UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

In the matter of:	)	
	)	
Jerk, LLC, a limited liability company,	)	DOCKET NO. 9361
	)	
Also d/b/a JERK.COM, and	)	
	)	PUBLIC
John Fanning,	)	
Individually and as a member of Jerk, LLC,	)	
	)	
Respondents.	)	
	)	

OPPOSITION OF RESPONDENT JOHN FANNING TO COMPLAINT COUNSEL'S MOTION FOR SUMMARY DECISION

Respondent John Fanning ("Fanning"), pursuant to Section 3.24 of the Commission's Rules of Practice, opposes Complaint Counsel's Motion for Summary Decision. Complaint Counsel is not entitled to relief, as a matter of law. Complaint Counsel fails to establish all essential elements of a Section 5 claim, improperly seeks to extend the Commission's regulatory authority, unlawfully seeks to repress Fanning's free speech in violation of the First Amendment, improperly pierces the corporate structure, and requests remedies that multiple courts have rejected as over-reaching and in violation of the Commission's mandate. Fanning is entitled to the benefit of all inferences at this stage of the litigation. Summary decision is not appropriate, and Fanning is entitled to trial on the merits of the claims before an Administrative Law Judge, a neutral arbiter who will weigh the evidence and determine credibility, and not merely adopt Complaint Counsel's version of the facts and law. In further Opposition, Fanning relies upon the

Affidavit of John Fanning and the *Affidavit of Peter F. Carr, II, Esquire*, as well as his Memorandum of Law filed contemporaneously herewith.

For the foregoing reasons, Respondent John Fanning requests the Commission to deny Complaint Counsel's motion for summary decision, in its entirety.

Respectfully submitted,

JOHN FANNING,

By his attorneys,

/s/ Peter F. Carr, II
Peter F. Carr, II
ECKERT, SEAMANS, CHERIN & MELLOTT, LLC
Two International Place, 16th Floor
Boston, MA 02110
617.342.6800
617.342.6899 (FAX)
Email: pcarr@eckertseamans.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes, Rules, and Constitutional Provisions

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

In the matter of:	)	
Jerk, LLC, a limited liability company,	)	DOCKET NO. 9361
Also d/b/a JERK.COM, and	)	
John Fanning,	)	PUBLIC
Individually and as a member of Jerk, LLC,	)	
Respondents.	)	

MEMORANDUM OF RESPONDENT JOHN FANNING IN OPPOSITION TO COMPLAINT COUNSEL'S MOTION FOR SUMMARY DECISION

I. INTRODUCTION

Respondent John Fanning ("Fanning") cannot possibly be expected to respond to each and every statement, allegation, claim, or innuendo posited by Complaint Counsel in its Motion for Summary Decision, and the 183 separate statements of purported undisputed material facts strewn over 75 pages.[1] Indeed, many of the claimed facts by Complaint Counsel are not material, are disputed, and submitted solely to cast Fanning in a negative light. Complaint Counsel has no desire to try the case on the merits, so instead characterizes evidence and takes statements out of context to distort the truth to convince the Commission that punishment of Fanning is necessary because he is a scoundrel. Indeed, Complaint Counsel's statement of so-

[1] Because of the scope and breadth of the Statement of Material Facts, Fanning does not set forth specific responses to each numbered paragraph. The task would be virtually impossible, especially where many of the so-called facts are characterizations of the evidence by Complaint Counsel, who consistently lumps Fanning and Jerk, LLC together as "Respondents" throughout the pleadings. Complaint Counsel's flouting the rules requiring a short and plain statement of only those undisputed material facts excuses Fanning from any point by point response.

called undisputed material facts is such a blatant violation of the procedural rules, and all notions of fairness, that the motion should be stricken so that the case can proceed to trial where the Administrative Law Judge will weigh credibility, draw inferences, and make ultimate findings of fact to which the controlling law will apply. Summary disposition of the claims against Fanning is barred, no matter how many pages Complaint Counsel files. Complaint Counsel intentionally over-reaches, ignores controlling law, and attempts to expand unilaterally the regulatory authority of the Commission because Complaint Counsel cannot establish all essential elements of a Section 5 deception claim necessary to impose liability on Fanning. All claims asserted and remedies requested by Complaint Counsel must be tried on the merits consistent with Due Process and fairness instead of decided on summary disposition.

II. FACTUAL SUMMARY

Jerk.com was launched in approximately 2009 as an alternate social media and reputational website. Fanning served as an advisor to Jerk, LLC through another company called NetCapital.com, LLC. (Fanning Aff., ¶ 2). NetCapital.com. LLC is a private equity/venture capital firm that invests in and provides advisory services to technology start-ups. (Fanning Aff., ¶ 2). Jerk, LLC, an internet technology start-up, was not a typical large company with levels of management and regular employees. (Fanning Aff., ¶ 3). Fanning's authority was limited, and at all times Fanning acted on behalf of NetCapitlal.com, LLC as a corporate entity, never in his individual capacity. (Fanning Aff., ¶ 3). Fanning did not write any software code for Jerk, LLC to operate Jerk.com, and did not place any consumer content on Jerk.com. (Fanning Aff., ¶ 3). Fanning, personally, was not responsible for spearheading and operating Jerk, LLC or Jerk.com. (Fanning Aff., ¶ 3).

Jerk, LLC did not even own a website. Rather, Jerk, LLC operated the Jerk.com site through a lease with an option to purchase agreement entered into with a company called Internet Domains in February 2011. (CX0526-007). In or about May 2013, Internet Domains terminated the lease agreement and took control of the Jerk.com domain. (CX0527-001-003). Any information posted on Jerk.com prior to the commencement of the domain lease and after May 2013 is highly suspect, given that Internet Domains owned the domain name. Jerk, LLC terminated involvement with Jerk.com by the end of 2013, and profiles previously posted on Jerk.com no longer existed.

Jerk, LLC established an agent, a lawyer in Phoenix, Arizona, to accept service of complaints about Jerk.com. (Fanning Aff., ¶ 4). Each time that Jerk, LLC received a valid complaint, Jerk, LLC took action including to remove content from the Jerk.com site and to refund money to consumers who claimed they had paid but had not received services. (Fanning Aff., ¶ 4). Jerk, LLC experienced a number of problems in operating the site, including the site being hacked. (Fanning Aff., ¶ 4). The FTC also made written demand on Jerk, LLC to take corrective action. Although the company denied any liability, Jerk, LLC consistently complied with the FTC's demands. (Fanning Aff., ¶ 4).

Facebook complained that Jerk, LLC was violating policies and procedures concerning use of Facebook. Jerk, LLC rejected the allegations, and neither Jerk, LLC nor Fanning violated any valid contract or agreement with Facebook with respect to Jerk.com. (Fanning Aff., ¶ 5). Any information posted on Jerk.com that Facebook charged was a violation derived from users or public sources. (Fanning Aff., ¶ 5). In fact, the entire Facebook directory containing user information and photographs was readily available to the public through the internet, and any person could have accessed the directory and posted the information on Jerk.com. (Fanning Aff.,

¶ 5). Fanning never hacked into Facebook, and never directed anyone affiliated with Jerk, LLC to hack into Facebook with respect to Jerk.com. (Fanning Aff., ¶ 5).

On December 17, 2009, the Electronic Privacy Information Center ("EPIC"), a Washington-based advocacy group, filed a complaint against Facebook related to its privacy policies and procedures. (EPIC Complaint, attached to Carr Aff., at **Tab A**). The FTC conducted an investigation into Facebook's privacy settings. The FTC subsequently filed an enforcement Complaint against Facebook. (FTC Complaint, attached to Carr Aff., at **Tab B**). In summary, the FTC alleged that Facebook deceived consumers by representing that consumers could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. The FTC claimed that Facebook's privacy settings, revised in November 2009 without notice to its users, were unfair and deceptive toward users because the settings permitted personal information to be disclosed to the public and third-party application developers. Facebook treated the following categories of personal data as "publicly available information" subject to public disclosure and access: user names, profile photos, lists of friends, pages users are fans of, gender, geographic regions, and networks to which users belonged. By default, Facebook regularly disclosed "publicly available information" to search engines, to internet users whether or not they used Facebook, and other third-parties. Facebook eventually settled the case with the FTC pursuant to a consent order. (Decision and Order, attached to Carr Aff., at **Tab C**).

In 2012, Complaint Counsel commenced an investigation of Jerk, LLC related to Jerk.com, claiming violations of Section 5 of the FTC Act based on alleged deceptive conduct. Complaint Counsel served broad Civil Investigative Demands on Jerk, LLC and numerous third-parties. The FTC was upset when Fanning refused to be interviewed as part of the investigation. (Fanning Aff., ¶ 6). During the course of the investigation, Complaint Counsel obtained sworn

statements, drafted with the direct assistance of Complaint Counsel and other FTC agents, from various consumers who had visited Jerk.com. According to Complaint Counsel, profiles posted on Jerk.com grew to in excess of 85 million. Yet, Complaint Counsel obtained sworn statements from a limited number of consumers. The bulk of the complaints involved angry consumers who allegedly learned that information they had posted on Facebook, and believed was private, appeared on Jerk.com without their consent. Not one of the sworn statements indicates that a consumer posted information on Jerk.com in reliance on any representations made by Jerk, LLC or Fanning.

III. LAW AND ARGUMENT

A. Complaint Counsel is Not Entitled to Summary Decision

The Commission has recognized that the standard of review for summary decision is "virtually identical to Federal Rule of Civil Procedure 56." In re McWane, Inc., 2012 WL 4101793, at *5 (2012), citing In re Polygram Holding, 136 F.T.C. 310, 2002 WL 31433923, at * 1 (2002). Summary judgment under Rule 56 is appropriate "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). In order to prevail, a party moving for summary judgment must show the absence of a genuine issue of material fact with respect to an essential element of the nonmoving party's claim, or to a defense on which the non-moving party will bear the burden of persuasion at trial. Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). "[T]he inquiry involved in a ruling on a motion for summary judgment ... implicates the substantive evidentiary standard of proof that would apply at the trial on the merits." Anderson v. Liberty Lobby Inc., 477 U.S. 242, 252 (1986). On summary judgment, the court draws all reasonable factual inferences in favor of the non-movant. Anderson, 477 U.S. at 255.

A court's role in ruling on motions for summary judgment is limited. "[A]t the summary judgment stage the judge's function is not . . . to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial." FTC v. Ross, 2012 WL 2126533, at * 4 (D.Md. 2012), quoting Anderson, 477 U.S. at 249 (copy attached to Carr Aff., at **Tab E**). "Even if the facts are undisputed, summary judgment may not be granted where there is disagreement over inferences that can be reasonably drawn from those facts." Ross, at *4, quoting In re Unisys Sav. Plan Litig., 74 F.3d 420, 433 (3rd Cir. 1996).

Applying these well-established standards, Complaint Counsel fails to conclusively establish Section 5 liability, and summary decision must be denied. Complaint Counsel has the burden of proving each essential element of each alleged violation of law. 16 C.F.R. § 3.43(a). As set forth below, Complaint Counsel fails to establish all essential elements of a Section 5 claim for deception, as a matter of law. Further, the relief sought by Complaint Counsel in its Proposed Order is unlawful applying well-settled legal principles governing FTC authority.

B. Complaint Counsel Fails to State a Legal Claim For Deception

Section 5 of the FTC Act expressly provides, "[t]he commission is empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce." FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 235 (1972), quoting 15 U.S.C. § 45(a)(6). The elements of a deceptive act or practice are: (1) a representation that is (2) likely to mislead the consumer acting reasonably in the circumstances that is (3) material. See FTC Policy Statement on Deception, appended to In re Cliffdale Assocs., Inc., 103 F.T.C. 1, 10, appendix at pp. 175-84 (1984). Complaint Counsel is unable to prove each essential element.

Sensing weakness in the claims asserted, Complaint Counsel either ignores or improperly attempts to expand the essential elements of deception liability under the FTC Act. Complaint Counsel did not include any claim for "unfairness" under Section 5, because of the more stringent standard that applies in unfairness cases, including the required showing of substantial injury to consumers. There is no basis for substantial injury in this case. Complaint Counsel should not be permitted to avoid the more stringent analysis by characterizing and pleading the claims under deception jurisdiction.

1. There is no material misrepresentation about Jerk.com content

With respect to the first prong, a representation conveys "a claim if consumers, acting reasonably under the circumstances, would interpret the advertisement to contain that message." POM Wonderful, LLC, 2013 LEXIS 6, at *20 (FTC Jan. 10, 2013). The heart of a "representation" giving rise to Section 5 liability is a "claim" communicated to the consuming public. See Cliffdale Assocs., 103 F.T.C. at 176. See also POM Wonderful, at *20 (actionable representation is one that conveys a particular interpretation to a reasonable consumer); In re Novartis Corp., 127 F.T.C 580, 689 (1999) (liability premised on respondent's knowledge that the deceptive claim was being communicated to the public); Kraft, Inc. v. FTC, 970 F.2d 311, 322 (7th Cir. 1992) (describing three types of "claims" within the FTC's statutory purview). Whether a statement is a "claim" constituting a "representation" is a question of fact. See FTC v. QT, Inc., 448 F.Supp.2d 908, 957-958 (N.D.Ill. 2006), citing National Bakers Services, Inc. v. FTC, 329 F.2d 365, 367 (7th Cir.1964) (meaning of an advertisement, the claims or net impressions communicated to reasonable consumers, is fundamentally a question of fact); Kraft, 970 F.2d at 317 ("[T]he determination of whether an ad has a tendency to deceive is an impressionistic one more closely akin to a finding of fact than a conclusion of law.").

Complaint Counsel cites as the lynchpin of Count I as follows: "Respondents represented that content on Jerk, including names, photographs, and other content, was created by Jerk.com users and reflected those users' views of the profiled individuals." (CCSMF, ¶ 39). Complaint Counsel, however, mis-states and falsely depicts the statements on the website. The interpretations and characterizations postured by Complaint Counsel do not suffice.

Complaint Counsel far exceeds the legal bounds of a "claim" properly regulated by the FTC by parsing and characterizing the language on the homepage, instead of pointing to specific, affirmative statements that were made to advertise or promote Jerk.com. This fatal defect alone requires denial of the relief requested. The Court in FTC v. Direct Marketing Concepts, Inc., 569 F.Supp.2d 285, 298-299 (D.Mass. 2008) outlined the rubric that is supposed to govern, as follows:

> Generally, claims can be divided into two categories-establishment claims and non-establishment claims. Establishment claims are those that contain "statements regarding the amount of support the advertiser has for the product claim." Policy Statement on Advertising Substantiation. They are in effect statements "that scientific tests establish that a product works." Removatron, 884 F.2d at 1492 n. 3. Common examples include statements such as "tests prove," "doctors recommend," or "studies show." Policy Statement on Advertising Substantiation; see also Thompson Med. Co. v. Fed. Trade Comm'n, 791 F.2d 189, 194 (D.C.Cir. 1986); Spalding Sports Worldwide, Inc. v. Wilson Sporting Goods Co., 198 F.Supp.2d 59, 67 (D.Mass. 2002); Gillette Co. v. Norelco Consumer Prods. Co., 946 F.Supp. 115, 121 (D.Mass. 1996) ("An establishment claim is one that says, in substance, that 'tests or studies prove' a certain fact."). In the case of establishment claims, the advertiser must be able to demonstrate that it has at least the advertised level of substantiation.
>
> In contrast, for non-establishment claims, what constitutes sufficient substantiation may depend on multiple factors, such as the type of claim, the product, the consequences of a false claim, the benefits of a truthful claim, the cost of developing substantiation for the claim, and the amount of substantiation experts in the field believe is reasonable. Removatron, 884 F.2d at 1492 n. 3; QT, 448 F.Supp.2d at 959 (citing Policy Statement Regarding Advertising Substantiation). For health-related efficacy and safety claims, the FTC has commonly insisted on "competent and reliable scientific evidence." See, e.g., Removatron, 884 F.2d at 1498 (reviewing Commission Order that required claims

to be supported by "competent and reliable scientific evidence"); Sterling Drug, Inc. v. Fed. Trade Comm'n, 741 F.2d 1146, 1156-57 (9th Cir. 1984) (same).

Instead of meeting this rigorous standard, Complaint Counsel falsely cites the statements appearing on the homepage, and concocts out of whole-cloth the claimed representations. The website does not include any affirmative statement about the origin of content. Complaint Counsel relies solely on and quotes to the statements previously featured on the Jerk.com homepage in the "About Us" and "Welcome to Jerk" tabs. (CCSMF, ¶¶ 40-46). A closer review, however, of the actual language shows that nothing is stated about content or views of users. In reality and taken in context, the language cited by Complaint Counsel is part of a legal disclaimer intended to advise users of the restrictions on use and limitation of liability associated with use of the site. (CX0273). Nothing contained in the homepage disclaimer constitutes a "claim" about the source of content, either express or implied, or could possibly be construed as an advertisement intended to lure users to the Jerk.com site. As a matter of law, Complaint Counsel has no legal basis to invoke deception jurisdiction based on the language cited. See Kraft, 970 F.2d at 322 (FTC authority is limited to (1) express claims; (2) implied claims where there is evidence that the seller intended to make the claim; and (3) claims that significantly involve health, safety, or other areas with which reasonable consumers would be concerned).

Moreover, a "material" misrepresentation is one that involves information important to consumers and that is therefore likely to affect the consumer's choice of, or conduct regarding, a product. In re Novartis Corp., 127 F.T.C. at 689. See also POM Wonderful, at *121 ("A misleading claim or omission in advertising will violate Section 5 . . . only if the omitted information would be a material factor in the consumer's decision to purchase the product."); Kraft, 970 F.2d at 322, quoting Cliffdale Assocs., 103 F.T.C. at 165 (claim considered material if

it "involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding a product."). The language in the legal disclaimer cribbed by Complaint Counsel was not presumptively material, and did not shape any reasonable consumer's choice with respect to Jerk.com.

It is pure speculation to infer that any reasonable consumer would have read the homepage disclaimer advising on limitations of liability, prohibited practices, and other technical information as concerning the purpose, safety, efficacy, or cost of the product or service. Nonetheless, to the extent Complaint Counsel relies upon inferences, Fanning is entitled to the benefit of all inferences at this stage. Further, Complaint Counsel provides no evidence to show that any consumer made or was likely to make any choice whether or not to participate in the Jerk.com site based on anything expressly or impliedly stated in the legal disclaimer language posted on the homepage. None of the consumer statements submitted by Complaint Counsel prove that any consumer was caused to participate or not participate in Jerk.com based on any statement contained on the site concerning the origin of content, users, or otherwise.

Tellingly, not one consumer who submitted a sworn statement indicates actually using the site to post content. The mere fact that consumers who viewed content on the site believed that it was posted by a friend or family member or could not understand how the information was posted, as asserted in the consumer statements, does not establish inducement. Instead, a review of the consumer statements collected by Complaint Counsel show, in essence, that individuals were upset that the information they had posted on Facebook, and believed was private, was appearing on Jerk.com.

All allegations concerning Facebook are irrelevant to the Section 5 claim. Significantly, Complaint Counsel only argues that the allegations pertaining to Facebook establish that the

alleged representations were intentionally false. However, at the same time, Complaint Counsel argues that a respondent's intent is wholly-irrelevant in assessing Section 5 liability. The Facebook allegations do not form any basis for liability in this case and must be stricken.

