Kurt Medley

Seminar Paper 1

SNS and Translucent Data Mining

With the advent of the SNS comes the redefinition of what “personal privacy” constitutes and how it is interpreted. Data mining, which was originally exclusive to public records, has now breached the physical limitations of such restrictive mediums and has had considerable leverage with reference to our perception of “personal” information and how it subsequently should be handled.

Data mining involves the indirect gathering of personal information through an analysis of implicit patterns discoverable in data (Tavani 151). The Nissenbaum model explains that a violation of “contextual integrity” involves disseminating information provided outside its original context. The violation within this theory outlines the unethical nature of data-mining and data-matching. The arrival of SNSs like Facebook have made access to such “personal” information conveniently accessible. Public personal information (PPI) has been a tool for SNSs and search engines alike. Web servers request “cookies” from the individual which are then generated into consumer profiles and sold to third parties (156).

Since current privacy laws offer individuals no protection in respect to how information about them acquired through data mining activities is subsequently used, we are left with the conceptual muddle of what the definition of “private” personal information is composed of. Because most personal data collected and used in data mining applications is considered neither confidential nor intimate in nature, there is a tendency to presume that such data must be default public data. The ability of third party, unaffiliated

entities absorbing information about potential clientele remains a prominent drawback in the struggle for online personal privacy. The Facebook Beacon initiative further represents the necessity for some kind of regulatory framework for the preservation of personal privacy. Facebook's original privacy agreement stated: "We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers, and other users of Facebook, to supplement your profile." (Tavani 155). The clause concerning Facebook's right to sell users' data to private companies initially stated: "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 [1].

According to Moor's Just-Consequentialist framework, the subjugation of such information to third parties represents an unethical policy based on the fact that certain harvested information may unwittingly cause unfavorable results. Information stored in data servers can be freely accessed by third parties. Techniques can then be used to cross reference personal information which may suggest a person's connection with two or more groups. And with the absence of policy protecting such activities, the individual has no power in protecting his/her identity.

"Terms of Use" contracts obscure what online-companies claim they have a right to do with personal information. 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) selected third parties who in turn have the ability to further circulate information. The "Terms of Use" agreement offers a scapegoat

to any claims of “personal privacy” infringement. A potential user of the SNS service is subjugated to an array 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 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 [2].

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. Implementing a method for the guarantee of online personal privacy would be to enact a sort of monitoring convention upon these services. This, unfortunately, seems to be the only effective way of overseeing the trafficking (and harvesting) of personal data across cyberspace. 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.

Moor stresses the “selection stage” as being a more practical solution for adopting policies based on a “better vs. worse” schema. There are some advantages to pattern

matching credit card history like the example where Tavani's credit card is fraudulently used and reported immediately to him based on his spending habits (154). These examples seem few and far between though. And as the definition of "personal privacy" expands with the exploitation of personal information, we are likely to see further restriction of the violation of "contextual integrity".

Works Cited

1. Peterson, Chris (February 13, 2006). "Who's Reading Your Facebook?". The Virginia Informer.

2. *Los Angeles Times*. 3/1/11. http://articles.latimes.com/2011/mar/01/business/la-fi-facebook-minors-201103

3. Ethics and Technology; Controversies, Questions, and Strategies for Ethical Computing. Herman T. Tavani