SPALDING & THOMASON

LAW OFFICE

From The Desk of
Lee Thomason, Esq.
thomason@spatlaw.com

July 8, 2010

Hon. Donald S. Clark
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex J)
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: In the Matter of Twitter, FTC File No. 092 3093
Request for Public Comments, 75 Fed. Reg. 37806 (Jun. 30, 2010)

Dear Secretary Clark,

The following comments are submitted in response to the FTC's request for public comments on a proposed Consent Decree with Twitter. Confidential treatment is not requested for any part of this paper or any of the comments.

The summary description of the Twitter matter in the agency's News Release, and the provisions of the proposed Consent Decree, have dissimilarities. In summary, the FTC noted specific "steps," such as "hard to guess passwords," and "passwords in plain text," but in the proposed Consent Decree those steps are not expressly mentioned. Moreover, the unique Twitter passwords, and where and in what format to stored, are matters for consumers to decide, not the FTC. Indeed, the Commission has "no authority" over practices which are "reasonably avoidable by consumers themselves." 15 U.S.C. §45(n).

A broader question is whether the FTC has general jurisdiction over websites, or over website operation protocols, or the data protection measures used by website and social network operators. The corollary issue is whether FTC has power over website and social media network operators to impose standards that are co-extensive with the data protection standards that legally it may require of companies regulated by the agency, such as financial institutions and those handling financial transactions and payment card transactions.

Twitter is a social media network, which one can join without payment, or use of a payment card or bank account, and without use of any phone number, or disclosing any physical address, social security or drivers license number, or equivalent information. The individualized Twitter site name and unique password are chosen by users. In fact, users are free to join Twitter using anonymous names and 'dummy' email addresses. Users can choose who to communicate with, or whose communications get "blocked".

106 North 4th St.
P.O. Box 745
Bardstown, KY 40004
tel. (502) 349-7227

Directives in the proposed Consent Decree with Twitter are the same as, or are wholly similar to those in FTC decrees with companies that plainly are subject to the Gramm-Leach-Bliley requirements, *e.g.*, 16 C.F.R. Part 313. FTC clearly has authority, for example, over the "acts or practices by banks, savings and loan institutions," per 15 U.S.C. §57a(f). However, whether the FTC has statutory authority to impose mandates on social media networks and their operators is not free from doubts.

Prior FTC decrees, which arose largely from data security breaches involving payment cards, for example, mandates in order with CardSystems Solutions (FTC File No. 052 3148), with CVS Caremark (FTC File No. 072 3119), and with TJMaxx (FTC File No. 072 3055), are practically identical with Section II, parags. A-E of the decree proposed for Twitter. Again, those earlier decrees arose from transactions, and were with companies subject to, the administrative, technical and physical safeguards necessary for "financial institutions" to comply with the Gramm-Leach-Bliley requirements, *e.g.*, 16 C.F.R. Part 313.2(k)(2). Twitter is not subject to that regulatory regime. Twitter, as well as many other social networks, do not engage in financial activities or process payment card transactions, or provide equivalent services.

The administrative, technical and physical safeguard requirements in 16 C.F.R. Part 313 were duly promulgated, based on a rulemaking record supporting the rationale for imposing those requirements on "financial institutions." 65 Fed. Reg. 33646 (May 24, 2000). The same can be said about HIPAA privacy requirements. No support for administrative action imposing the same requirements on social networks is known.

For FTC to engraft these administrative, technical and physical safeguard requirements - appropriate to highly-regulated companies – into standards for the operation of social networking sites may be *de facto* rulemaking done outside the bounds of the APA. An agency cannot "create *de facto* a new regulation." *Christensen v. Harris County*, 529 U.S. 576, 588 (2000). To determine appropriately what data protection mandates can be imposed on social networks and their operators, the FTC would need to "give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments." 5 U.S.C. § 553(c). Doing less procedurally, but imposing mandates as burdensome "without observance of procedure required by law," exposes the agency action to judicial review. 5 U.S.C. § 706(2)(D).

The FTC Improvements Act authorizes the Commission to issue trade regulation rules which define unfair or deceptive acts or practices in or affecting commerce, but within statutory constraints. 15 U.S.C. § 57a(1)(B). The statutory mission of the FTC and its general jurisdiction has limits, and the agency "is constrained by its congressional mandate." *F.C.C. v. Fox Television Stations, Inc.* ___ U.S. ___ , 129 S.Ct. 1800, 1826, 173 L.Ed.2d 738 (2009) J. Stevens, dissenting. "In relation to administrative agencies, the question in a given case is whether it falls within the scope of the authority validly conferred." *Crowell v. Benson*, 285 U.S. 22, 55 fn. 17 (1932).

The proposed Consent Decree, imposing on Twitter, a non-financial institution, the same operational safeguards and data protection requirements appropriate to regulated companies that maintain consumers' personally-identifying information and financial data, may be taken as the FTC setting rules generally applicable to companies and data operations outside the statutory and regulatory limits of the agency.

Simply put, if the FTC mandates that Twitter implements these "administrative, technical and physical" safeguards, then every social network and most every website operator must too implement protocols no less stringent. In the normal course, for an administrative agency to impose such requirements, broadly on all sorts of non-financial and non-healthcare business, would require a rulemaking process, and it would be based on an issued rule or paper that is reviewable as agency action.

The proposed Consent Decree is less connected to the business regulated by the FT than to technical issues surrounding occasions when "Twitter was vulnerable" to hacker attacks, in part because Twitter users failed to do what might have made the unauthorized actions avoidable. It too is noted that wording in the proposed Consent Decree is ambiguous and undefined, or only gains clarity or definition when terms from the Gramm-Leach-Bliley regulations, 16 C.F.R. Part 313, are incorporated *sub silentio* into the operative terms of the Decree.

Based on the foregoing, the Commission should reconsider the Decree, and too, should consider the broader questions about whether the FTC is tasked to regulate the social networks, and whether safeguards and protocols appropriate to financial and medical data are equally appropriate to social networks.

Respectfully submitted,

~ S ~

Lee Thomason

Cc: Laura Berger
Bureau of Consumer Protection
Via telefax: (202) 326-3799