Nonetheless, Complaint Counsel's conclusory statements and arguments based on counsel's interpretation of Facebook's terms of use are of no consequence. Complaint Counsel never segregates specific profiles allegedly "scraped" from Facebook, as opposed to generated by some other source. Complaint Counsel speculates that profiles appeared on Jerk.com as a result of a violation of Facebook policies, which the FTC has no authority to enforce. Complaint Counsel likewise asserts, without admissible evidence, that Jerk, LLC was a party to a valid agreement with Facebook. Even if relevant, the existence of any such binding contractual relationship with Facebook is denied. (Fanning Aff., ¶ 5). Complaint Counsel also relies primarily upon the allegations contained in Facebook's legal cease and desist letter to Jerk, LLC as the basis for a violation. Such a bogus position, especially on summary decision, cannot possibly prevail. Complaint Counsel is, in fact, attempting to boot-strap the alleged violation of Facebook terms and conditions as forming the basis of a Section 5 action, as alleged in the Complaint. (Complaint, ¶¶ 10-11). Any such argument constitutes an unlawful expansion of the FTC's deception authority.

The irony of Complaint Counsel's position concerning Facebook cannot be overstated. The FTC charged Facebook with deception by representing to consumers that information posted in individual profiles was private with limited accessibility, when Facebook actually made the information publicly available through the internet. The FTC specifically identified information that was publicly available, and not actually private contrary to Facebook's representations, including user names, profile photos, lists of friends, pages users are fans of, gender, geographic

regions, and networks to which users belonged. This is the exact information that Complaint Counsel now contends was accessed improperly and posted on Jerk.com. Complaint Counsel states no legitimate explanation as to how Fanning or Jerk, LLC are liable for deception by allegedly posting the exact same information that was publicly available because Facebook made it publicly available. Even if Jerk, LLC or Fanning somehow violated a term and condition of use of Facebook, which is disputed, Complaint Counsel is unable to separate information taken from the public domain as opposed to information that may have violated a Facebook policy. The FTC also complained that Facebook regularly and by default disclosed "publicly available information" to search engines, to Internet users whether or not they used Facebook, and other third-parties. Now, Complaint Counsel contends, citing the FTC's regulatory authority, that Jerk.com violated the law by accessing and publishing the same information that Facebook permitted to be released to the public. Complaint Counsel's position is not only illogical, but meritless.

Complaint Counsel also fails, as a matter of law, to prove conclusively a Section 5 deception claim based on statements about the benefits of a paid Jerk membership, as generally asserted in Count II of the Complaint. Complaint Counsel improperly styles the claim as one for deception, without any basis, because consumers did not suffer any substantial injury to support an unfairness claim as required by the Act. 15 U.S.C. § 45(n). Count II should be stricken in its entirety. In no way does Count II, related to payment for membership services, permit or justify the overly-broad permanent injunctive relief sought in the Proposed Order. Count II is a total throw-in by Complaint Counsel.

The lack of merit of Count II is reflected in the vague pleading of the claim and arguments made by Complaint Counsel. The accusations are predicated on a mischaracterization

of the circumstances surrounding memberships and payments. Complaint Counsel comingles and interchanges references to enhanced membership benefits, subscriptions, and the ability to dispute or remove posted information from profiles. The facts cited indicate no such representations by Jerk, LLC or Fanning posted on the website. With no specific "claim" cited by Complaint Counsel, no deception exists. The mere fact that Complaint Counsel cites to testimony wherein Fanning allegedly discussed internally charging fees does not constitute a material representation relied upon by any consumer. Complaint Counsel combines all of these various statements from various sources, including upset consumers, to conflate a representation. Sometimes there is a reference to a $30.00 charge, and other times $2.00 to $5.00 per month is quoted. "Impressions" of consumers or FTC investigators are insufficient to prove undisputed facts supporting an actual false representation that was material.

The evidence does not conclusively establish that memberships did not exist, or that there were no actual subscriptions, or that the only way to remove a post was by paying money. It is just as likely that the failure to deliver so-called memberships, subscriptions, or passwords could have been the result of technical problems with the site. Indeed, Jerk, LLC refunded payments to disappointed consumers who reported problems with the site. Of the 85 million profiles that Complaint Counsel claims were posted on Jerk.com, only a handful of consumers, at best, apparently were not satisfied. Moreover, the evidence establishes that profiles were removed from the site at the request of consumers, law enforcement, and the FTC thereby establishing no nexus between payment of money and removal of a profile, as Complaint Counsel assumes, infers, and concludes. Complaint Counsel has not established a clear pattern or practice of deception. Instead, the evidence shows that there was a legitimate process for rectifying complaints and removing profiles, notwithstanding Complaint Counsel's exaggeration.

Finally, Fanning identifies the following categories of alleged facts identified by Complaint Counsel which unequivocally do not and cannot sustain a Section 5 deception claim as a matter of law and FTC regulatory policy:

> (i) Statements purportedly made by and between Fanning, interns, web designers, or other individuals to potential investors or other financial contacts within the technology investment community by email or otherwise, including statements contained in an alleged Executive Summary and other materials undeniably circulated for investment or internal promotional purposes, and not conveyed to or involving consumers (CCSMF, ¶¶ 47, 49, 59, 90);
>
> (ii) Statements purportedly made by and between Fanning to interns, web designers, programmers, or other individuals working on the Jerk.com project, and not conveyed to or involving consumers (CCSMF, ¶¶ 47, 54, 58);
>
> (iii) Observations made by or the understandings, beliefs, or impressions of interns, programmers, web designers, and other consultants working on the project about the scope, development, and purpose of the site, and not conveyed to or involving consumers (CCSMF, ¶¶ 48, 55, 57, 58, 60, 90); and,
>
> (iv) Statements made by and between legal counsel to Jerk, LLC to Complaint Counsel, third-parties, law enforcement, or other attorneys in response to discovery demands, cease and desist demands, or other legal proceedings (CCSMF, ¶ 50).

None of the above can be considered in the context of either the motion for summary decision or when the case proceeds to trial on the merits, because they do not involve communications directed to any consumer. No reasonable consumer could have acted on any statement that was not publicly communicated. Consequently, Section 5 is not triggered. Permitting Complaint Counsel to establish deception liability based on alleged internal communications within Jerk, LLC or communications involving non-consumers would turn the FTC's stated policy on deception on its head, and create an entirely new theory of FTC regulatory authority aimed at statements that never reach the public domain. Instead, Complaint Counsel's sole purpose of including this irrelevant information, most of which does not even constitute admissible evidence, is to portray Fanning in a false negative light and to play upon

the emotions of the finder of fact. Complaint Counsel does a fine job of character assassination, but fails to establish a legally-cognizable Section 5 claim.

2. Complaint Counsel cannot lawfully regulate the content of free public expression of thoughts, opinions, and ideas

In reality, this case is being driven by the substantive content of individual profiles on Jerk.com, not "claims" about the source of the content. Complaint Counsel is offended by or uncomfortable with the actual content of the individual profiles appearing on the Jerk.com site, and the alleged practice of Jerk.com posting publicly available information allegedly obtained from Facebook. Complaint Counsel dedicates numerous proposed findings of fact to a description of the content on the Jerk.com site, from photographs to personal information, as well as allegations pertaining to Facebook and its policies. Control of content far exceeds the Commission's regulatory authority and is unlawful.

Complaint Counsel fails to provide any basis for the FTC's authority within it regulatory mandate to determine what is proper content of an individual's profile. It is not a violation of Section 5 to call someone a jerk, or to invite dialogue and conversation about personal traits of an individual. Jerk.com provided a platform to exchange opinions and ideas in the free-flow of human relationships at the essence of social media. Each and every day, media outlets, pundits, newspaper editors, and talk show hosts opine on stories involving individuals, and provide personal views on people and events. Censorship and compression of the free flow of ideas and opinions is abhorrent to a democratic society, whereas the freedom of expression is the bedrock of the First Amendment. Complaint Counsel has no right to regulate, control, or halt the exchange and flow of ideas and information that is at the core of First Amendment freedoms. See, e.g., Kleindienst v. Mandel, 408 U.S. 753, 762-753 (1972) (First Amendment includes the right to "receive information and ideas" and freedom of speech "necessarily protects the right to

receive."); Central Hudson, 447 U.S. at 575 (Blackmun, J., concurring) ("If the First Amendment guarantee means anything, it means that, absent a clear and present danger, government has no power to restrict expression because of the effect its message is likely to have on the public."); Linmark Assocs., Inc. v. Louisiana, 379 U.S. 64, 74-75 (1964) ("speech concerning public affairs is more than self-expression; it is the essence of self-government.")

Complaint Counsel incorrectly attempts to portray the conduct as commercial speech subject to restraint. Commercial speech is defined as "expression related solely to the economic interests of the speaker and its audience." Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 561 (1980). Even commercial speech is protected from government repression. See Virginia St. Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762-764 (1976) (commercial speech protected by First Amendment because "consumer's interest in the free flow of commercial information" may be "as keen, if not keener by far, than his interest in the day's most urgent political debate."). Nevertheless, the speech actually championed by Jerk, LLC does not involve solely economic interests necessary to constitute commercial speech. Rather, the speech protected is the flow of information and public dialogue, including by posting a statement on the internet that someone is or acted like a jerk, and then receiving broader feedback on the opinions. The speech is not aimed at causing any consumer to act or rely for commercial purposes, or to generate revenue. It is aimed at criticizing, commenting on, and taking issue with individuals and points of view. Jerk, LLC had an absolute right to provide a forum for open public speech and debate despite Complaint Counsel's disagreement with the content of the views and opinions of citizens. Complaint Counsel cannot stand as the arbiter of proper conversation between and among users, and cannot prevent the flow of information under the pretext of protecting against deception. See Linmark

Assocs., Inc. v. Willingboro, 431 U.S. 85, 96 (1977) (striking ordinance banning "for sale" signs on residential property enacted for the goal of promoting stable, racially integrated housing, where Court found that the town council unlawfully "acted to prevent its residents from obtaining certain information" and "sought to restrict the free flow of data" out of fear that homeowners would leave town).

Jerk, LLC also provided a public referendum on Facebook, which also triggers essential First Amendment concepts. In addition to having the unfettered, lawful right to post and re-publish information that Facebook placed in the public domain, Jerk, LLC exercised the right to expose the falsity of Facebook's representations that all information posted was private. Jerk, LLC was not competing with Facebook for economic benefit; it was examining and exposing Facebook. Jerk, LLC showed that Facebook, the anointed darling of the social media world, was a sham on the issue of user privacy. The proclamations of privacy made by Facebook to increase its user base, and its revenue, were false and Jerk, LLC had an absolute right to expose them as false, just as the FTC did in bringing its enforcement action against Facebook. Public exposure serves the public interest, and increases competition in an open economy. Although Jerk, LLC's activities of exposing Facebook do not implicate commercial speech, the central First Amendment tenet of generating marketplace discussion reigns supreme even where commercial speech is involved. Virginia Pharmacy Bd., 425 U.S. at 763 (society has a strong interest "in the free flow of commercial information" critical to a free market economy).

Complaint Counsel's claims, which seek to quell speech and bolster Facebook, are unlawful and anti-competitive at their core, in direct contravention of the FTC's primary mandate to prevent methods of unfair competition to promote a level economic playing field. Jerk, LLC merely seized the opportunity to force Facebook to realize its own short-falls.

Facebook's claims of privacy were a hook that lured consumer users and investors alike. Jerk, LLC did not just state publicly that such promises were false. Jerk, LLC showed it. Shining the light on marketplace activity is the bedrock of free trade and a healthy economy. Any government interference is abhorrent to core freedoms. As Justice Brandeis once forcefully and artfully opined:

> If there be time to expose through discussion the falsehood and falacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.
>
> Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

3. Complaint Counsel's theory of liability unlawfully expands the FTC's regulatory reach contrary to its own prior rulings

The FTC's observations in the case of FTC v. ReverseAuction.com, Inc., 2000 US Dist. LEXIS 20761 (D.D.C. 2000) bear on Complaint Counsel's unlawful expansion of regulatory authority in the present action.[2] The FTC asserted that ReverseAuction, a competing auction site, willfully misled eBay by registering as an eBay user and representing that it would comply with the terms and conditions of eBay's User Agreement, including the agreement to refrain from using any personal identifying information of any eBay user obtained through the site for sending unsolicited commercial e-mails. The findings of the Commissioners in approving the Complaint are compelling and relevant to this case. Commissioners Swindle and Leary, concurring and dissenting in part, stated as follows:

> ReverseAuction represented to eBay that it would not use the information it obtained about other members to send unsolicited commercial e-mail. ReverseAuction, however, sent unsolicited e-mails promoting its auction site to eBay members using e-mail addresses harvested from eBay's site. ReverseAuction thereby deceived eBay directly and, in doing so, also misled other members of the eBay community who believed that all participants in the eBay marketplace would abide by the same privacy rules.

[2] Available at http://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm

> We recognize that the Commission's decision to proceed against the deception alleged in Count One could be construed as placing the Commission in the position of enforcing eBay's privacy policy. Nevertheless, we want to emphasize that our decision to challenge ReverseAuction's deception is an effort to buttress, not supplant or detract from, initiatives of private parties (like eBay) who develop and implement their own privacy arrangements. We further believe that it is in the public interest for the Commission to pursue the deception allegation in Count One because such deceptive conduct undermines consumer confidence in the nascent electronic marketplace at a critical point in time and may thereby inhibit its development.

See Statement of Commissioners Orson Swindle and Thomas B. Leary Concurring in Part and Dissenting in Part, in ReverseAuction.com, Inc., File No. 0023046 (attached to Carr Aff., at **Tab E**).[3]

These observations, analyses, and conclusions evidence the unlawful expansion of regulatory authority practiced by Complaint Counsel in this case. Perhaps most significantly, the Commission ultimately approved taking action under the FTC's deception jurisdiction because ReverseAuction made affirmative misrepresentations to eBay about compliance with terms of use, which the FTC concluded had an impact on consumers. Here, Jerk, LLC and Fanning made no such representations to Facebook. The Commissioners in ReverseAuction seemed to bend over backwards to justify enforcement action, particularly to protect the emerging electronic marketplace that existed at that specific time in 2000. Years have now passed, and the electronic marketplace, including the social media space, cannot possibly be described as "nascent" requiring protection. There exists no need to protect and coddle Facebook, the publicly-traded multi-media giant that dominates the space, in the ever-evolving and fast-paced competitive social media marketplace. Further, regulatory enforcement in this instance is inimical to Facebook's policies that absolutely did not promote and protect individual privacy, as the FTC specifically charged in filing its Complaint against Facebook. Commissioner Swindle

[3] http://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversesl.htm

emphasized that "our decision to challenge ReverseAuction's deception is an effort to buttress, not supplant or detract from, initiatives of private parties (like eBay) who develop and implement their own privacy arrangements." According to the Commission's own allegations, Facebook did not develop and implement "privacy arrangements" aimed at protecting the public from disclosure. There is nothing to buttress, using Commissioner Swindle's words, with respect to Facebook's policy of making information readily accessible to the public through the internet. The interests underlying the novel decision reached in ReverseAuction, which governed the FTC's decision to approve expanded Section 5 authority in that case, are not present here.

The significant evolution of the statutory landscape with respect to data privacy, internet security, and technology since the ReverseAuction case further cements the refusal to extend Section 5 deception authority under the facts and circumstances in this specific case. Congress has supplanted, and even preempted, the FTC's regulatory authority in the data privacy and security space by enacting a host of laws and regulations that govern on-line activities. See, e.g., The Digital Millennium Copyright Act,[4] The Fair Credit Reporting Act,[5] The Gramm-Leach-Bliley Act,[6] The Children's Online Privacy Protection Act,[7] and The Cable Television Consumer Protection and Competition Act[8]. Consequently, the field of on-line data and information including data privacy is completely occupied by other agencies empowered to regulate and establish rights and obligations with respect to internet privacy and data, and the FTC is out.

---

[4] 17 U.S.C. §512 et seq., (provides certain limitations on the liability of online service providers for copyright infringement)
[5] 15 U.S.C. §1681 et seq., (regulates data collected by consumer reporting agencies)
[6] 15 U.S.C. §6801 et seq., (imposes data-security requirements for financial institutions)
[7] 15 U.S.C. §6501 et seq., (regulates online collection of personal information of children under 13 by website operators – details what website operators must include in privacy policies, how to seek consent from parent or guardian, restrictions on marketing to children)
[8] 42 U.S.C. §552 (requires cable companies to protect subscriber information)

C. **Whether Fanning Controlled Jerk, LLC is a Fact Question**

The concept of "control" over any entity or organization for the purpose of imposing Section 5 liability is essentially grounded in traditional notions of common law agency. Agency is a question of fact, and must be determined by the finder of fact upon weighing all facts and circumstances concerning the scope of the agency relationship with the principal. See White's Farm Dairy, Inc. v. DeLaval Separator Company, 433 F.2d 63, 66-67 (1st Cir. 1970) (citations omitted) (proof of agency is ordinarily a question of fact for the jury). Here, there exists a healthy dispute as to the scope of Fanning's authority as an agent of NetCapital.com, LLC through which Fanning served as an advisor to Jerk, LLC, and any concomitant control over Jerk, LLC within the agency relationship. Fanning, individually, did not have express authority to control Jerk, LLC or Jerk.com. Jerk, LLC was not a typical company with a specific corporate or ownership management structure with ongoing employee relationships and designated titles. Jerk, LLC was a fledgling internet technology company that changed as the business model and operations evolved. Fanning, at all times, acted within the corporate context and within the limited authority granted. Fanning, individually, took no action with respect to Jerk, LLC.

Complaint Counsel's leap that Fanning is personally and individually liable for the actions and conduct of Jerk, LLC eviscerates all notions of corporate existence. NetCapital.com. LLC, as a firm, provided guidance and assistance to Jerk, LLC, as a technology start-up. Exposing Fanning to personal liability for actions taken on behalf NetCapital.com, LLC with respect to Jerk, LLC unlawfully ignores the corporate structure. Complaint Counsel provides no evidence to substantiate or support such a corporate veil-piercing theory of liability. Imposing liability on individuals acting within a corporate capacity for the acts of the principal company violates notions of agency and corporate existence. If the theory of personal liability fashioned

by Complaint Counsel is permitted to stand, each and every enforcement action by the FTC against a company necessarily will trigger individual liability, because companies can only act through individuals. Further, every officer or employee of any private equity or venture capital firm that invests in a technology start-up would suffer possible individual liability merely because the firm manages a portfolio company that ends up in the cross-hairs of an FTC investigation. Complaint Counsel's argument turns otherwise exceptional, limited circumstances of individual liability into the rule governing all FTC enforcement actions. Such a broad standard would stymie investment and have a huge negative impact on the economy. This is bad public policy, and cannot possibly be consistent with the expectations of Congress when it granted the FTC its regulatory mandate.

Moreover, the true focus of this case is control over website content and statements made on Jerk.com, and not control over Jerk, LLC as an entity. Specifically, a valid dispute exists as to whether the content about consumers that existed on the Jerk.com site rested within Fanning's purview as an advisor to Jerk, LLC through NetCapital.com, LLC. Fanning did not write any software code for Jerk, LLC to operate Jerk.com, and did not place any consumer content on Jerk.com. Fanning was not a software developer or web developer for Jerk, LLC. Fanning had no authority over or advisory agreement with the primary developers of the Jerk, LLC software. Jerk.com essentially was operated and controlled by Louis Lardass of Internet Domains, which owned the Jerk.com domain, and foreign software developers who were reportedly supported by various interns, college students, and other independent contractors working for their own benefit. Complaint Counsel does not establish that Fanning, or even Jerk, LLC, was responsible for or controlled any of the statements on the site. Rather, Complaint Counsel draws the illogical inference that Fanning controlled Jerk, LLC and therefore Fanning must have controlled content.

