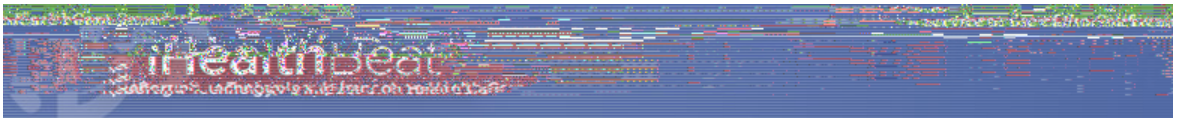

by Thomas H. Lee M.D.

Just when you thought all was harmonious in the land of open-source and socially collaborative Web 2.0, Facebook recently announced it would no longer allow Google's Friend Connect application to access Facebook users' data over "concerns about privacy."

According to Facebook engineer Charlie Cheever, "In the past, when we found applications passing user data to another party (for instance, to ad networks for the purpose of targeting), we suspended those applications and worked with those developers to ensure they respect user privacy. Now that Google has launched Friend Connect, we've had a chance to evaluate the technology. We've found that it redistributes user information from Facebook to other developers without users' knowledge, which doesn't respect the privacy standards our users have come to expect and is a violation of our Terms of Service."

For those not familiar with Google's Friend Connect, it's an interoperable application framework that allows users to bring their social networks and information to other sites without having to rebuild their social network information. As described by Google to potential beta hosts, "Google Friend Connect lets you grow traffic by easily adding social features to your Web site. With just a few snippets of code, you get more people engaging more deeply with your site."

Most view this move by Facebook as not for the sake of privacy (after all, this is the same company that created Beacon, an application where third-party sites were allowed to send unauthorized notices to friend networks in Facebook) but rather for the sake of maintaining control of user and social network data.

As odd and remote as the turf war for friendship networks may seem, the case helps illustrate some of the pivotal issues that could potentially impact the national roadmap to interoperable, private and secure health information. If powerhouses like Google and Facebook can't even reconcile how information about friends should be shared,

same volume of diabetic traffic but with only half reporting themselves as such due to privacy concerns.

Adding to the complexity, there are capitalist forces that promote interoperability at the expense of privacy (reselling data to third parties, transaction-based models) as well as privacy at the expense of interoperability (corporate consolidation/oligopolies, privacy-based subscription services). It is this fluid, complex dynamic that we're just beginning to see in the social networking space. And, as the stakes get higher, it's unlikely that it will get any simpler in the future.

How then do we foresee any resolution? Are we doomed to witness endless interoperability/privacy turf wars between Google Health, WebMD, Revolution Health and a myriad of upstart social network and health information service companies? Possibly. Unchecked, the forces seem to be moving us in that direction.

Nevertheless, it's possible that there are a few scenarios in which a more functional and balanced system could emerge.

One possibility is if the rules of engagement for using and sharing sensitive health information were to be more centrally or federally controlled. Currently, many information service vendors including Google Health are not subject to HIPAA or other privacy/sharing regulations. Instead, we must rely on privacy policies and trust the shareholders and executives of a corporation.

By mandating a uniform playing field for all vendors, some element of