FISH & RICHARDSON P.C.

One Marina Park Drive
Boston, Massachusetts
02210-1878

Telephone
617 542-5070

Facsimile
617 542-8906

Web Site
www.fr.com

Frederick P. Fish
1855-1930

W.K. Richardson
1859-1951

**VIA EMAIL**
[redacted]@perkinscoie.com

September 5, 2011

[redacted], Esq.
Perkins Coie
1201 Third Avenue
Suite 4800
Seattle, WA 98101-3099

Re: Face-to-Facebook Matter
Our Matter: 30625-0001001

Dear Mr. [redacted]:

We write in response to your April 7, 2011 letter. There, you purport to identify several "technical and security measures" that our clients allegedly evaded in their "Face to Facebook" project. In particular, and without any substantiation, you claim that our clients' bots "operate[d] at a speed that evaded Facebook's captcha-based protections" and "pretend[ed] to be a different browser (cycling through approximately ten different browsers) each time it issued a scraping request to Facebook." Finally, you assert that our clients "were aware of and blatantly ignored Facebook's robots.txt file."

We have investigated these allegations and are concerned that Facebook is either woefully uninformed about its own practices generally and this particular matter specifically, or that Facebook is demonstrating a lack of candor in this discussion, for several reasons.

First, our understanding is that Facebook did not implement any captcha-based protections at the time of the Face to Facebook project, other than to protect against a user who appeared to be adding too many friends at once—an activity clearly not at issue here. Indeed, readily-available public documents indicate that the "captcha-based protections" Facebook contends were evaded were only implemented by Facebook as a response to several high-profile "crawling" incidents, ***after*** the data was collected for the Face to Facebook project. In particular, we draw your attention

to the following articles, all of which post-dated the data collection at issue here:

- **100 Million Facebook Pages Leaked On Torrent Site**
  July 28, 2010
  http://slashdot.org/story/10/07/28/1350222/100-Million-Facebook-Pages-Leaked-On-Torrent-Site

- **Russian Hacker Selling 1.5 Million Facebook Accounts**
  April 23, 2010
  http://mashable.com/2010/04/23/hacker-facebook/

- **Facebook Kills Dataset of Crawled Public Profiles**
  March 31, 2010
  http://yro.slashdot.org/story/10/03/31/1430256/Facebook-Kills-Dataset-of-Crawled-Public-Profiles
  (Discussing crawler that collated 210 million Facebook profiles)

- **Data sifted from Facebook wiped after legal threats**
  March 31, 2010
  http://www.newscientist.com/article/dn18721-data-sifted-from-facebook-wiped-after-legal-threats.html

Moreover, the speed at which our clients' software operated was specifically designed to prevent undue load on their computer—and not to evade any alleged captcha protections.

Second, regarding your claim that our clients' software "pretend[ed] to be a different browser," we have also been unable to uncover any evidence that Facebook used the browser string in an HTTP request for any security purpose.

Finally, we do not understand the basis for your claim that our clients were "aware of and blatantly ignored Facebook's robots.txt file," nor, in any event, do we see the legal significance of this claim. As we understand your claim, a user violates the Computer Fraud and Abuse Act, potentially incurring criminal liability, when he or she fails to comply with the voluntary protocol described in the December 6, 1996 IETF Internet Draft entitled "A Method for Web Robots Control." This is not the law. *See Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627 (E.D. Pa. 2007).

As we do not see any proper basis for liability, we also do not understand why Facebook believes it is entitled to the relief demanded in your April 7 letter. Moreover, given the recent controversy and questions regarding the legality of

Facebook's own "facial recognition" software (see attached), we are surprised that Facebook would continue to aggressively pursue a nonprofit conceptual art project that illustrated the risks of sharing data on social networking websites and wrapped up long ago.

Very truly yours,


Adam J. Kessel

cc: Joel Leviton, Esq.
Matthew L. Levine, Esq. (Law Offices of Matthew L. Levine, PLLC)

Enclosure