Nothing in the law, however, permits Complaint Counsel merely to impute the content of the Jerk.com site to Fanning. Complaint Counsel also ignores Fanning is entitled to the benefit of all inferences for the purposes of summary decision. Even if Fanning was involved at the level Complaint Counsel postures, the legal test is not facilitation or encouragement, but rather a more stringent standard requiring a conclusive showing that Fanning "participated directly in the practices or acts or had authority to control them." FTC v. Amy Travel Serv., Inc., 875 F.2d 564, 573 (7th Cir. 1989). Complaint Counsel fails to meet this high standard.

Directly to the point, Complaint Counsel presents no admissible evidence that Fanning, individually, directed or controlled the Romanian developers whom Complaint Counsel contends were managing the content and other technical aspects of the project. Complaint Counsel cites to testimony from a former intern that completely undercuts the theory of Fanning's ultimate control, as follows: "A third idea championed, by software engineers from a Romanian firm called Software Assist, was that we generate profiles on Jerk.com by bulk-loading user information from Facebook." (CX0057-002). Complaint Counsel merely piles inference upon inference to reach the conclusion that Fanning must be responsible. Such bare assertions fail in the face of contradictory evidence, including presented through Complaint Counsel's own witnesses. Much of the so-called evidence relied upon by Complaint Counsel is actually rank speculation, belief, and multi-level hearsay all of which is not admissible evidence. A live issue exists about the scope of Fanning's agency and control, which must be decided by the finder of fact on a full record after weighing credibility. Summary decision is not appropriate as a matter of law on the issue of Fanning's personal liability. See Ross,, at * 4 ("Notwithstanding the fact that the FTC's evidence is substantial, at this stage of the litigation, this Court is unable to conclusively determine whether the FTC is entitled to summary judgment against Kristy Ross

because to do so would require this Court to make credibility findings, inferences, and findings of fact that are more properly made in the context of a bench trial.").[9]

D. The Relief Sought by Complaint Counsel is Unlawful

Even if summary disposition in violation of Fanning's due process rights is granted, the broad relief requested by Complaint Counsel in the Proposed Order far exceeds proper regulatory authority and cannot enter. It is nearly impossible even to comment upon and address the legal merits of the requested relief where it is so broad and expansive and relies upon the unspecified nature of the claims asserted. This is not a situation where an order restricting or deterring certain future claims about a product or service is even possible where there is no specific advertisement or mode of presenting a claim present. Moreover, the request seeks remedies unrelated to any alleged conduct. For instance, Complaint Counsel requests an order pertaining to misrepresentation of privacy protections despite no mention or reference to such allegations in the Complaint. While injunctive relief entered under the FTC Act may be broad, it must bear a reasonable relation to the unlawful practices found to have occurred. Litton Industries, Inc. v. FTC, 676 F.2d 364, 370 (9th Cir. 1982), citing FTC v. Colgate-Palmolive Co., 380 U.S. 374, 394-95 (1965).

Complaint Counsel's knee-jerk pro forma request to restrain for twenty (20) or even ten (10) years Fanning's involvement with respect to each and every actual or potential business venture involving the internet, public information, or personal data without exception or any degree of specificity fails to consider the seriousness and deliberateness of the violation, the ease

[9] Complaint Counsel has made much of the fact that "Respondents" allegedly flouted the Civil Investigative Demand process and failed to answer discovery in the litigation, again seeking to prevail based on the drawing of adverse inferences. Putting aside Complaint Counsel's mischaracterizations, "Respondents'" conduct throughout the course of the proceedings does not permit the granting of summary judgment. See Ross, at * 6 (refusing to grant summary judgment based on an adverse inference where respondent asserted Fifth Amendment privilege and failed to provide any meaningful discovery).

in which the violative claim may be transferred to other products, and whether Fanning has any history of prior violations as mandated to support such sweeping relief. See FTC v. John Beck Amazing Profits, 888 F.Supp.2d 1006, 1012 (C.D. Cal. 2012) (citations omitted). The Proposed Order lacks specificity, and is unlawful. Colgate-Palmolive Co., 380 U.S. at 393 (FTC orders should be "as specific as the circumstances will permit"); FTC v. Henry Broch & Co., 368 U.S. 360, 367-68 (1962) (FTC orders must be sufficiently precise to "avoid raising serious questions as to their meaning and application"). Even so-called "fencing in" provisions must bear a "reasonable relation to the unlawful practices found to exist." Colgate-Palmolive Co., 380 U.S. at 394-95 (footnote omitted). See also Standard Oil of California v. FTC, 577 F.2d 653, 663 (9th Cir. 1978) (court rejected order that applied to all of respondent's products, not just those involved in the violation, absent circumstances justifying broad coverage, such as a long history of violations).

The most chilling aspect of the Proposed Order is the prior restraint over free speech, including restriction on use and dissemination of information gathered from public sources. Imposing any restrictions on the use and publication of any information, whether in a commercial setting or otherwise, is an extreme abrogation of Fanning's First Amendment rights and privileges. Complaint Counsel intends to restrain in advance all future speech, no matter the content or purpose. Complaint Counsel impermissibly ignores that only commercial speech that is "actually misleading" may be prohibited in its entirety. In re R.M.J., 455 U.S. 191, 203 (1982). Government is barred from placing an absolute prohibition on potentially misleading information. Wine & Spirits Retailers, Inc. v. Rhode Island, 481 F.3d 1, 8-9 (1st Cir. 2007) (citations omitted). Taken literally, the injunction sought against Fanning would bar him from commenting on or utilizing any information that exists or potentially exists in the public domain,

and effectively prohibits or regulates Fanning from engaging in any business that involves social media or the internet. Complaint Counsel's proposed order, as drafted, would even unlawfully regulate or prohibit Fanning from making or publishing statements that are true. See Cotherman v. FTC, 417 F.2d 587, 595-596 (5th Cir. 1969). Complaint Counsel is barred from repressing speech and expression by Fanning, and the relief requested must be rejected in its entirety. See Beneficial Corp. v. FTC, 542 F.2d 611, 619-620 (3rd Cir. 1976), cert. denied, 430 U.S. 983 (1977) ("The Commission, like any governmental agency, must start from the premise that any prior restraint is suspect, and that a remedy, even for deceptive advertising, can go no further than is necessary for the elimination of the deception.").

At a minimum, relief should not be adjudicated in summary fashion on this record. Complaint Counsel must be required to justify the broad relief requested with specificity, instead of through sweeping statements and citations to "fencing in" cases that have no legitimate application to this instant action. Numerous fact issues remain unresolved. Fanning must have a right to address and defend against any affirmative proposed order in the spirit of due process, with actual notice and an opportunity to be heard. See FTC v. Direct Marketing Concepts, Inc., 569 F.Supp.2d 285, 307 (D.Mass. 2008).

IV. CONCLUSION

For the foregoing reasons, Respondent John Fanning requests the Commission to deny Complaint Counsel's request for summary decision, in its entirety.

Respectfully submitted,

JOHN FANNING,

By his attorneys,

/s/ Peter F. Carr, II
Peter F. Carr, II
ECKERT, SEAMANS, CHERIN & MELLOTT, LLC
Two International Place, 16th Floor
Boston, MA 02110
617.342.6800
617.342.6899 (FAX)
Email: pcarr@eckertseamans.com

PUBLIC DOCUMENT

CERTIFICATE OF SERVICE

I hereby certify that on November 4, 2014, I caused a true and accurate copy of the documents entitled *Opposition of Respondent John Fanning to Complaint Counsel's Motion for Summary Decision, Memorandum of Respondent John Fanning in Opposition to Complaint Counsel's Motion for Summary Decision, Affidavit of John Fanning* and *Affidavit of Peter F. Carr, II in Support of Opposition of Respondent John Fanning to Complaint Counsel's Motion for Summary Judgment*, and accompanying exhibits, to be served electronically through the FTC's e-filing system and I caused a true and accurate copy of the foregoing to be served as follows:

One electronic copy to the Office of the Secretary:

Donald S. Clark, Secretary
Federal Trade Commission
600 Pennsylvania Ave., N.W., Room H-159
Washington, DC 20580
Email: secretary@ftc.gov

One electronic copy to the Office of the Administrative Law Judge:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Avenue, N.E., Room H-110
Washington, DC 20580
Email: oalj@ftc.gov

One electronic copy to the Office of the Counsel for the Federal Trade Commission:

Sarah Schroeder
Federal Trade Commission
901 Market Street, Suite 670
San Francisco, CA 94103
Email: sschroeder@ftc.gov

/s/ Peter F. Carr, II
Peter F. Carr, II
ECKERT, SEAMANS, CHERIN & MELLOTT, LLC
Two International Place, 16th Floor
Boston, MA 02110
617.342.6800
617.342.6899 (FAX)

AFFIDAVIT OF JOHN FANNING

I, John Fanning, upon my own personal knowledge, under oath hereby depose and state as follows:

1. Jerk. LLC launched Jerk.com in approximately 2009 as an alternate social media and reputational website. The primary mission of Jerk, LLC was to educate, to provide a platform for public dialogue and discussion, and eventually to comment on and to expose Facebook's lack of privacy.

2. I formerly served as an advisor to Jerk, LLC through another company called NetCapital.com, LLC, and not in my individual capacity. NetCapital.com. LLC is a private equity/venture capital firm, with a number of partners, that invests in and provides advisory services to a wide-range of technology start-ups including those in its portfolio of companies. My authority was limited, and at all times I acted on behalf of NetCapitlal.com, LLC with respect to Jerk, LLC. I never acted in my individual capacity.

3. Jerk, LLC, as an internet technology start-up, was not a large company with levels of management and regular employees. Jerk.com essentially was operated and controlled by Louis Lardass of Internet Domains, which owned the Jerk.com domain, and foreign software developers who were reportedly supported by various interns, college students, and other independent contractors working for their own benefit. I was not responsible for spearheading and operating Jerk, LLC or Jerk.com. Through and on behalf of NetCapital.com. LLC, I was part of a group involved in efforts to launch, finance, and expand the Jerk brand through the Jerk.com website. I did not write any software code for Jerk, LLC to operate Jerk.com, and did not place any consumer content on Jerk.com. I was not a software developer or web developer

for Jerk, LLC. I had no authority over or advisory agreement with the primary developers of the Jerk, LLC software.

4. Jerk, LLC established an agent, a lawyer in Phoenix, Arizona, to accept service of complaints about Jerk.com while Jerk, LLC held a paid option to purchase the domain name. As far as I am aware, Jerk, LLC took action including to remove content from Jerk.com whenever it was obligated to do so. As far as I am aware, Jerk, LLC would refund money to users who claimed they had paid but had not received membership services via a web form. Jerk, LLC experienced a number of problems in operating the site, including the site being hacked and being "snaked" by the FTC which disrupted the services. The FTC also made demands on Jerk, LLC to take corrective action. I understand that Jerk, LLC complied with the FTC's demands, although the company denied any liability.

5. Facebook complained that Jerk, LLC was violating its policies and procedures concerning use. Jerk, LLC rejected the allegations. As far as I am aware, Jerk, LLC never violated any valid contract or agreement with Facebook with respect to Jerk.com. Any information posted on Jerk.com that Facebook claimed was a violation came from users or derived from public sources. The entire Facebook directory containing user information and photographs was readily available to the public through the internet without ever having to agree to the Facebook terms of service, and any user of Jerk.com, or independent third party, could have accessed the directory and posted the information on Jerk.com. Even today, the images and names of Facebook users are freely available to anyone without requiring any agreement with Facebook or its terms of service simply by going to www.facebook.com/directory. I never hacked into Facebook, and I never directed anyone affiliated with Jerk, LLC to hack into Facebook with respect to Jerk.com.

6. The FTC was upset when I refused to be interviewed as part of its investigation prior to the filing of the Complaint. It is my opinion that the FTC's actions and investigations are intended to harass, and are a blatant attempt to chill free speech because the nature of that speech makes the FTC uncomfortable. The Government only began to take issue with the content published on Jerk.com after the President appeared on the front page during the last election cycle.

7. As far as I am aware, Jerk, LLC, while it owned an option to buy the Jerk.com domain, never made any false or deceptive claims to consumers or users about the Jerk.com website, content, or users. I know that I did not.

SWORN TO AND SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 4th DAY OF NOVEMBER, 2014.

/s/ John Fanning
John Fanning

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

In the matter of:	)	
Jerk, LLC, a limited liability company,	)	DOCKET NO. 9361
Also d/b/a JERK.COM, and	)	
John Fanning, Individually and as a member of Jerk, LLC,	)	PUBLIC
Respondents.	)	

AFFIDAVIT OF PETER F. CARR, II
IN SUPPORT OF OPPOSITION OF RESPONDENT JOHN FANNING TO COMPLAINT COUNSEL'S MOTION FOR SUMMARY DECISION

I, Peter F. Carr, II, Esquire, upon my own personal knowledge, under oath hereby depose and state as follows:

1. I currently serve as counsel to Respondent John Fanning in the above-captioned matter. I make this affidavit solely in support of Mr. Fanning's Opposition to Complaint Counsel's Motion for Summary Decision.

2. Attached hereto at **Tab A** is a true and accurate copy of the Complaint, Request for Investigation, Injunction, and Other Relief filed with the Federal Trade Commission by Electronic Privacy Information Center dated December 17, 2009.

3. Attached hereto at **Tab B** is a true and accurate copy of the Complaint filed by the Federal Trade Commission in the action In the Matter of Facebook, Inc., File No. 092-3184, Docket No. C-4365.

4. Attached hereto at **Tab C** is a true and accurate copy of the Decision and Order entered on July 27, 2012 filed in the action In the Matter of Facebook, Inc.

5. Attached hereto at **Tab D** is a true and accurate copy of the decision in the case Federal Trade Commission v. Ross, 2012 WL 2126533 (D.Maryland 2012).

6. Attached hereto at **Tab E** is a true and accurate copy of the Statement of Commissioners Orson Swindle and Thomas B. Leary Concurring in Part and Dissenting in Part, In the Matter of ReverseAuction.com, Inc., File No. 0023046.

SWORN TO AND SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 5th OF NOVEMBER, 2014.

/s/ Peter F. Carr, II
Peter F. Carr, II, Esquire

TAB A

Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Facebook, Inc.	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

I. Introduction

1. This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.

2. These business practices impact more than 100 million users of the social networking site who fall within the jurisdiction of the United States Federal Trade Commission.[1]

3. EPIC urges the Commission to investigate Facebook, determine the extent of the harm to consumer privacy and safety, require Facebook to restore privacy settings that were previously available as detailed below, require Facebook to give users meaningful control over personal information, and seek appropriate injunctive and compensatory relief.

[1] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009); *see also* Eric Eldon, *Facebook Reaches 100 Million Monthly Active Users in the United States*, InsideFacebook.com, Dec. 7, 2009, http://www.insidefacebook.com/2009/12/07/facebook-reaches-100-million-monthly-active-users-in-the-united-states (last visited Dec. 15, 2009).

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. Among its other activities, EPIC first brought the Commission's attention to the privacy risks of online advertising.[2] In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, calling the Commission's attention to "data products circumvent[ing] the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices."[3] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million.[4] EPIC initiated the complaint to the FTC regarding Microsoft Passport.[5] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[6] EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,[7] which resulted in the issuance of a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology sold for individuals to spy on other individuals.[8]

---

[2] *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), *available at* http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[3] *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[4] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress, http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited Dec. 13, 2009).

[5] *In the Matter of Microsoft Corporation*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), *available at* http://epic.org/privacy/consumer/MS_complaint.pdf.

[6] *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm. *See also* Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microst.shtm.

[7] *In the Matter of Awarenesstech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, *available at* http://epic.org/privacy/dv/spy_software.pdf.

[8] FTC v. Cyberspy Software, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), *available at* http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf.

5. Earlier this year, EPIC urged the FTC to undertake an investigation of Google and cloud computing.[9] The FTC agreed to review the complaint, stating that it "raises a number of concerns about the privacy and security of information collected from consumers online."[10] More recently, EPIC asked the FTC to investigate the "parental control" software firm Echometrix.[11] Thus far, the FTC has failed to announce any action in this matter, but once the Department of Defense became aware of the privacy and security risks to military families, it removed Echometrix's software from the Army and Air Force Exchange Service, the online shopping portal for military families.[12]

6. The American Library Association is the oldest and largest library association in the world, with more than 64,000 members. Its mission is "to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all."

7. The Center for Digital Democracy ("CDD") is one of the leading non-profit groups analyzing and addressing the impact of digital marketing on privacy and consumer welfare. Based in Washington, D.C., CDD has played a key role promoting policy safeguards for interactive marketing and data collection, including at the FTC and Congress.

8. Consumer Federation of America ("CFA") is an association of some 300 nonprofit consumer organizations across the U.S. CFA was created in 1968 to advance the consumer interest through research, advocacy, and education.

9. Patient Privacy Rights is a non-profit organization located in Austin, Texas. Founded in 2004 by Dr. Deborah Peel, Patient Privacy Rights is dedicated to ensuring Americans control all access to their health records.

10. Privacy Activism is a nonprofit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal

---

[9] *In the Matter of Google, Inc., and Cloud Computing Services*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[10] Letter from Eileen Harrington, Acting Director of the FTC Bureau of Consumer Protection, to EPIC (Mar. 18, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

[11] *In the Matter of Echometrix, Inc.*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Sep. 25, 2009), *available at* http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.

[12] EPIC, *Excerpts from Echometrix Documents*, http://epic.org/privacy/echometrix/Excerpts_from_echometrix_docs_12-1-09.pdf (last visited Dec. 13, 2009).

level. A key goal of the organization is to inform the public about the importance of privacy rights and the short- and long-term consequences of losing them, either inadvertently, or by explicitly trading them away for perceived or ill-understood notions of security and convenience.

11. The Privacy Rights Clearinghouse ("PRC") is a nonprofit consumer organization with a two-part mission—consumer information and consumer advocacy. It was established in 1992 and is based in San Diego, CA. Among its several goals, PRC works to raise consumers' awareness of how technology affects personal privacy and to empower consumers to take action to control their own personal information by providing practical tips on privacy protection.

12. The U. S. Bill of Rights Foundation is a non-partisan public interest law policy development and advocacy organization seeking remedies at law and public policy improvements on targeted issues that contravene the Bill of Rights and related Constitutional law. The Foundation implements strategies to combat violations of individual rights and civil liberties through Congressional and legal liaisons, coalition building, message development, project planning & preparation, tactical integration with supporting entities, and the filings of complaints and of *amicus curiae* briefs in litigated matters.

13. Facebook Inc. was founded in 2004 and is based in Palo Alto, California. Facebook's headquarters are located at 156 University Avenue, Suite 300, Palo Alto, CA 94301. At all times material to this complaint, Facebook's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

III. The Importance of Privacy Protection

14. The right of privacy is a personal and fundamental right in the United States.[13] The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.[14]

---

[13] *See Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person"); *Whalen v. Roe*, 429 U.S. 589, 605 (1977); *United States v. Katz*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[14] Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* 11 (2009) (charts describing how identity theft victims' information have been misused).

15. The excessive collection of personal data in the United States coupled with inadequate legal and technological protections have led to a dramatic increase in the crime of identity theft.[15]

16. The federal government has established policies for privacy and data collection on federal web sites that acknowledge particular privacy concerns "when uses of web technology can track the activities of users over time and across different web sites" and has discouraged the use of such techniques by federal agencies.[16]

17. As the Supreme Court has made clear, and the Court of Appeals for the District of Columbia Circuit has recently held, "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."[17]

18. The Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard."

19. The appropriation tort recognizes the right of each person to protect the commercial value of that person's name and likeness. The tort is recognized in virtually every state in the United States.

