further circulate this information. The conceptual muddle lies with the fundamentals of the phrase, "Terms of Use", where a potential user is subjugated to an ar-

ray of fine printed terms by which they must agree to proceed. Usually within these agreements hide elusive ways of maneuvering around a potential user's true information confidentiality. In December 2009, US privacy organizations filed a complaint with the Federal Trade Commission regarding Facebook's Terms of Service. They claimed that Facebook's new policy of sharing users' home addresses and mobile phone information with third-party developers were 'misleading and fail[ed] to provide users clear and privacy protections', particularly for children under age 18 [3].

The problem lies with the notion of "privacy" on a public medium like the internet. Often, people argue against the legitimacy of a system that could lead to complete confidentiality in regard to SNS. An effectuate method for the guarantee of online personal privacy would be to implement a sort of policing force upon these systems. This, unfortunately, seems to be the only effective way of monitoring the trafficking of personal data across cyberspace and into data pools used by affiliated parties (or unaffiliated parties). This policy vacuum seems untouchable in the sense that a policing system installed to monitor SNS would be an infringement of a company's rights and would encourage an uproar of anti-censorship protests amongst supporters of SNS. The only viable solution may lay with the ethical development of particular SNS features by ethically polarized developers; how modules harvest, store, and share information inputed from the user. Search engines come under direct fire with these issues as well; Google and Yahoo having to rework and restructure their entire privacy policies for the conservation of user loyalty and thereby continuing their revenue stream. The ambiguity residing in the semantics used in "Terms of Use" and "Terms of Service" agreements must be disseminated themselves and reinterpreted for the safe passage and/or storage of information.

But with a medium like the internet and cyberspace, I see no immediate solution that would satisfy all parties.

Works Cited

1. Jones, Harvey, & Soltren, José Hiram (2005). *Facebook: Threats to Privacy*. Cambridge, MA: MIT (MIT 6.805/STS085: Ethics and Law on the Electronic Frontier - Fall 2005).
2. Peterson, Chris (February 13, 2006). "Who's Reading Your Facebook?". The Virginia Informer.
3. *Los Angeles Times*. 3/1/11. http://articles.latimes.com/2011/mar/01/business/la-fi-facebook-minors-201103