

5/18/12 NOBRNC (No Page)

5/18/12 News & Observer (Raleigh NC) (Pg. Unavail. Online)

2012 WLNR 10505660

Loaded Date: 05/18/2012

News & Observer, The (Raleigh, NC)

Copyright 2012 McClatchy-Tribune Information Services

May 18, 2012

Opening up Facebook's privacy technology

Andrew Chin

If Facebook's initial public offering succeeds in achieving a \$90 billion valuation for the social network, each of Facebook's 900 million users can take pride in contributing \$100 toward the company's fortunes. If you're a user, Facebook's founder and 28 percent owner Mark Zuckerberg should consider you his friend. How many of your Facebook friends have enriched you by as much as \$28?

Facebook users would also be well advised to think of Zuckerberg as a Facebook friend. No matter how closely users may choose to guard their profiles and postings, they have no choice but to allow Facebook to access and store every piece of information they put on the site. Facebook has the access privileges enjoyed by their best friends, and then some.

Zuckerberg undoubtedly has better things to do with his time than spy on Facebook's users. But users should be aware that they're sharing information with a friend whose prime directive is to use that information to generate as much wealth for Facebook's shareholders as he can.

Given Facebook's difficulties in keeping its privacy promises in recent years, there's reason for worry. In November, Facebook settled a Federal Trade Commission complaint charging that the company deceived consumers by repeatedly allowing private user information to be shared and made public. The settlement requires Facebook to undergo audits for the next 20 years to "certify that the [company's] privacy controls are operating with sufficient effectiveness to provide reasonable assurance" that the FTC's concerns have been addressed.

Facebook should do more. When it goes public, it should release the full details of its privacy technology for public scrutiny, thereby disavowing any reliance on

the long-discredited practice of "security through obscurity." A strong privacy technology will be resistant to attack even when the technology is known.

In a reverse-engineering case study soon to be published in the North Carolina Law Review, Anne Klinefelter and I present evidence that Facebook has already quietly begun using one such technology.

Facebook never tells advertisers the exact number of users in their target audiences, even though it could. Instead, our study finds Facebook gives advertisers a number that includes statistical noise (taken from the Laplace distribution, for the nerds out there) and has been rounded to the nearest multiple of 20, and even internally stores these noisy numbers to hide the exact count from a persistent attacker.

It turns out that this elaborate technique is one of a small number of known approaches that can assure users of "differential privacy" – the guarantee that no one using Facebook's advertising system can tell whether any particular person is or is not a targeted Facebook user. And a differential privacy guarantee holds even if the whole world knows what privacy technology is being used to obtain it.

Why would Facebook go to such lengths to protect user privacy and not tell anyone? Because Facebook really doesn't want to share your information with every advertiser who comes along. Remember Facebook's prime directive. Access to your information is the source of Facebook's wealth; it's Facebook's competitive advantage.

But if we're right about the kind of privacy technology Facebook is using, there's no reason for Facebook to keep its details secret. When Facebook becomes a public company, it should make its privacy technology public, so that users can judge for themselves how effectively Zuckerberg is able to keep their information just among friends.

Andrew Chin is associate professor of law at the UNC School of Law . He also holds a doctoral degree in mathematics. The forthcoming North Carolina Law Review article is available at <http://unclaw.com/chin/scholarship/facebookprivacy.pdf>