20. The Madrid Privacy Declaration of November 2009 affirms that privacy is a basic human right, notes that "corporations are acquiring vast amounts of personal data without independent oversight," and highlights the critical role played by "Fair Information Practices that place obligations on those who collect and process personal information and gives rights to those whose personal information is collected."[18]

21. The Federal Trade Commission is "empowered and directed" to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where the privacy interests of Internet users are at issue.[19]

---

[15] *Id.* at 5 (from 2000-2009, the number of identity theft complaints received increased from 31,140 to 313,982); *see* U.S. Gen. Accounting Office, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009); Fed. Trade Comm'n, *Security in Numbers: SSNs and ID Theft* 2 (2008).

[16] Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies* (2000), *available at* http://www.whitehouse.gov/omb/memoranda_m00-13 (last visited Dec. 17, 2009).

[17] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n*, No. 07-1312 (D.C. Cir. Feb. 13, 2009).

[18] The Madrid Privacy Declaration: Global Privacy Standards for a Global World, Nov. 3, 2009, *available at* http://thepublicvoice.org/madrid-declaration/.

[19] 15 U.S.C. § 45 (2006).

IV. Factual Background

Facebook's Size and Reach Is Unparalleled Among Social Networking Sites

22. Facebook is the largest social network service provider in the United States. According to Facebook, there are more than 350 million active users, with more than 100 million in the United States. More than 35 million users update their statuses at least once each day.[20]

23. More than 2.5 billion photos are uploaded to the site each month.[21] Facebook is the largest photo-sharing site on the internet, by a wide margin.[22]

24. As of August 2009, Facebook is the fourth most-visited web site in the world, and the sixth most-visited web site in the United States.[23]

Facebook Has Previously Changed Its Service in Ways that Harm Users' Privacy

25. In September 2006, Facebook disclosed users' personal information, including details relating to their marital and dating status, without their knowledge or consent through its "News Feed" program.[24] Hundreds of thousands of users objected to Facebook's actions.[25] In response, Facebook stated:

> We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead, we did a bad job of explaining what the new features were and an even worse job of giving you control of them.[26]

26. In 2007, Facebook disclosed users' personal information, including their online purchases and video rentals, without their knowledge or consent through its "Beacon" program.[27]

27. Facebook is a defendant in multiple federal lawsuits[28] arising from the "Beacon" program.[29] In the lawsuits, users allege violations of federal and state law, including the

---

[20] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009).

[21] *Id.*

[22] Erick Schonfeld, *Facebook Photos Pulls Away From the Pack*, TechCrunch (Feb. 22, 2009), http://www.techcrunch.com/2009/02/22/facebook-photos-pulls-away-from-the-pack/.

[23] Erick Schonfeld, *Facebook is Now the Fourth Largest Site in the World*, TechCrunch (Aug. 4, 2009), http://www.techcrunch.com/2009/08/04/facebook-is-now-the-fourth-largest-site-in-the-world/.

[24] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).

[25] Justin Smith, *Scared students protest Facebook's social dashboard, grappling with rules of attention economy*, Inside Facebook (Sept. 6, 2006), http://www.insidefacebook.com/2006/09/06/scared-students-protest-facebooks-social-dashboard-grappling-with-rules-of-attention-economy/.

[26] Mark Zuckerberg, *An Open Letter from Mark Zuckerberg* (Sept. 8, 2006), http://blog.facebook.com/blog.php?post=2208562130.

[27] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).

Video Privacy Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Computer Crime Law.[30]

28. On May 30, 2008, the Canadian Internet Policy and Public Interest Clinic filed a complaint with Privacy Commissioner of Canada concerning the "unnecessary and non-consensual collection and use of personal information by Facebook."[31]

29. On July 16, 2009, the Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[32]

30. The Privacy Commissioner's Office found:

> Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers.[33]

31. On February 4, 2009, Facebook revised its Terms of Service, asserting broad, permanent, and retroactive rights to users' personal information—even after they deleted their accounts.[34] Facebook stated that it could make public a user's "name, likeness and image for any purpose, including commercial or advertising."[35]

32. Users objected to Facebook's actions, and Facebook reversed the revisions on the eve of an EPIC complaint to the Commission.[36]

---

[28] In *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008), Facebook has requested court approval of a class action settlement that would terminate users' claims, but provide no monetary compensation to users. The court has not ruled on the matter.

[29] *See e.g.*, *Harris v. Facebook, Inc.*, No. 09-01912 (N.D. Tex. filed Oct. 9, 2009); *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008); *see also Harris v. Blockbuster*, No. 09-217 (N.D. Tex. filed Feb. 3, 2009), *appeal docketed*, No. 09-10420 (5th Cir. Apr. 29, 2009).

[30] *Id.*

[31] Letter from Philippa Lawson, Director, Canadian Internet Policy and Public Interest Clinic to Jennifer Stoddart, Privacy Commissioner of Canada (May 30, 2008), *available at* http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.

[32] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, July 16, 2009, *available at* http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

[33] *Id.* at 3.

[34] Chris Walters, *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."* The Consumerist, Feb. 15, 2009, *available at* http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html#reset.

[35] *Id.*

[36] JR Raphael, *Facebook's Privacy Flap: What Really Went Down, and What's Next*, PC World, Feb. 18, 2009, http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html.

Changes in Privacy Settings: "Publicly Available Information"

33. Facebook updated its privacy policy and changed the privacy settings available to users on November 19, 2009 and again on December 9, 2009.[37]

34. Facebook now treats the following categories of personal data as "publicly available information:"

    - users' names,
    - profile photos,
    - lists of friends,
    - pages they are fans of,
    - gender,
    - geographic regions, and
    - networks to which they belong.[38]

35. By default, Facebook discloses "publicly available information" to search engines, to Internet users whether or not they use Facebook, and others. According to Facebook, such information can be accessed by "every application and website, including those you have not connected with . . . ."[39]

36. Prior to these changes, only the following items were mandatorily "publicly available information:"

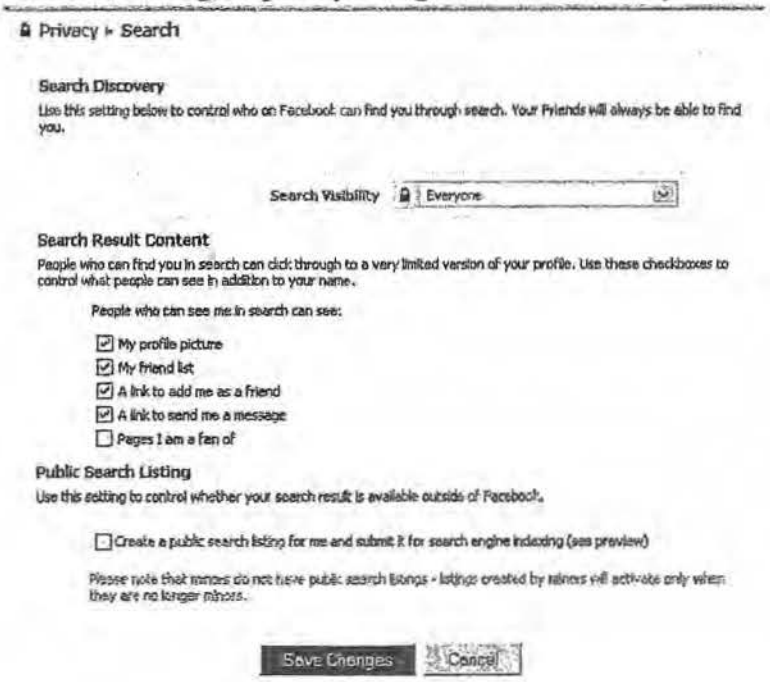
    - a user's name and
    - a user's network.

[37] Facebook, *Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy* (Dec. 9, 2009), *available at* http://www.facebook.com/press/releases.php?p=133917.

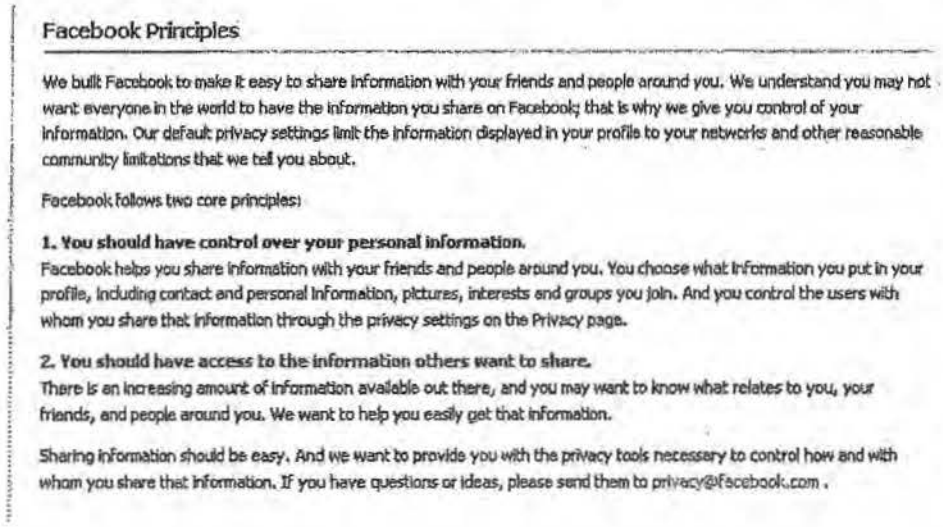
[38] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).

[39] *Id.*

37. Users also had the option to include additional information in their public search listing. as the screenshot of the original privacy settings for search discovery demonstrates.



38. Facebook's original privacy policy stated that users "may not want everyone in the world to have the information you share on Facebook" as the screenshot below makes clear:



Facebook Principles

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

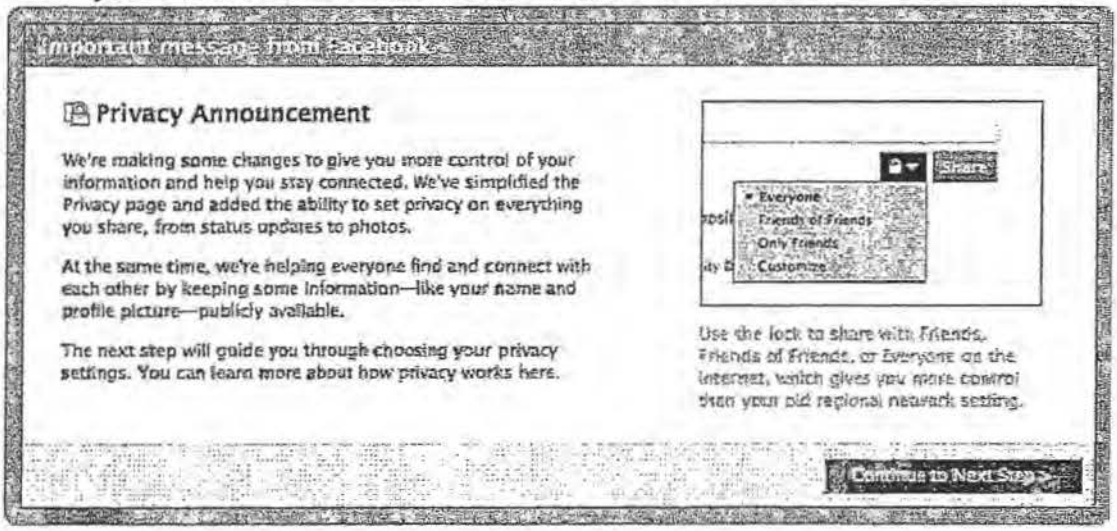
1. You should have control over your personal information.
Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

2. You should have access to the information others want to share.
There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com .

39. Facebook's Chief Privacy Officer, Chris Kelly, testified before Congress that Facebook gives "users controls over how they share their personal information that model real-world information sharing and provide them transparency about how we use their information in advertising."[40] Kelly further testified, "many of our users choose to limit what profile information is available to non-friends. Users have extensive and precise controls available to choose who sees what among their networks and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities."[41]

40. In an "Important message from Facebook," Facebook told users it was giving "you more control of your information . . . and [had] added the ability to set privacy on everything you share . . ." as the screen from the transition tool illustrates:



41. Facebook's CEO, Mark Zuckerberg, reversed changes to his personal Facebook privacy settings after the transition from the original privacy settings to the revised settings made public his photographs and other information.[42]

42. Barry Schnitt, Facebook's Director of Corporate Communications and Public Policy, "suggests that users are free to lie about their hometown or take down their profile picture to protect their privacy."[43]

---

[40] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.

[41] *Id.*

[42] Kashmir Hill, *Either Mark Zuckerberg got a whole lot less private or Facebook's CEO doesn't understand the company's new privacy settings* (Dec. 10, 2009), http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings/.

43. Providing false information on a Facebook profile violates Facebook's Terms of Service.[44]

44. Facebook user profile information may include sensitive personal information.

45. Facebook users can indicate that they are "fans" of various organizations, individuals, and products, including controversial political causes.[45]

46. Under the original privacy settings, users controlled public access to the causes they supported. Under the revised settings, Facebook has made users' causes "publicly available information," disclosing this data to others and preventing users from exercising control as they had under the original privacy policy.

47. Based on profile data obtained from Facebook users' friends lists, MIT researchers found that "just by looking at a person's online friends, they could predict whether the person was gay."[46] Under Facebook's original privacy policy, Facebook did not categorize users' friends lists as "publicly available information." Facebook now makes users' friends lists "publicly available information."

48. Dozens of American Facebook users, who posted political messages critical of Iran, have reported that Iranian authorities subsequently questioned and detained their relatives.[47] Under the revised privacy settings, Facebook makes such users' friends lists publicly available.

---

[43] Julia Angwin, *How Facebook Is Making Friending Obsolete*, Wall St. J., Dec. 15, 2009, *available at* http://online.wsj.com/article/SB126084637203791583.html.

[44] Facebook, Statement of Rights and Responsibilities, http://www.facebook.com/terms.php (last visited Dec. 16, 2009); *see* Jason Kincaid, *Facebook Suggests You Lie, Break Its Own Terms Of Service To Keep Your Privacy*, Washington Post, Dec. 16, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/15/AR2009121505270.html.

[45] *See, e.g.,* Facebook, *Prop 8*, http://www.facebook.com/pages/Prop-8/86610985605 (last visited Dec. 15, 2009); Facebook, *No on Prop 8 Don't Eliminate Marriage for Anyone*, http://www.facebook.com/#/pages/No-on-Prop-8-Dont-Eliminate-Marriage-for-Anyone/29097894014 (last visited Dec. 15, 2009); *see also Court Tosses Prop. 8 Ruling on Strategy Papers*, San Francisco Chron. (Dec. 12, 2009), *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/12/11/BA3A1B34VC.DTL.

[46] *See* Carolyn Y. Johnson, *Project "Gaydar,"* Sep. 20, 2009, Boston Globe, *available at* http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=full

[47] Farnaz Fassihi, *Iranian Crackdown Goes Global*, Wall Street Journal (Dec. 4, 2009), *available at* http://online.wsj.com/article/SB125978649644673331.html.

49. According to the Wall Street Journal, one Iranian-American graduate student received a threatening email that read, "we know your home address in Los Angeles," and directed the user to "stop spreading lies about Iran on Facebook."[48]

50. Another U.S. Facebook user who criticized Iran on Facebook stated that security agents in Tehran located and arrested his father as a result of the postings.[49]

51. One Facebook user who traveled to Iran said that security officials asked him whether he owned a Facebook account, and to verify his answer, they performed a Google search for his name, which revealed his Facebook page. His passport was subsequently confiscated for one month, pending interrogation.[50]

52. Many Iranian Facebook users, out of fear for the safety of their family and friends, changed their last name to "Irani" on their pages so government officials would have a more difficult time targeting them and their loved ones.[51]

53. By implementing the revised privacy settings, Facebook discloses users' sensitive friends lists to the public and exposes users to the analysis employed by Iranian officials against political opponents.

Changes to Privacy Settings: Information Disclosure to Application Developers

54. The Facebook Platform transfers Facebook users' personal data to application developers without users' knowledge or consent.[52]

55. Facebook permits third-party applications to access user information at the moment a user visits an application website. According to Facebook, third party applications receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them."[53]

56. As Facebook itself explains in its documentation, when a user adds an application, by default that application then gains access to everything on Facebook that the user can

---

[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *See* Facebook, *Facebook Platform*, http://www.facebook.com/facebook#/platform?v=info (last visited Dec. 13, 2009).
[53] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).

see.[54] The primary "privacy setting" that Facebook demonstrates to third-party developers governs what other users can see from the application's output, rather than what data may be accessed by the application.[55]

57. According to Facebook:

> Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall, a list of user IDs mapped to your friends, your social timeline, notifications that you have received from other applications, and events associated with your profile.[56]

58. To access this information, developers use the Facebook Application Programming Interface ("API"), to "utiliz[e] profile, friend, Page, group, photo, and event data."[57] The API is a collection of commands that an application can run on Facebook, including authorization commands, data retrieval commands, and data publishing commands.[58]

---

[54] Facebook, *About Platform*, http://developers.facebook.com/about_platform.php (last visited Dec. 16, 2009).

[55] Facebook Developer Wiki, *Anatomy of a Facebook App*, http://wiki.developers.facebook.com/index.php/Anatomy_of_a_Facebook_App#Privacy_Settings (last visited Dec. 16, 2009).

[56] Facebook, *About Platform*, http://developers.facebook.com/about_platform.php (last visited Dec. 16, 2009).

[57] Facebook Developer Wiki, *API*, http://wiki.developers.facebook.com/index.php/API (last visited Dec. 16, 2009).

[58] *Id.*

59. Third-parties who develop Facebook applications may also transmit the user information they access to their own servers, and are asked only to retain the information for less than 24 hours.[59]

60. A 2007 University of Virginia study of Facebook applications found that "90.7% of applications are being given more privileges than they need."[60]

61. According to the Washington Post, many Facebook developers who have gained access to information this way have considered the "value" of having the data, even when the data is not relevant to the purpose for which the user has added the application.[61]

62. Under the revised privacy policy, Facebook now categorizes users' names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong as "publicly available information," and Facebooks sets the "default privacy setting for certain types of information [users] post on Facebook . . . to 'everyone.'"[62]

63. Facebook allows user information that is categorized as publicly available to "everyone" to be: "accessed by everyone on the Internet (including people not logged into Facebook);" made subject to "indexing by third party search engines;" "associated with you outside of Facebook (such as when you visit other sites on the internet);" and "imported and exported by us and others *without* privacy limitations."[63]

64. With the Preferred Developer Program, Facebook will give third-party developers access to a user's primary email address, personal information provided by the user to Facebook to subscribe to the Facebook service, but not necessarily available to the public or to developers.[64] In fact, some users may choose to create a Facebook account precisely to prevent the disclosure of their primary email address.

---

[59] Facebook Developer Wiki, *Policy Examples and Explanations/Data and Privacy*, http://wiki.developers.facebook.com/index.php/Policy_Examples_and_Explanations/Data_and_Privacy (last visited Dec. 16, 2009).

[60] Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs*, http://www.cs.virginia.edu/felt/privacy/ (last visited Dec. 16, 2009).

[61] Kim Hart, *A Flashy Facebook Page, at a Cost to Privacy*, Wash. Post, June 12, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html

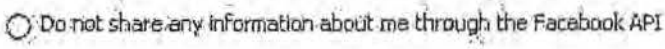
[62] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).

[63] *Id.* (emphasis added)

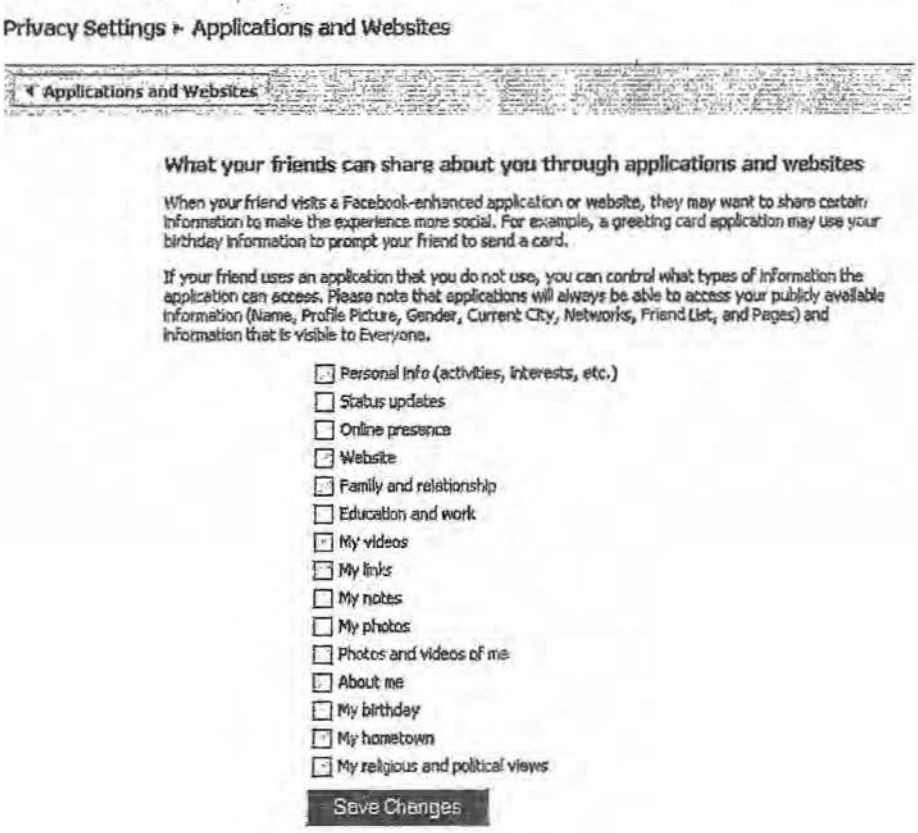
[64] Facebook, *Developer Roadmap*, http://wiki.developers.facebook.com/index.php/Developer_Roadmap (last visited Dec. 17 2009); Facebook, *Roadmap Email*, http://wiki.developers.facebook.com/index.php/Roadmap_Email (last visited Dec. 17, 2009); *see also* Mark Walsh, *Facebook Starts Preferred Developer Program* (Dec. 17, 2009), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=119293.

65. Facebook states in the revised privacy policy that users can "opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings."[65] Facebook further states that, "you can control how you share information with those third-party applications and websites through your application settings."[66]

66. In fact, under the original privacy settings, users had a one-click option to prevent the disclosure of personal information to third party application developers through the Facebook API, as the screenshot below indicates:



67. Under the revised privacy settings, Facebook has eliminated the universal one-click option and replaced it with the screen illustrated below:[67]



[65] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).

[66] *Id.*

[67] Facebook, *Privacy Settings*, http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share (last visited Dec. 13, 2009).

68. Under the revised settings, even when a user unchecks all boxes and indicates that none of the personal information listed above should be disclosed to third party application developers, Facebook states that "applications will *always* be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone."[68]

69. Facebook's "Everyone" setting overrides the user's choice to limit access by third-party applications and websites.

70. Facebook does not now provide the option that explicitly allows users to opt out of disclosing all information to third parties through the Facebook Platform.

71. Users can block individual third-party applications from obtaining personal information by searching the Application Directory, visiting the application's "about" page, clicking a small link on that page, and then confirming their decision.[69] A user would have to perform these steps for each of more than 350,000 applications in order to block all of them.[70]

Facebook Users Oppose the Changes to the Privacy Settings

72. Facebook users oppose these changes. In only four days, the number of Facebook groups related to privacy settings grew to more than five hundred.[71] Many security experts, bloggers, consumer groups, and news organizations have also opposed these changes.

73. More than 1,050 Facebook users are members of a group entitled "Against The New Facebook Privacy Settings!" The group has a simple request: "We demand that Facebook stop forcing people to reveal things they don't feel comfortable revealing."[72]

74. More than 950 Facebook users are members of a group entitled "Facebook! Fix the Privacy Settings," which exhorts users to "tell Facebook that our personal information is private, and we want to control it!"[73]

---

[68] *Id.* (emphasis added)

[69] Facebook, *General Application Support: Application Safety and Security*, http://www.facebook.com/help.php?page=967 (last visited Dec. 14, 2009).

[70] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009).

[71] Facebook, *Search "privacy settings,"* http://www.facebook.com/search/?o=69&init=s%3Agroup&q=privacy%20settings (last visited Dec. 15, 2009).

[72] Facebook, *Against The New Facebook Privacy Settings!*, http://www.facebook.com/group.php?gid=209833062912 (last visited Dec. 15, 2009).

75. More than 74,000 Facebook users are members of a group entitled "Petition: Facebook, stop invading my privacy!"[74] The group objects to the revisions and hopes to "get a message across to Facebook."[75] The group description explains, "[o]n December 9, 2009 Facebook once again breached our privacy by imposing new 'privacy settings' on 365+ million users. These settings notably give us LESS privacy than we had before, so I ask, how exactly do they make us more secure? . . . . Perhaps the most frustrating and troublesome part is the changes Facebook made on our behalf without truly making us aware or even asking us."[76]

76. A Facebook blog post discussing the changes to Facebook's privacy policy and settings drew 2,000 comments from users, most of them critical of the changes.[77] One commenter noted, "I came here to communicate with people with whom I have some direct personal connection; not to have my personal information provided to unscrupulous third party vendors and made available to potential stalkers and identity thieves."[78] Another commented, "I liked the old privacy settings better. I felt safer and felt like I had more control."[79]

77. The Electronic Frontier Foundation posted commentary online discussing the "good, the bad, and the ugly" aspects of Facebook's revised privacy policy and settings. More than 400 people have "tweeted" this article to encourage Facebook users to read EFF's analysis.[80]

78. The American Civil Liberties Union of Northern California's Demand Your dotRights campaign started a petition to Facebook demanding that Facebook (1) give full control of user information back to users; (2) give users strong default privacy settings; and (3) restrict the access of third party applications to user data.[81] The ACLU is "concerned that

---

[73] Facebook, *Facebook! Fix the Privacy Settings*, http://www.facebook.com/group.php?gid=192282128398 (last visited Dec. 15, 2009).

[74] Facebook, *Petition: Facebook, stop invading my privacy!*, http://www.facebook.com/group.php?gid=5930262681&ref=share (last visited Dec. 15, 2009).

[75] *Id.*

[76] *Id.*

[77] *See* The Facebook Blog, *Updates on Your New Privacy Tools*, http://blog.facebook.com/blog.php?post=197943902130 (last visited Dec. 14, 2009).

[78] *Id.*

[79] *Id.*

[80] *See* Twitter, *Twitter Search "eff.org Facebook,"* http://twitter.com/#search?q=eff.org%20facebook (last visited Dec. 14, 2009).

[81] American Civil Liberties Union, *Demand Your dotRights: Facebook Petition*, https://secure.aclu.org/site/SPageNavigator/CN_Facebook_Privacy_Petition (last visited Dec. 15, 2009).

the changes Facebook has made actually remove some privacy controls and encourage Facebook users to make other privacy protections disappear."[82]

79. In the past week, more than 3,000 blog posts have been written focusing on criticism of Facebook's privacy changes.[83]

80. After rolling out the revised Facebook privacy settings, widespread user criticism of the change in the "view friends" setting prompted Facebook to roll back the changes in part: "In response to your feedback, we've improved the Friend List visibility option described below. Now when you uncheck the 'Show my friends on my profile' option in the Friends box on your profile, your Friend List won't appear on your profile regardless of whether people are viewing it while logged into Facebook or logged out." Facebook further stated that "this information is still publicly available, however, and can be accessed by applications."[84]

81. Ed Felten, a security expert and Princeton University professor,[85] stated:

> As a user myself, I was pretty unhappy about the recently changed privacy control. I felt that Facebook was trying to trick me into loosening controls on my information. Though the initial letter from Facebook founder Mark Zuckerberg painted the changes as pro-privacy ... the actual effect of the company's suggested new policy was to allow more public access to information. Though the company has backtracked on some of the changes, problems remain.[86]

82. Joseph Bonneau, a security expert and University of Cambridge researcher, criticized Facebook's disclosure of users' friend lists, observing,

> there have been many research papers, including a few by me and colleagues in Cambridge, concluding that [friend lists are] actually the most important information to keep private. The threats here are more

---

[82] *Id*; *see also* ACLUNC dotRights, *What Does Facebook's Privacy Transition Mean for You?*, http://dotrights.org/what-does-facebooks-privacy-transition-mean-you (last visited Dec. 16, 2009).

[83] *See* Google, *Google Blog Search "facebook privacy criticism,"* http://blogsearch.google.com/blogsearch?client=news&hl=en&q=facebook+privacy+criticism&ie=UTF-8&as_drrb=q&as_qdr=w (last visited Dec. 14, 2009).

[84] The Facebook Blog, *Updates on Your New Privacy Tools*, http://blog.facebook.com/blog.php?post=197943902130 (last visited Dec. 14, 2009).

[85] Prof. Felton is also Director of the Princeton Center for Information Technology Policy, a cross-disciplinary effort studying digital technologies in public life.

[86] Ed Felten, *Another Privacy Misstep from Facebook* (Dec. 14, 2009), http://www.freedom-to-tinker.com/blog/felten/another-privacy-misstep-facebook.

> fundamental and dangerous-unexpected inference of sensitive information, cross-network de-anonymisation, socially targeted phishing and scams.[87]

Bonneau predicts that Facebook "will likely be completely crawled fairly soon by professional data aggregators, and probably by enterprising researchers soon after."[88]

83. Security expert[89] Graham Cluley stated:

> if you make your information available to "everyone," it actually means "everyone, forever." Because even if you change your mind, it's too late - and although Facebook say they will remove it from your profile they will have no control about how it is used outside of Facebook.

Cluley further states, "there's a real danger that people will go along with Facebook's recommendations without considering carefully the possible consequences."[90]

84. Other industry experts anticipated the problems that would result from the changes in Facebook's privacy settings. In early July, TechCrunch, Jason Kincaid wrote:

> Facebook clearly wants its users to become more comfortable sharing their content across the web, because that's what needs to happen if the site is going to take Twitter head-on with real-time search capabilities Unfortunately that's far easier said than done for the social network, which has for years trumpeted its granular privacy settings as one of its greatest assets.[91]

Kincaid observed that "Facebook sees its redesigned control panel as an opportunity to invite users to start shrugging off their privacy. So it's piggybacking the new 'Everyone' feature on top of the Transition Tool . . ."[92]

---

[87] Joseph Bonneau, *Facebook Tosses Graph Privacy into the Bin* (Dec. 11, 2009), http://www.lightbluetouchpaper.org/2009/12/11/facebook-tosses-graph-privacy-into-the-bin/; *see also* Arvind Narayanan and Vitaly Shmatikov, *De-Anonymizing Social Networks, available at* http://www.scribd.com/doc/15021482/DeAnonymizing-Social-Networks-Shmatikov-Narayanan; *Phishing Attacks Using Social Networks*, http://www.indiana.edu/~phishing/social-network-experiment/ (last visited Dec. 15, 2009).

[88] Bonneau, *Facebook Tosses Graph Privacy into the Bin.*

[89] Wikipedia, *Graham Cluley*, http://en.wikipedia.org/wiki/Graham_Cluley.

[90] Graham Cluley, *Facebook privacy settings: What you need to know* (Dec. 10, 2009) http://www.sophos.com/blogs/gc/g/2009/12/10/facebook-privacy/.

[91] Jason Kincaid, *The Looming Facebook Privacy Fiasco* (July 1, 2009), http://www.techcrunch.com/2009/07/01/the-looming-facebook-privacy-fiasco/.

[92] *Id.*

85. Following the changes in Facebook privacy settings, noted blogger Danny Sullivan wrote, "I came close to killing my Facebook account this week." He went on to say, "I was disturbed to discover things I previously had as options were no longer in my control." Sullivan, the editor of Search Engine Land and an expert in search engine design,[93] concluded:

> I don't have time for this. I don't have time to try and figure out the myriad of ways that Facebook may or may not want to use my information. That's why I almost shut down my entire account this week. It would be a hell of a lot easier than this mess.[94]

86. Carleton College librarian Iris Jastram states that the privacy trade-off resulting from the Facebook changes is not "worth it." She writes,

> I'm already making concessions by making myself available to the students who want to friend me there and by grudgingly admitting that I like the rolodex function it plays. But I feel zero motivation to give up more than I can help to Facebook and its third party developers. They can kindly leave me alone, please.[95]

87. Chris Bourg, manager of the Information Center at Stanford University Libraries, notes that "[t]here are some concerns with the new default/recommended privacy settings, which make your updates visible to Everyone, including search engines."[96]

88. Reuters columnist Felix Salmon learned of Facebook's revised privacy settings when Facebook disclosed his "friends" list to critics, who republished the personal information. Salmon apologized to his friends and denounced the Facebook "Everyone" setting:

> I'm a semi-public figure, and although I might not be happy with this kind of cyberstalking, I know I've put myself out there and that there will be consequences of that. But that decision of mine shouldn't have some kind

---

[93] Wikipedia, *Danny Sullivan (technologist)*, http://en.wikipedia.org/wiki/Danny_Sullivan_(technologist) (last visited Dec. 15, 2009).

[94] Danny Sullivan, *Now Is It Facebook's Microsoft Moment?* (Dec. 11, 2009), http://daggle.com/facebooks-microsoft-moment-1556.

[95] Iris Jastram, *Dear Facebook: Leave Me Alone*, Pegasus Librarian Blog (Dec. 10, 2009), http://pegasuslibrarian.com/2009/12/dear-facebook-leave-me-alone.html.

[96] Chris Bourg, *Overview of new Facebook Privacy Settings*, Feral Librarian (Dec. 9, 2009), http://chrisbourg.wordpress.com/2009/12/09/overview-of-new-facebook-privacy-settings/.

> of transitive property which feeds through to my personal friends, and I don't want the list of their names to be publicly available to everyone.[97]

89. In a blog post responding to the revisions, Marshall Kirkpatrick of ReadWriteWeb wrote, "the company says the move is all about helping users protect their privacy and connect with other people, but the new default option is to change from 'old settings' to becoming visible to 'everyone.' . . . . This is not what Facebook users signed up for. It's not about privacy at all, it's about increasing traffic and the visibility of activity on the site."[98]

90. Jared Newman of PC World details Facebook's privacy revisions.[99] He is particularly critical of the "Everyone" setting:

> By default, Facebook suggests sharing everything on your profile to make it 'easier for friends to find, identify and learn about you.' It should read, 'make it easier for anyone in the world to find, identify and learn about you.' A little creepier, sure, but this is part of Facebook's never-ending struggle to be, essentially, more like Twitter. Thing is, a lot of people like Facebook because it isn't like Twitter. Don't mess with a good thing.[100]

91. Rob Pegoraro blogged on the Washington Post's "Faster Forward" that the Facebook changes were "more of a mess than I'd expected." He criticized the revised "Everyone" privacy setting, stating the change "should never have happened. *Both from a usability and a PR perspective, the correct move would have been to leave users' settings as they were, especially for those who had already switched their options from the older defaults.*"[101]

92. In another Washington Post story, Cecilia Kang warned users, "post with care."[102] According to Kang:

> While Facebook users will be able to choose their privacy settings, the problem is that most people don't take the time to do so and may simply

---

[97] Felix Salmon, *Why Can't I Hide My List of Facebook Friends?*, Reuters (Dec. 10, 2009), http://blogs.reutes.com/felix-salmon/2009/12/10/why-cant-i-hide-my-list-of-facebook-friends/.

[98] Marshall Kirkpatrick, ReadWriteWeb, *The Day Has Come: Facebook Pushes People to Go Public*, http://www.readwriteweb.com/archives/facebook_pushes_people_to_go_public.php (last visited Dec. 14, 2009).

[99] http://www.pcworld.com/article/184465/facebook_privacy_changes_the_good_and_the_bad.html

[100] *Id.*

[101] Rob Pegoraro, *Facebook's new default: Sharing updates with 'Everyone'*, Washington Post, Dec. 10, 2009, *available at* http://voices.washingtonpost.com/fasterforward/2009/12/facebook_default_no-privacy.html (emphasis added)

[102] Cecilia Kang, *Facebook adopts new privacy settings to give users more control over content*, Washington Post, Dec. 10, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/09/AR2009120904200.html?hpid=topnews.

> stick with the defaults. Others may find the process confusing and may not understand how to adjust those settings. Facebook said about one in five users currently adjusts privacy settings.[103]

93. New York Times technology writer Brad Stone reported that these changes have not been welcomed by many users.[104] One user wrote:

> It's certainly a violation of my privacy policy. My own 'personal' privacy policy specifically states that I will not share information about my friends with any potential weirdos, child molesters, homicidal maniacs, or anyone I generally don't like.[105]

94. Stone invited readers to comment on their understanding of the changes. Of the more than 50 responses received, most expressed confusion, concern, or anger. One user explained,

> I find the changes to be the exact opposite of what Facebook claims them to be. Things that were once private for me, and for carefully selected Facebook friends, are now open to everyone on the Internet. This is simply not what I signed up for. These are not the privacy settings I agreed to. It is a complete violation of privacy, not the other way around.[106]

95. Another Facebook user wrote,

> There are users like myself that joined Facebook because we were able to connect with friends and family while maintaining our privacy and now FB has taken that away. Im [*sic*] wondering where are the millions of users that told FB it would be a good idea to offer real-time search results of their FB content on Google.[107]

96. A Boston Globe editorial, "Facebook's privacy downgrade," observes that "Facebook's subtle nudges toward greater disclosure coincided with other disconcerting changes: The site is treating more information, such as a user's home city and photo, as 'publicly available information' that the user cannot control. Over time, privacy changes can only

---

[103] *Id.*

[104] Brad Stone, *Facebook's Privacy Changes Draw More Scrutiny*, N.Y. Times, Dec. 10, 2009, *available at* http://bits.blogs.nytimes.com/2009/12/10/facebooks-privacy-changes-draw-more-scrutiny.

[105] *Id.*

[106] *Id.*

[107] Riva Richmond, *The New Facebook Privacy Settings: A How-To*, N.Y. Times, Dec. 11, 2009, *available at* http://gadgetwise.blogs.nytimes.com/2009/12/11/the-new-facebook-privacy-settings-a-how-to/?em.

alienate users." Instead, the Globe argues, "Facebook should be helping its 350 million members keep more of their information private."[108]

97. An editorial from the L.A. Times states simply "what's good for the social networking site isn't necessarily what's good for users."[109]

V. Legal Analysis

The FTC's Section 5 Authority

98. Facebook is engaging in unfair and deceptive acts and practices.[110] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[111] These powers are described in FTC Policy Statements on Deception[112] and Unfairness.[113]

99. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[114]

100. The injury must be "substantial."[115] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[116] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[117] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the

---

[108] Editorial, *Facebook's privacy downgrade*, Boston Globe, Dec. 16, 2009, *available at* http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2009/12/16/facebooks_privacy_downgrade.

[109] Editorial, *The business of Facebook*, L.A. Times, Dec. 12, 2009, *available at* http://www.latimes.com/news/opinion/editorials/la-ed-facebook12-2009dec12,0,4419776.story.

[110] *See* 15 U.S.C. § 45.

[111] *Id.*

[112] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), *available at* *http://www.ftc.gov/bcp/policystmt/ad-decept.htm* [*hereinafter* FTC Deception Policy].

[113] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [*hereinafter* FTC Unfairness Policy].

[114] 15 U.S.C. § 45(n); *see, e.g., Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").

[115] FTC Unfairness Policy, *supra* note 113.

[116] *Id.*; *see, e.g., Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").

[117] FTC Unfairness Policy, *supra* note 113.

sales practice also produces."[118] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[119] Finally, "the injury must be one which consumers could not reasonably have avoided."[120] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[121] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[122]

101. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise."[123] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present."[124]

102. The FTC will make a finding of deception if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[125]

103. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[126] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[127] Second, the act or practice must be considered from the perspective of a reasonable consumer.[128] "The test is whether the consumer's interpretation or reaction is reasonable."[129] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the

---

[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] FTC Deception Policy, *supra* note 112.
[126] FTC Deception Policy, *supra* note 112; *see, e.g.*, *Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).
[127] FTC Deception Policy, *supra* note 112.
[128] *Id.*
[129] *Id.*

omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[130]

104. Finally, the representation, omission, or practice must be material.[131] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[132] Express claims will be presumed material.[133] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[134] The harms of this social networking site's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

Material Changes to Privacy Practices and Misrepresentations of Privacy Policies Constitute Consumer Harm

105. Facebook's actions injure users throughout the United States by invading their privacy; allowing for disclosure and use of information in ways and for purposes other than those consented to or relied upon by such users; causing them to believe falsely that they have full control over the use of their information; and undermining the ability of users to avail themselves of the privacy protections promised by the company.

106. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices, that constitute consumer harm.[135] The Commission realizes the importance of transparency and clarity in privacy policies. "Without real transparency, consumers cannot make informed decisions about how to share their information."[136]

107. The FTC recently found that Sears Holding Management Corporations business practices violated the privacy of its customers.[137] The consent order arose from the company's use of software to collect and disclose users' online activity to third parties,

---

[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] 15 U.S.C. § 45.
[136] Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection, New York University: "Promoting Consumer Privacy: Accountability and Transparency in the Modern World" (Oct. 2, 2009).
[137] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

and a misleading privacy policy that did not "adequately [inform consumers as to] the full extent of the information the software tracked."[138] The order requires that the company fully, clearly, and prominently disclose the "types of data the software will monitor, record, or transmit."[139] Further, the company must disclose to consumers whether and how this information will be used by third parties.[140]

108. The Commission has also obtained a consent order against an online company for changing its privacy policy in an unfair and deceptive manner. In 2004, the FTC charged Gateway Learning Corporation with making a material change to its privacy policy, allowing the company to share users' information with third parties, without first obtaining users' consent.[141] This was the first enforcement action to "challenge deceptive and unfair practices in connection with a company's material change to its privacy policy."[142] Gateway Learning made representations on the site's privacy policy, stating that consumer information would not be sold, rented or loaned to third parties.[143] In violation of these terms, the company began renting personal information provided by consumers, including gender, age and name, to third parties.[144] Gateway then revised its privacy policy to provide for the renting of consumer information "from time to time," applying the policy retroactively.[145] The settlement bars Gateway Learning from, among other things, "misrepresent[ing] in any manner, expressly or by implication . . . the manner in which Respondent will collect, use, or disclose personal information."[146]

109. Furthermore, the FTC has barred deceptive claims about privacy and security policies with respect to personally identifiable, or sensitive, information.[147] In 2008, the FTC issued an order prohibiting Life is Good, Inc. from "misrepresent[ing] in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected

---

[138] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (complaint), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf (last visited Sep. 25, 2009).

[139] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

[140] *Id.*

[141] Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm.

[142] *Id.*

[143] In re Gateway Learning Corp., No. C-4120 (2004) (complaint), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.

[144] *Id.*

[145] *Id.*

[146] In re Gateway Learning Corp., No. C-4120 (2004) (decision and order), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

[147] In re Life is Good, No. C-4218 (2008) (decision and order), *available at* http://www.ftc.gov/os/caselist/0723046/080418do.pdf.

from or about consumers."[148] The company had represented to its customers, "we are committed to maintaining our customers' privacy," when in fact, it did not have secure or adequate measures of protecting personal information.[149] The Commission further ordered the company to establish comprehensive privacy protection measures in relation to its customers' sensitive information.[150]

Facebook's Revisions to the Privacy Settings Constitute an Unfair and Deceptive Trade Practice

110. Facebook represented that users "may not want everyone in the world to have the information you share on Facebook," and that users "have extensive and precise controls available to choose who sees what among their network and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities."[151]

111. Facebook's changes to users' privacy settings and associated policies in fact categorize as "publicly available information" users' names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong.[152] Those categories of user data are no longer subject to users' privacy settings.

112. Facebook represented that its changes to its policy settings and associated policies regarding application developers permit users to "opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings,"[153] and tells users, "you can control how you share information with those third-party applications and websites through your application settings"[154]

113. Facebook's changes to users' privacy settings and associated policies regarding application developers in fact eliminate the universal one-click option for opting out of Facebook Platform and Facebook Connect, and replaces it with a less comprehensive

---

[148] *Id.*
[149] *Id.*
[150] *Id.*
[151] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.
[152] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 13, 2009).
[153] *Id.*
[154] *Id.*

option that requires users to provide application developers with personal information that users could previously prevent application developers from accessing.[155]

114. Facebook's representations regarding its changes to users' privacy settings and associated policies are misleading and fail to provide users clear and necessary privacy protections.

115. Wide opposition by users, commentators, and advocates to the changes to Facebook's privacy settings and associated policies illustrate that the changes injure Facebook users and harm the public interest.

116. Absent injunctive relief by the Commission, Facebook is likely to continue its unfair and deceptive business practices and harm the public interest.

117. Absent injunctive relief by the Commission, the privacy safeguards for consumers engaging in online commerce and new social network services will be significantly diminished.

VI. Prayer for Investigation and Relief

118. EPIC requests that the Commission investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users. Specifically, EPIC requests the Commission to:

Compel Facebook to restore its previous privacy settings allowing users to choose whether to publicly disclose personal information, including name, current city, and friends;

Compel Facebook to restore its previous privacy setting allowing users to fully opt out of revealing information to third-party developers;

Compel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers; and

Provide such other relief as the Commission finds necessary and appropriate.

---

[155] Facebook, *Privacy Settings*, http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share (last visited Dec. 13, 2009).

119. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
John Verdi, EPIC Senior Counsel
Kimberly Nguyen, EPIC Consumer Privacy Counsel
Jared Kaprove, EPIC Domestic Surveillance Counsel
Matthew Phillips, EPIC Appellate Advocacy Counsel
Ginger McCall, EPIC National Security Counsel

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

American Library Association
The Center for Digital Democracy
Consumer Federation of America
FoolProof Financial Education
Patient Privacy Rights
Privacy Activism
Privacy Rights Now Coalition
The Privacy Rights Clearinghouse
The U. S. Bill of Rights Foundation

December 17, 2009

TAB B

0923184

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	
FACEBOOK, INC.,	)	
a corporation.	)	**DOCKET NO. C-**

COMPLAINT

The Federal Trade Commission, having reason to believe that Facebook, Inc., a corporation ("Respondent") has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Facebook, Inc. ("Facebook"), is a privately-owned, Delaware corporation with its principal office or place of business at 1601 S. California Avenue, Palo Alto, California 94304.

2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

FACEBOOK'S BUSINESS PRACTICES

3. Since at least 2004, Facebook has operated www.facebook.com, a social networking website. Users of the site create online profiles, which contain content about them such as their name, interest groups they join, the names of other users who are their "friends" on the site, photos albums and videos they upload, and messages and comments they post or receive from their friends. Users also may add content to other users' profiles by sharing photos, sending messages, or posting comments. As of August 2011, Facebook had approximately 750 million users.

4. Since approximately May 2007, Facebook has operated the Facebook Platform ("Platform"), a set of tools and programming interfaces that enables third parties to

develop, run, and operate software applications, such as games, that users can interact with online ("Platform Applications").

5. Facebook obtains revenue by placing third-party advertisements on its site and by selling Facebook Credits, a virtual currency that it offers on its website and through retail outlets. The company also has obtained revenue from fees paid by applicants for its Verified Apps program, described below in Paragraphs 43-47. In 2009, the company had revenues of approximately $777.2 million.

FACEBOOK'S COLLECTION AND STORAGE OF USER INFORMATION

6. Facebook has collected extensive "profile information" about its users, including, but not limited to:

   a. mandatory information that a user must submit to register with the site, including Name, Gender, Email Address, and Birthday;

   b. optional information that a user may submit, such as:

      i. Profile Picture;
      ii. Hometown;
      iii. Interested in (*i.e.*, whether a user is interested in men or women);
      iv. Looking for (*i.e.*, whether a user is looking for friendship, dating, a relationship, or networking);
      v. Relationships (*e.g.*, marital or other relationship status and the names of family members);
      vi. Political and Religious Views;
      vii. Likes and Interests (*e.g.*, activities, interests, music, books, or movies that a user likes); and
      viii. Education and Work (*e.g.*, the name of a user's high school, college, graduate school, and employer);

      and

   c. other information that is based on a user's activities on the site over time, such as:

      i. a Friend List (*i.e.*, a list of users with whom a user has become "Friends" on the site);
      ii. Pages (*e.g.*, any web page on Facebook's web site, belonging to an organization, brand, interest group, celebrity, or other entity, that a user has clicked an online button to "fan" or "like");
      iii. Photos and Videos, including any that a user has uploaded or been "tagged in" (*i.e.*, identified by a user such that his or her name is displayed when a user "hovers" over the likeness); and

iv. messages that a user posts and comments made in response to other users' content.

7. Each user's profile information becomes part of the user's online profile and can be accessible to others, as described below.

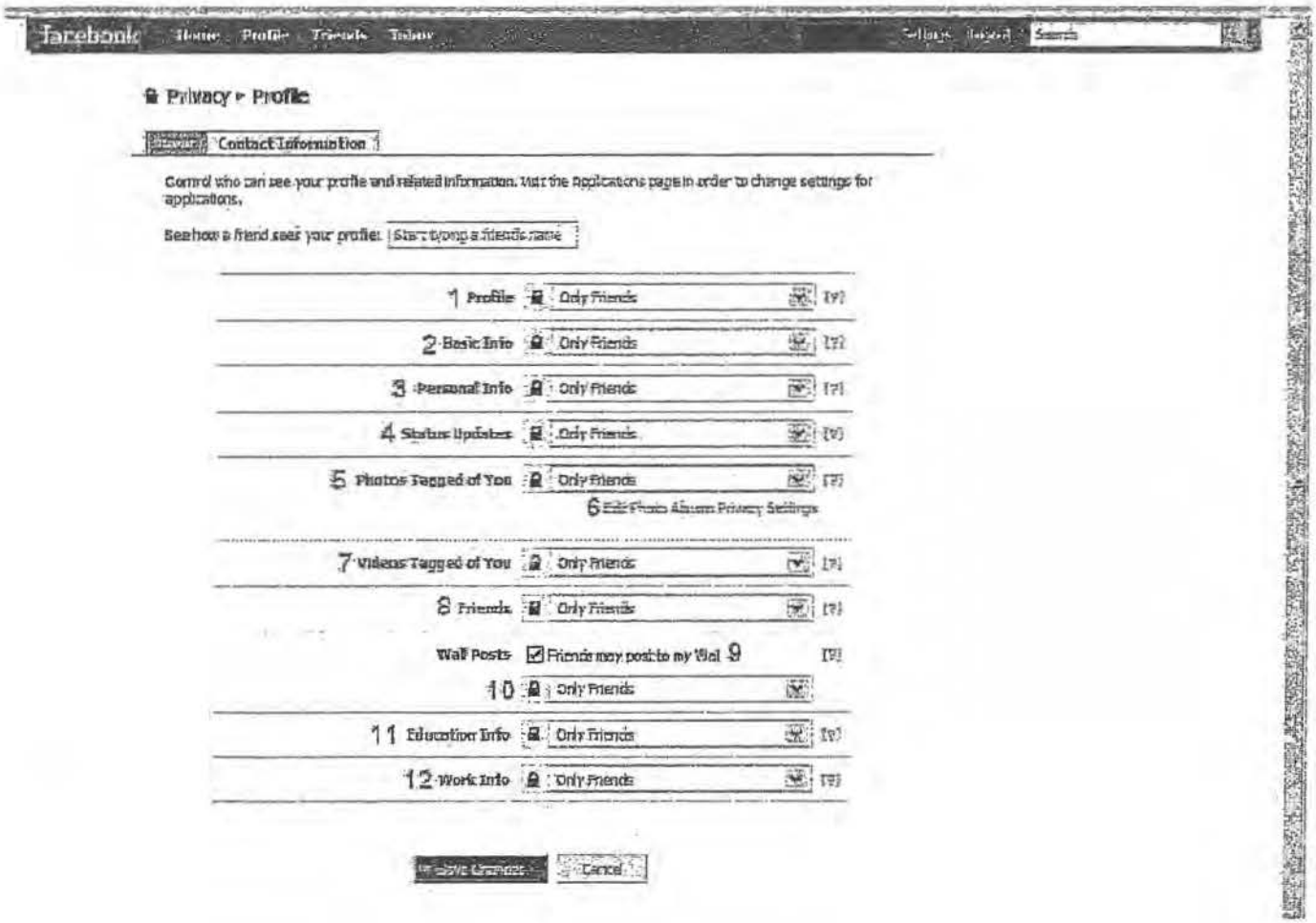
8. Facebook has stored users' profile information on a computer network that it controls. It has assigned to each user a User Identification Number ("User ID"), a persistent, unique number that Platform Applications and others can use to obtain certain profile information from Facebook.

9. Facebook has designed its Platform such that Platform Applications can access user profile information in two main instances. First, Platform Applications that a user authorizes can access the user's profile information. Second, if a user's "Friend" authorizes a Platform Application, that application can access certain of the user's profile information, even if the user has not authorized that Application. For example, if a user authorizes a Platform Application that provides reminders about Friends' birthdays, that application could access, among other things, the birthdays of the user's Friends, even if these Friends never authorized the application.

FACEBOOK'S DECEPTIVE PRIVACY SETTINGS
(Count 1)

10. Since at least November 2009, Facebook has, in many instances, provided its users with a "Central Privacy Page," the same or similar to the one depicted below. Among other things, this page has contained a "Profile" link, with accompanying text that has stated "[c]ontrol who can see your profile and personal information."

11. When users have clicked on the "Profile" link, Facebook has directed them to a "Profile Privacy Page," the same or similar to the one depicted below, which has stated that users could "[c]ontrol who can see your profile and related information." For each "Profile Privacy Setting," depicted below, users could click on a drop-down menu and restrict access to specified users, *e.g.*, "Only Friends," or "Friends of Friends."



12. Although the precise language has changed over time, Facebook's Central Privacy Page and Profile Privacy Page have, in many instances, stated that the Profile Privacy Settings allow users to "control who can see" their profile information, by specifying who can access it, *e.g.*, "Only Friends" or "Friends of Friends." (*See* Central Privacy Page and Profile Privacy Page screenshots, Exhibit A).

13. Similarly, although the precise interface has changed over time, Facebook's Profile Privacy Settings have continued to specify that users can restrict access to their profile information to the audience the user selects, *e.g.*, "Only Friends," "Friends of Friends." (*See* Profile Privacy Page screenshots, Exhibits A, B). In many instances, a user's Profile Privacy Settings have been accompanied by a lock icon. *Id.*

14. None of the pages described in Paragraphs 10-13 have disclosed that a user's choice to restrict profile information to "Only Friends" or "Friends of Friends" would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to "Only Friends" or "Friends of Friends" accessible to any Platform Applications that the user's Friends have used (hereinafter "Friends' Apps"). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (*e.g.*, schools attended), place of employment, photos, and videos.

15. Facebook's Central Privacy Page and Profile Privacy Page have included links to "Applications," "Apps," or "Applications and Websites" that, when clicked, have taken users to a page containing "Friends' App Settings," which would allow users to restrict the information that their Friends' Apps could access.

16. However, in many instances, the links to "Applications," "Apps," or "Applications and Websites" have failed to disclose that a user's choices made through Profile Privacy Settings have been ineffective against Friends' Apps. For example, the language alongside the Applications link, depicted in Paragraph 10, has stated, "[c]ontrol what information is available to applications **you use** on Facebook." (Emphasis added). Thus, users who did not themselves use applications would have had no reason to click on this link, and would have concluded that their choices to restrict profile information through their Profile Privacy Settings were complete and effective.

Count 1

17. As described in Paragraphs 10-13, Facebook has represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends."

18. In truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends" through their Profile Privacy Settings. Instead, such information could be accessed by Platform

Applications that their Friends used. Therefore, the representation set forth in Paragraph 17 constitutes a false or misleading representation.

FACEBOOK'S UNFAIR AND DECEPTIVE DECEMBER 2009 PRIVACY CHANGES (Count 2 and Count 3)

19. On approximately November 19, 2009, Facebook changed its privacy policy to designate certain user information as "publicly available" ("PAI"). On approximately December 8, 2009, Facebook began implementing the changes referenced in its new policy ("the December Privacy Changes") to make public in new ways certain information that users previously had provided.

20. Before December 8, 2009, users could, and did, use their Friends' App Settings to restrict Platform Applications' access to their PAI. For example, as of November 2009, approximately 586,241 users had used these settings to "block" Platform Applications that their Friends used from accessing any of their profile information, including their Name, Profile Picture, Gender, Friend List, Pages, and Networks. Following the December Privacy Changes, Facebook users no longer could restrict access to their PAI through these Friends' App Settings, and all prior user choices to do so were overridden.

21. Before December 8, 2009, users could, and did, use their Profile Privacy Settings to limit access to their Friend List. Following the December Privacy Changes, Facebook users could no longer restrict access to their Friend List through their Profile Privacy Settings, and all prior user choices to do so were overridden, making a user's Friend List accessible to other users. Although Facebook reinstated these settings shortly thereafter, they were not restored to the Profile Privacy Settings and instead were effectively hidden.

22. Before December 8, 2009, users could, and did, use their Search Privacy Settings (available through the "Search" link on the Privacy Settings Page depicted in Paragraph 11) to restrict access to their Profile Picture and Pages from other Facebook users who found them by searching for them on Facebook. For example, as of June 2009, approximately 2.5 million users who had set their Search Privacy Settings to "Everyone," still hid their Profile Picture. Following the December Privacy Changes, Facebook users could no longer restrict the visibility of their Profile Picture and Pages through these settings, and all prior user choices to do so were overridden.

23. To implement the December Privacy Changes, Facebook required each user to click through a multi-page notice, known as the Privacy Wizard, which was composed of:

a. an introductory page, which announced:

> We're making some changes to give you more control of your information and help you stay connected. We've simplified the Privacy page and added the ability to set privacy on everything you share, from status updates to photos.

> At the same time, we're helping everyone find and connect with each other by keeping some information – like your name and current city – publicly available. The next step will guide you through choosing your privacy settings.

b. privacy update pages, which required each users to choose, via a series of radio buttons, between new privacy settings that Facebook "recommended" and the user's "Old Settings," for ten types of profile information (*e.g.*, Photos and Videos of Me, Birthday, Family and Relationships, etc.), and which stated:

> Facebook's new, simplified privacy settings give you more control over the information you share. We've recommended settings below, but you can choose to apply your old settings to any of the fields.

and

c. a confirmation page, which summarized the user's updated Privacy Settings.

(*See* Privacy Wizard screenshots, Exhibit C).

24. The Privacy Wizard did not disclose adequately that users no longer could restrict access to their newly-designated PAI via their Profile Privacy Settings, Friends' App Settings, or Search Privacy Settings, or that their existing choices to restrict access to such information via these settings would be overridden. For example, the Wizard did not disclose that a user's existing choice to share his or her Friend List with "Only Friends" would be overridden, and that this information would be made accessible to the public.

25. The information that Facebook failed to disclose as described in Paragraph 24 was material to Facebook users.

26. Facebook's designation of PAI caused harm to users, including, but not limited to, threats to their health and safety, and unauthorized revelation of their affiliations. Among other things:

a. certain users were subject to the risk of unwelcome contacts from persons who may have been able to infer their locale, based on the locales of their Friends (*e.g.*, their Friends' Current City information) and of the organizations reflected in their Pages;

b. each user's Pages became visible to anyone who viewed the user's profile, thereby exposing potentially controversial political views or other sensitive information to third parties – such as prospective employers, government organizations, or business competitors – who sought to obtain personal information about the user;

c. each user's Friend List became visible to anyone who viewed the user's profile, thereby exposing potentially sensitive affiliations, that could, in turn, reveal a user's political views, sexual orientation, or business relationships, to third parties – such as prospective employers, government organizations, or business competitors – who sought to obtain personal information about the user; and

d. each user's Profile Photo became visible to anyone who viewed the user's profile, thereby revealing potentially embarrassing or political images to third parties whose access users previously had restricted.

Count 2

27. As described in Paragraph 23, Facebook has represented, expressly, or by implication, that its December Privacy Changes provided users with "more control" over their information, including by allowing them to preserve their "Old Settings," to protect the privacy of their profile information.

28. As described in Paragraph 24-26, Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them. Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks. These facts would be material to consumers. Therefore, Facebook's failure to adequately disclose these facts, in light of the representation made, constitutes a deceptive act or practice.

Count 3

29. As described in Paragraphs 19-26, by designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice constitutes an unfair act or practice.

SCOPE OF PLATFORM APPLICATIONS' ACCESS TO FACEBOOK USERS' INFORMATION
(Count 4)

30. Facebook has disseminated or caused to be disseminated numerous statements to users stating that Platform Applications they use will access only the profile information these applications need to operate, including, but not limited to:

a. the following statement, which appeared within a dialog box that each user must click through before using a Platform Application for the first time:

> Allowing [name of Application] access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

(Authorization Dialog box, Exhibit D); and

b. the following additional statements on www.facebook.com:

i. Applications you use will access your Facebook information in order for them to work.

(Facebook Privacy Settings: What You Share, Exhibit E); and

ii. When you authorize an application, it will be able to access any information associated with your account that it requires to work.

(Facebook Privacy Settings: How Applications Interact With Your Information, Exhibit F).

31. Contrary to the statements set forth in Paragraph 30, in many instances, a Platform Application could access profile information that was unrelated to the Application's purpose or unnecessary to its operation. For example, a Platform Application with a narrow purpose, such as a quiz regarding a television show, in many instances could access a user's Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook's web site, despite the lack of relevance of this information to the Application.

Count 4

32. As set forth in Paragraph 30, Facebook has represented, expressly or by implication, that it has provided each Platform Application access only to such user profile information as the Application has needed to operate.

33. In truth and in fact, as described in Paragraph 31, from approximately May 2007 until July 2010, in many instances, Facebook has provided Platform Applications unrestricted access to user profile information that such Applications have not needed to operate. Therefore, the representation set forth in Paragraph 32 constitutes a false or misleading representation.

FACEBOOK'S DISCLOSURE OF USER INFORMATION TO ADVERTISERS (Count 5)

34. Facebook has displayed advertisements ("ads") from third-parties ("Platform Advertisers") on its web site.

35. Facebook has allowed Platform Advertisers to target their ads ("Platform Ads") by requesting that Facebook display them to users whose profile information reflects certain "targeted traits," including, but not limited to:

    a. location (*e.g.*, city or state),

    b. age,

    c. sex,

    d. birthday,

    e. "Interested in" responses (*i.e.*, as described in Paragraph 6(b), whether a user is interested in men or women),

    f. Relationship Status,

    g. Likes and Interests,

    h. Education (*e.g.*, level of education, current enrollment in high school or college, affiliation with a particular college, and choice of major in college), and

    i. name of employer.

36. Facebook has disseminated or caused to be disseminated numerous statements that it does not share information about its users with advertisers, including:

    a. Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as . . . personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an

advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

(Facebook Privacy Policy, November 26, 2008, Exhibit G).

b. We don't share information with advertisers without your consent . . . We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are . . . Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement, there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.

(Facebook Privacy Policy, November 19, 2009, Exhibit H).

c. We do not give your content to advertisers. (Facebook Statement of Rights and Responsibilities, May 1, 2009, Exhibit I).

d. Still others asked to be opted-out of having their information shared with advertisers. This reflects a common misconception about advertising on Facebook. We don't share your information with advertisers unless you tell us to ([*e.g.*,] to get a sample, hear more, or enter a contest). Any assertion to the contrary is false. Period . . . we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads.

(Facebook Blog, http://blog.facebook.com/blog.php, "Responding to Your Feedback," Barry Schnitt, April 5, 2010, Exhibit J).

e. We never share your personal information with advertisers. We never sell your personal information to anyone. These protections are yours no matter what privacy settings you use; they apply equally to people who share openly with everyone and to people who share with only select friends.

The only information we provide to advertisers is aggregate and anonymous data, so they can know how many people viewed their ad and general categories of information about them. Ultimately, this helps advertisers better understand how well their ads work so they can show better ads.

(Facebook Blog, http://blog.facebook.com/blog.php, "The Role of Advertising on Facebook," Sheryl Sandberg, July 6, 2010, Exhibit K).

37. Contrary to the statements set forth in Paragraph 36(a)-(d), in many instances, Facebook has shared information about users with Platform Advertisers by identifying to them the users who clicked on their ads and to whom those ads were targeted. Specifically, from at least September 2008 until May 26, 2010, Facebook designed and operated its web site such that, in many instances, the User ID for a user who clicked on a Platform Ad was shared with the Platform Advertiser.

38. As a result of the conduct described in Paragraph 37, Platform Advertisers potentially could take steps to get detailed information about individual users. For example, a Platform Advertiser could use the User ID to:

a. access the user's profile page on www.facebook.com, to obtain his or her real name, and, after December 8, 2009, other PAI which has included a user's Profile Picture, Gender, Current City, Friend List, Pages, and Networks;

b. combine the user's real name with:

i. any targeted traits used for the ad the user clicked (*e.g.*, if the ad targeted 23-year-old men who were "Interested In" men and "liked" a prescription drug, the advertiser could ascribe these traits to a specific user); and

ii. information about the user's visit to the advertiser's website, including: the time and date of the visit, the pages viewed, and time spent viewing the ad (collectively, "browsing information"); and

c. over time, combine the information described in subparts (a) - (b) with targeting traits related to additional ads or other information about the user's browsing activities across the web.

39. In addition, contrary to the statements set forth in Paragraph 36, Facebook has shared information about users with third parties that advertise on certain Platform Application web sites ("Application Advertisers"), by identifying to them the specific users who visited these applications. Specifically, at various times relevant to this Complaint, when a user visited certain Platform Applications, Facebook disclosed the user's User ID, in plain text, to any Application Advertiser that displayed an ad on the application's web page.

40. As a result of the conduct described in Paragraph 39, Application Advertisers potentially could take steps to get detailed information, similar to those steps described in Paragraph 38(a), (b)(ii), and (c), regarding the user and his or her activities on any Platform Application web site where the advertiser displayed an ad.

Count 5

41. As set forth in Paragraph 36, Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users.

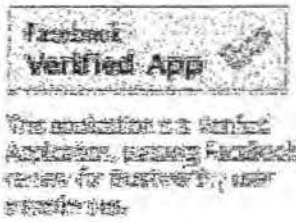
42. In truth and in fact, as described in Paragraphs 37-40, Facebook has provided advertisers with information about its users. Therefore, the representation set forth in Paragraph 41 constitutes a false or misleading representation.

FACEBOOK'S DECEPTIVE VERIFIED APPS PROGRAM
(Count 6)

43. From approximately May 2009 until December 2009, Facebook operated a Verified Apps program, through which it designated certain Platform Applications as "Facebook Verified Apps" ("Verified Apps").

44. Facebook provided each Verified App with preferential treatment compared to other Platform Applications, including, but not limited to:

a. a Verified Apps badge, the same or similar to the badge depicted below, for display on the application's profile page on www.facebook.com; and



b. a green check mark alongside the Platform Application's name, and higher ranking among search results, on www.facebook.com and within Facebook's Application Directory.

45. To apply for the Verified Apps badge, a Platform Application developer paid Facebook a fee of $375, or $175 for a student or nonprofit organization. Facebook awarded the badge to approximately 254 Platform Applications.

46. Facebook has disseminated or caused to be disseminated statements to consumers conveying that it has taken steps to verify the security of Verified Apps, compared to the security of other Platform Applications, including:

a. the Verified Apps badge, described in Paragraph 44(a);

b. the Verified Apps green check mark, described in Paragraph 44(b); and

c. the following statements on its website:

i. **Application Verification** Facebook is introducing the Application Verification program **which is designed to offer extra assurances to help users identify applications they can trust – applications that are secure, respectful and transparent, and have demonstrated commitment to compliance with Platform policies.**

(Press Release, "Facebook Expands Power of Platform Across the Web and Around the World," July 23, 2008, Exhibit L (latter emphasis added)); and

ii. What are Verified Applications?

Verified applications have passed a detailed Facebook review to confirm that the user experience they provide complies with Facebook policies. Verified Applications have committed to be transparent about how they work and will respect you and your friends when they send communication on your behalf.

What is the green check mark next to some applications?

Applications that choose to participate in Facebook's Application Verification Program receive a green check mark when they pass Facebook's detailed review process. The review process is designed to ensure that the application complies with Facebook policies. In addition, Verified applications have committed to be transparent about how they work and will respect you and your friends when they send communication on your behalf.

(Facebook Help Center FAQ, Exhibit M (emphases added)).

47. Contrary to the statements set forth in Paragraph 46, before it awarded the Verified Apps badge, Facebook took no steps to verify either the security of a Verified Application's website or the security the Application provided for the user information it collected, beyond such steps as it may have taken regarding any other Platform Application.

Count 6

48. As set forth in Paragraph 46, Facebook has represented, expressly or by implication, that Facebook has permitted a Platform Application to display its Verified Apps badge when Facebook's review of the security of such Applications has exceeded its review of the security of other Platform Applications.

49. In truth and in fact, as described in Paragraph 47, in many instances Facebook has permitted a Platform Application to display its Verified Apps badge when its review of the application's security has not exceeded its review of other Platform Applications. Therefore, the representation set forth in Paragraph 48 constitutes a false or misleading representation.

FACEBOOK'S DISCLOSURE OF USER PHOTOS AND VIDEOS (Count 7)

50. As described above, Facebook has collected and stored vast quantities of photos and videos that its users upload, including, but not limited to: at least one such photo from approximately ninety-nine percent of its users, and more than 100 million photos and 415,000 videos from its users, collectively, every day.

51. Facebook has stored users' photos and videos such that each one is assigned a Content URL – a uniform resource locator that specifies its location on Facebook's servers. Facebook users and Platform Applications can obtain the Content URL for any photo or video that they view on Facebook's web site by, for example, right-clicking on it. If a user or Application further disseminates this URL, Facebook will "serve" the user's photo or video to anyone who clicks on the URL.

52. Facebook has disseminated or caused to be disseminated statements communicating that a user can restrict access to his or her profile information – including, but not limited to, photos and videos that a user uploads – by deleting or deactivating his or her user account. Such statements include:

a. **Deactivating or deleting your account.** If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted . . . When you delete an account, it is permanently deleted from Facebook.

* * *

Backup copies. Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others;

(Facebook Privacy Policy, November 19, 2009, Exhibit H);

b. To deactivate your account, navigate to the "Settings" tab on the Account Settings page. Deactivation will remove your profile and content associated with your account from Facebook. In addition, users will not be able to search for you or view any of your information.

(Facebook Help Center FAQ, Exhibit N);

> If you deactivate your account, your profile and all information associated with it are immediately made inaccessible to other Facebook users.

(Facebook Help Center FAQ, Exhibit O); and

> If you deactivate your account from the "Deactivate Account" section on the Account page, your profile and all information associated with it are immediately made inaccessible to other Facebook users.

(Facebook Help Center FAQ, Exhibit P).

53. Contrary to the statements set forth in Paragraph 52, Facebook has continued to display users' photos and videos to anyone who accesses Facebook's Content URLs for them, even after such users have deleted or deactivated their accounts.

Count 7

54. As set forth in Paragraph 52, Facebook has represented, expressly or by implication, that after a user has deleted or deactivated his or her account, Facebook does not provide third parties with access to his or her profile information, including any photos or videos that the user has uploaded.

55. In truth and in fact, as described in Paragraph 53, in many instances, Facebook has provided third parties with access to a user's profile information – specifically photos or videos that a user has uploaded – even after the user has deleted or deactivated his or her account. Therefore, the representation set forth in Paragraph 54 constitutes a false or misleading representation.

U.S.-EU SAFE HARBOR FRAMEWORK
(Count 8)

56. The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of the European Union ("EU") that is consistent with the requirements of the European Union Data Protection Directive ("Directive"). The Directive sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission ("EC") has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is commonly referred to as meeting the EU's "adequacy" standard.

57. To satisfy the EU's adequacy standard for certain commercial transfers, the U.S. Department of Commerce ("Commerce") and the EC negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The Safe Harbor is a voluntary

framework that allows U.S. companies to transfer personal data lawfully from the EU to the U.S. To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.

58. The Safe Harbor privacy principles, issued by Commerce on July 21, 2000, include the following:

> **NOTICE:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.
>
> **CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

59. From at least May 10, 2007, until the present, Facebook has maintained a current self-certification to Commerce and has appeared on the list of Safe Harbor companies on the Commerce website. Pursuant to its self-certification, Facebook has transferred data collected from its users in the EU to the U.S. for processing.

60. From approximately May 2007 until the present, Facebook has stated in its Privacy Policy that it participates in, adheres to, and/or complies with "the EU Safe Harbor Privacy Framework as set forth by the United States Department of Commerce." (*See* Facebook Privacy Policy, November 26, 2008, Exhibit G; Facebook Privacy Policy, November 19, 2009, Exhibit H; Facebook Privacy Policy, December 9, 2009, Exhibit Q; Facebook Privacy Policy, April 22, 2010, Exhibit R; Facebook Privacy Policy, December 22, 2010, Exhibit S). Similarly, from approximately November 19, 2009 until the present, Facebook has stated on the Commerce website that it "adheres to the U.S. Safe Harbor Framework developed by the U.S. Department of Commerce and the European Union."

Count 8

61. As described in Paragraphs 59-60, Facebook has represented, expressly or by implication, that it has complied with the U.S. Safe Harbor Privacy Principles, including the principles of Notice and Choice.

62. In truth and in fact, as described in Paragraphs 10-42 and 50-55, in many instances, Facebook has not adhered to the U.S. Safe Harbor Privacy Principles of Notice and Choice. Therefore, the representation set forth in Paragraph 61 constitutes a deceptive act or practice.

63. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ___ day of _____, ____, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

TAB C

0923184

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
J. Thomas Rosch
Edith Ramirez
Julie Brill
Maureen K. Ohlhausen

In the Matter of	)	
	)	
	)	DOCKET NO. C-4365
FACEBOOK, INC.,	)	
a corporation.	)	
	)	

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*;

The Respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having carefully considered the comments filed by interested persons, now in further conformity with

the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Facebook, Inc. ("Facebook") is a Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "Respondent" shall mean Facebook, its successors and assigns. For purposes of Parts I, II, and III of this order, "Respondent" shall also mean Facebook acting directly, or through any corporation, subsidiary, division, website, or other device.

2. "Commerce" shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

3. "Clear(ly) and prominent(ly)" shall mean:

   A. in textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

   B. in communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;

   C. in communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and

   D. in all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in

mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

4. "Covered information" shall mean information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above.

5. "Nonpublic user information" shall mean covered information that is restricted by one or more privacy setting(s).

6. "Privacy setting" shall include any control or setting provided by Respondent that allows a user to restrict which individuals or entities can access or view covered information.

7. "Representatives" shall mean Respondent's officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

8. "Third party" shall mean any individual or entity that uses or receives covered information obtained by or on behalf of Respondent, other than: (1) a service provider of Respondent that (i) uses the covered information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the covered information, or any individually identifiable information derived from such covered information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a user and for no other purpose; or (2) any entity that uses the covered information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

9. "User" shall mean an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent's products and services.

I.

IT IS ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

A. its collection or disclosure of any covered information;

B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;

C. the extent to which Respondent makes or has made covered information accessible to third parties;

D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;

E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user's account with Respondent or during such time as a user's account is deactivated or suspended; and

F. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and

B. obtain the user's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. §45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

IV.

IT IS FURTHER ORDERED that Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to

implement and maintain appropriate privacy protections for such covered information.

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

V.

IT IS FURTHER ORDERED that, in connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is

terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

VI.

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;

B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

C. for a period of five (5) years from the date received, any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order;

D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent's attempt to obtain the consent of users referred to in Part II above, along with documents and information sufficient to show each user's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent; and

E. for a period of three (3) years after the date of preparation of each Assessment required under Part V of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VII.

IT IS FURTHER ORDERED that Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

VIII.

IT IS FURTHER ORDERED that Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of Facebook, Inc.*, FTC File No.[ ]. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IX.

IT IS FURTHER ORDERED that Respondent, within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, Respondent shall submit additional true and accurate written reports.

X.

This order will terminate on July 27, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Part of this order that terminates in fewer than twenty (20) years; and

B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that this order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Rosch dissenting and Commissioner Ohlhausen not participating.

Donald S. Clark
Secretary

SEAL
ISSUED: July 27, 2012

TAB D

2012 WL 2126533
United States District Court,
D. Maryland.

FEDERAL TRADE COMMISSION, Plaintiff,
v.
Kristy ROSS, individually and as an officer of Innovative Marketing, Inc., Defendant.

Civil Action No. RDB–08–3233. | June 11, 2012.

Attorneys and Law Firms

Carmen Louise Christopher, Colleen Brennan Robbins, Paul Bryan Spelman, Federal Trade Commission, Washington, DC, for Plaintiff.

William Thomas Welch, McMahon, Welch & Learned, Reston, VA, Russell D. Duncan, Garret G. Rasmussen, Jonathan Adler Direnfeld, Michael J. Madigan, Washington, DC, Carolyn Gurland, Carolyn Gurland Attorney at Law, Dan K. Webb, Justin E. Endres, Winston and Strawn, Thomas L. Kirsch, II, Chicago, IL, for Defendant.

MEMORANDUM OPINION

RICHARD D. BENNETT, District Judge.

*1 The Federal Trade Commission ("FTC") brought this case under sections 5(a) and 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a) and 53(b), against a group of corporate entities and individuals for alleged deceptive conduct in connection with the sale of software. Specifically, the FTC alleged that two companies, Defendants Innovative Marketing, Inc. ("Innovative Marketing") and ByteHosting Internet Services, LLC ("ByteHosting") operated as a common enterprise (the "IMI Enterprise" or "Enterprise") to conduct a massive "scareware" [1] scheme that marketed a variety of computer security software via deceptive advertising. The FTC alleged that several of the companies' officers and directors, namely, Sam Jain ("Jain"), Daniel Sundin ("Sundin"), Marc D'Souza ("D'Souza"), Kristy Ross ("Ross"), and James Reno ("Reno"), directed or participated in the IMI Enterprise.

The FTC filed the present action on December 2, 2008. After a hearing was held on December 12, 2008, this Court entered a Preliminary Injunction that served to, *inter alia,* prohibit Defendants from continuing the alleged deceptive business activities, freeze Defendants' assets, and compel Defendants to turn over certain business records to the FTC.

Of the original eight defendants, four have settled with the FTC, and three are in default and have had judgments entered against them for failure to appear and participate in this litigation. Defendant Kristy Ross is the only remaining defendant, and the sole remaining motion, the FTC's Motion for Summary Judgment, pertains to her alone. On May 9, 2012, this Court held a hearing on that motion pursuant to Local Rule 105.6 (D.Md.2011). [2] For the reasons that follow, the Federal Trade Commission's Motion for Summary Judgment (ECF No. 186) is DENIED, and a bench trial has been scheduled for September 10, 2012.

BACKGROUND

The background facts of this case were fully set forth in this Court's previous Memorandum Opinion entered on September 16, 2009. *See Federal Trade Commission v. Innovative Marketing, Inc.,* 654 F.Supp.2d 378 (D.Md.2009) (ECF Nos. 138 & 139). That background is repeated here, in part, so as to provide context for the pending motion for summary judgment.

The FTC's Complaint sets forth a host of factual allegations, general and specific, concerning misconduct committed by the corporate defendants, Innovative Marketing, and Bytehosting, and the individual defendants, Reno, Jain, Sundin, Ross, and Marc and Maurice D'Souza. The Complaint alleges that since at least 2003, the Defendants conspired to sell computer security software by means of deceptive Internet advertising. More specifically, Defendants allegedly issued exploitive advertisements that redirected consumers to sites that falsely claimed that the consumers' computers had been scanned and that certain viruses, pornographic pictures, or compromised files had been discovered. The consumers were then directed to purchase computer security software in order to purge their computers of the suspect files purportedly detected by the Defendants' fake scans.

*2 The Complaint also alleges that since 2004 or earlier, Defendants had placed misleading advertisements for their software products with major Internet advertising networks, which serve as brokers that distribute advertisements to their website partners. The advertising networks contracted

with their partners to display the Defendants' advertisements across the Internet. After the advertising networks, such as MyGeek, began to receive complaints, they stopped accepting Defendants' advertisements. At this point, in 2007, Defendants allegedly began creating a number of sham Internet advertising agencies that duped advertising networks and commercial websites into accepting their misleading advertisements. Toward this end, Defendants falsely represented that they were authorized to place advertisements, and they used sophisticated program coding that concealed the exploitative nature of the ads from the advertising networks to gain their approval for distribution. Once distributed and placed upon popular Internet sites, the exploitative content of the ads was revealed to many of the consumers, who were thereupon redirected to the Defendants' websites that operated the bogus scans. The FTC alleges that this scheme resulted in substantial consumer injury, and that more than one million consumers were deceived into purchasing the Defendants' software products.

Defendant Kristy Ross does not directly contradict these assertions made by the FTC and does not argue that Innovative Marketing or the other named defendants did not violate the FTC Act through unfair and deceptive advertising and marketing. Instead, her opposition to the FTC's motion centers on her role in the company—specifically, she argues that she was merely an employee and not a "control person" at the company, that she did not have the requisite knowledge of the misconduct at issue, and as a result, cannot be held individually liable under the Act. In this regard, the specific allegations concerning Ross' control and knowledge of the company's conduct will be discussed in the Analysis section *infra*.

STANDARD OF REVIEW

Rule 56 of the Federal Rules of Civil Procedure provides that a court "shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed.R.Civ.P. 56(c). A material fact is one that "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). A genuine issue over a material fact exists "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* In considering a motion for summary judgment, a judge's function is limited to determining whether sufficient evidence exists on a claimed factual dispute to warrant submission of the matter to a jury for resolution at trial. *Id.* at 249.

In undertaking this inquiry, this Court must consider the facts and all reasonable inferences in the light most favorable to the nonmoving party. *Ricci v. DeStefano*, 557 U.S. 557, 129 S.Ct. 2658, 2677, 174 L.Ed.2d 490 (U.S.2009) (quoting *Scott v. Harris*, 550 U.S. 372, 380, 127 S.Ct. 1769, 167 L.Ed.2d 686 (2007)). However, this Court must also abide by its affirmative obligation to prevent factually unsupported claims and defenses from going to trial. *Drewitt v. Pratt*, 999 F.2d 774, 778–79 (4th Cir.1993). If the evidence presented by the nonmoving party is merely colorable, or is not significantly probative, summary judgment must be granted. *Anderson*, 477 U.S. at 249–50. On the other hand, a party opposing summary judgment must "do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986); *see also In re Apex Express Corp.*, 190 F.3d 624, 633 (4th Cir.1999). This Court has previously explained that a "party cannot create a genuine dispute of material fact through mere speculation or compilation of inferences." *Shin v. Shalala*, 166 F.Supp.2d 373, 375 (D.Md.2001) (citations omitted).

ANALYSIS

*3 The FTC has brought the present action under sections 5(a) and 13 of the FTC Act. Section 5(a) of the Act, 15 U.S.C. § 45(a)(1), prohibits engaging in "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." Section 13, 15 U.S.C. § 53(b), authorizes the FTC to seek injunctive relief for section 5 violations.

To succeed under section 5(a), the FTC must prove (1) that there was a representation; (2) that the representation was likely to mislead consumers; and (3) that the misleading representation was material. *See FTC v. Tashman*, 318 F.3d 1273, 1277 (11th Cir.2003).

Upon the establishment of corporate liability, individual defendants may be held liable if the FTC can show that they "participated directly in the practices or acts or had authority to control them." *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 573 (7th Cir.1989); *see also, e.g., FTC v. Freecom Communs., Inc.*, 401 F.3d 1192, 1203 (10th Cir.2005); *FTC v. Publ'g Clearing House, Inc.*, 104 F.3d 1168, 1170 (9th Cir.1997).

"Authority to control the company can be evidenced by active involvement in business affairs and the making of corporate policy, including assuming the duties of a corporate officer." *Amy Travel,* 875 F.2d at 573. In addition, the FTC must show that the individual had some knowledge of the violative conduct. *See Publ'g Clearing House,* 104 F.3d at 1170 (noting that corporate individuals are liable if they "had knowledge that the corporation or one of its agents engaged in dishonest or fraudulent conduct, that the misrepresentations were the type which a reasonable and prudent person would rely, and that consumer injury resulted"). In this regard the FTC need not make a showing of "intent per se"—instead the knowledge requirement may be "fulfilled by showing that the individual had actual knowledge of material misrepresentations, reckless indifference to the truth or falsity of such misrepresentations, or an awareness of a high probability of fraud along with an intentional avoidance of the truth.' " *Amy Travel,* 875 F.2d at 574 (quoting *FTC v. Kitco of Nev., Inc.,* 612 F.Supp. 1282, 1292 (D.Minn.1985)); *see also FTC v. Direct Mktg. Concepts, Inc.,* 569 F.Supp.2d 285, 311 (D.Mass.2008) (noting that the FTC must prove "that the individual defendants either knew or should have known about the deceptive practices, but it is not required to prove subjective intent to defraud").

The crux of the FTC's case against the sole remaining Defendant Kristy Ross is based on its contention that she exercised significant control over, and had knowledge of, the company's illegal activities. As Ross does not contest much of the FTC's evidence regarding the other defendants' alleged violations of the FTC Act, this Court will assume *arguendo* that FTC Act violations did indeed occur and will concentrate on the parties' arguments pertaining to Ross' involvement with Innovative Marketing.

***4** As a preliminary matter, it must be noted that the FTC has clearly been able to compile a substantial and impressive amount of evidence in this case. Because this case is set for a bench trial, this Court will be the finder of fact, and will, in all likelihood, review much the same evidence and argument at trial. Given this, it would appear that the expense of further litigation could be avoided through summary judgment. However, this Court's role in evaluating evidence in the context of summary judgment is markedly different than in the context of a bench trial. Judge Nickerson of this Court recently described the interplay between the summary judgment and bench trial phases of a case as follows:

> In ruling on motions for summary judgment, the Court's role is limited. "[A]t the summary judgment stage the judge's function is not ... to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial." *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 249, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). "A judge does not sit as a trier of fact when deciding a motion for summary judgment even if the case is scheduled to be heard without a jury." *Med. Inst. Of Minn. v. Nat'l Ass'n of Trade & Technical Schs.,* 817 F.2d 1310, 1315 (8th Cir.1987). Furthermore, "even if the facts are undisputed, summary judgment may not be granted where there is disagreement over inferences that can be reasonably be drawn from those facts." *In re Unisys Sav. Plan Litig.,* 74 F.3d 420, 433 (3rd Cir.1996).
>
> In contrast, after a bench trial, the Court is required to weigh the evidence and make credibility determinations. *In re French,* 499 F.3d 345, 359 (4th Cir.2007). Rather than deciding whether a genuine issue of material fact exists, the Court makes findings of fact by evaluating the persuasiveness of conflicting evidence and "decid[ing] which is more likely true." *Kearney v. Standard Ins. Co.,* 175 F.3d 1084, 1095 (9th Cir.1999) (en banc).

Waterkeeper Alliance, Inc. v. Alan and Kristin Hudson Farm, et al., No. WMN–10–0487, Ltr. Order at 2, ECF No. 143 (D.Md. March 1, 2012); *see also* 10A CHARLES ALAN WRIGHT, ARTHUR R. MILLER, MARY KAY KANE & RICHARD L. MARCUS, FEDERAL PRACTICE AND PROCEDURE § 2712 (3d ed. 1998) ("A motion for summary judgment lies only when there is no genuine issue of material fact; summary judgment is not a substitute for the trial of disputed fact issues. Accordingly, the court cannot try issues of fact on a Rule 56 motion but is only empowered to determine whether there are issues to be tried.").

Notwithstanding the fact that the FTC's evidence is substantial, at this stage in the litigation, this Court is unable to conclusively determine whether the FTC is entitled to summary judgment against Kristy Ross because to do so would require this Court to make credibility findings, inferences, and findings of fact that are more properly made in the context of a bench trial.

***5** The FTC argues that Ross was a "control person" at Innovative Marketing, and points to evidence showing that Ross worked at the company since its inception and during her tenure, assumed the roles of Chief Operating Officer and Chief Technology Officer. *See* Ross Aff., Ex. 2 to FTC's Mot. for Summ. J.[3] Moreover, the FTC has propounded evidence showing that beginning in 2006, Ross held the position

of Vice President of Business Development and was later identified as a Vice President of Innovative Marketing as late as June 21, 2008. *See* FTC Mem. at 51, ECF No. 186–1 and supporting exhibits. Ross routinely approved and requested payment for expenses incurred by Innovative Marketing, and on several occasions, used her personal credit card to pay for certain advertising and operating expenses. *Id.* In Innovative Marketing's chat logs Ross is observed making executive-type decisions, demanding that employees fix problems and follow company procedures, and delegating Innovative Marketing business projects. In one telling instance, Ross threatens to fine an entire department if it does not complete a project on schedule. *Id.* at 52.

Regarding Ross' knowledge of the deceptive nature of Innovative Marketing's advertisements, the FTC has argued that Ross opened fifty-four individual accounts with MyGeek, an internet advertising company, routinely communicated with MyGeek regarding complaints that company received pertaining to Innovative Marketing ads, and routinely approved and edited the content of ads placed on the MyGeek network. *Id.* at 53–56. In the company's chat logs, Ross is observed directing employees to make ads more aggressive because "aggression zero doesnt [sic] give sales." *Id.* at 56.

As noted, the evidence propounded by the FTC is substantial, and drawing the required inferences from the evidence in favor of the FTC would result in a grant of summary judgment in its favor. However, as persuasively argued by Ross, inferences drawn from the very same evidence in her favor plausibly lead to the opposite conclusion—that Ross was merely an employee of Innovative Marketing and not a control person—and, at the very least, create genuine issues of material fact that cannot be decided on summary judgment.

For example, Ross notes that at the time Innovative Marketing was formed by Sam Jain and Daniel Sundin in 2002, Ross was twenty-two years old and was dating Sam Jain. *See* Ross Mem. at 2, ECF No. 199 and supporting exhibits. She argues that the FTC's evidence pertaining to her corporate titles with Innovative Marketing is essentially meaningless insofar as Innovative Marketing did not operate under traditional corporate formalities, and the titles given to employees were used only to explain employees' responsibilities to overseas employees. *Id.* In this regard, Ross points to a declaration made by one of the FTC's own investigators that states: "Innovative Marketing, Inc. did not adhere to corporate formalities with respect to business structure, the titles and roles of Officers or business records." *Id.* Regarding the Canadian Litigation documents cited extensively by the FTC, Ross argues that those same affidavits and pleadings conclusively show that she was *not* a control person or director at Innovative Marketing. For example, Daniel Sundin's affidavit in the Canadian Litigation indicates that Sundin and Sam Jain alone were the principals of the Innovative Marketing venture, and make no mention of Ross being a partner or director of the company. *Id.* at 14. Finally, when Marc D'Souza became a third partner at Innovative Marketing in 2006, Ross was not involved in any of the decisions regarding the additional partner or his level of compensation. *Id.* at 15.

***6** Similarly, Ross notes that while certain of the company's chat logs indicate that she had some degree of control over certain aspects of Innovative Marketing's affairs, the vast majority of those same logs show that instead of approving ads, Ross merely makes English language suggestions in order to assist Innovative Marketing's overseas employees. *Id.* at 18. Moreover, some of the chat logs, when viewed in the light most favorable to Ross, might possibly indicate that she actually believed Innovative Marketing was a legitimate company that provided "sound products" to its customer. *Id.* at 25–26. In addition, in a 2006 e-mail exchange between Sam Jain and James Reno, a co-defendant whom the FTC described in its Complaint as a "senior executive," Reno writes to Jain:

> Hey What is kristy's role in the company? How much access is she allowed to have' And how much stuff is she allowed to request to be completed' ie: removing accounts, ect. She has been increasingly making changes in access control lately, and I need to know if she's allowed. (ie: suddens acct, uni's ect.) Regards, James.

Jain responded:

> Yeah that should be fine. Sudden has been talking to her on an off when he's not sick. He told her to remove uni's vpn since uni's already quit, as well as sudden claimed he got his laptop stolen so he had to get his passwords changed....

Ross Mem. at 19–20 and supporting exhibits.

Put simply, the conflicting inferences that can be drawn from the extensive record in this case do not permit this Court to grant summary judgment to the FTC. Perhaps sensing this conclusion, the FTC seeks to have this Court draw an adverse inference against Ross for continually invoking her Fifth Amendment right against self-incrimination in response to deposition questions posed, and for failing to provide any meaningful discovery. However, at this stage of the litigation, this Court concludes that a finding of an adverse inference is not warranted. In ruling on a motion for summary judgment this Court must draw all reasonable inferences in favor of the nonmoving party and an adverse inference finding conflicts with that standard. *See, e.g., Stichting Ter Behartiging Van de Bel. V. Schreiber,* 407 F.3d 34, 55 (2d Cir.2005); *LaSalle Bank Lake View v. Seguban,* 54 F.3d 387, 391 (7th Cir.1995) ("Treating [the defendants'] silence as a separate piece of evidence supporting the Bank's motion for summary judgment and drawing inferences against [them] on the basis of that fact seems to be in tension with the ordinary summary judgment rule that all reasonable inferences must be drawn in favor of the nonmovant."); *In re Inflight Newspapers, Inc.,* 423 B.R. 6, 17 (Bankr.E.D.N.Y.2010) ("the summary judgment standard, requiring a Court to draw all reasonable inferences in favor of the nonmoving party, precludes the drawing of an adverse inference, despite potential for the ultimate trier of fact to draw an adverse inference.' ").

*7 The United States Court of Appeals for the Fourth Circuit has cautioned, however, that a defendant's assertion of her Fifth Amendment privilege can impose "severe burdens" and may "significantly reduce a party's chances of prevailing on the merits of his claim." *In re Grand Jury Subpoena,* 836 F.2d 1468, 1473 (4th Cir.1988). While this Court will not draw an adverse inference in the context of summary judgment, as a fact finder in a bench trial, this Court *is* "entitled to draw adverse inferences from a defendant's invocation of the privilege against self-incrimination." *Eplus Tech., Inc. v. Aboud,* 313 F.3d 166, 179 (4th Cir.2002).

In sum, after reviewing the record, as well as the pleadings, exhibits, and argument by counsel, this Court, taking the evidence in the light most favorable to the defendant, must deny the FTC's motion for summary judgment.

CONCLUSION

For the reasons stated above, the FTC's Motion for Summary Judgment (ECF No. 186) is DENIED, and this case will proceed to a bench trial on Monday, September 10, 2012.

ORDER

For the reasons stated in the foregoing Memorandum Opinion, it is this 11th day of June, 2012, ORDERED that:

1. Plaintiff Federal Trade Commission's Motion for Summary Judgment (ECF No. 186) is DENIED;

2. A bench trial in this case has been scheduled for Monday, September 10, 2012; and

3. The Clerk of the Court transmit copies of this Order and accompanying Memorandum Opinion to Counsel.

Parallel Citations

2012-2 Trade Cases P 78,075

Footnotes

1 As noted in the FTC's Complaint, "scareware" is a common term that refers to a software-driven, Internet-based scheme that "exploits consumers' legitimate concerns about Internet-based threats like spyware and viruses by issuing false security or privacy warnings to consumers for the sole purpose of selling software to fix the imagined problem." Compl. ¶ 15, ECF No. 1.

2 On May 27, 2010, the parties jointly moved for a sixty day stay of proceedings in order to pursue a settlement. This Court granted that request. *See* Order, ECF No. 170. On July 27, 2010, the parties moved for an additional sixty day stay of proceedings to pursue settlement. This Court granted that request as well, and the entire case was stayed. *See* Order, ECF No. 172. On September 22, 2010, the parties resumed litigation, and this Court entered an order lifting the stay and revising the scheduling order. *See* Order, ECF No. 175. As a result of a docketing error, however, the stay was not technically lifted and the case was not marked as an active case on this Court's docket. This matter was recently brought to the Court's attention, and the stay was promptly lifted. This Court regrets the error, and resulting delay in proceedings.

3 As the FTC continually points out, Kristy Ross has chosen to invoke her Fifth Amendment right against self-incrimination at nearly every turn in this litigation, and has effectively not participated in discovery. Her affidavit, cited by the FTC, was not made in connection with this case, but rather in connection with a Canadian lawsuit filed by Defendants Daniel Sundin and Sam Jain against co-Defendant Marc D'Souza regarding a dispute over Innovative Marketing's profits (hereinafter referred to as the "Canadian Litigation"). Ross sought to strike the affidavits and pleadings from the Canadian Litigation on the ground that they contained inadmissible hearsay. *See* Ross' Motion to Strike, ECF No. 204. This Court heard argument on that motion and denied it on the record during the May 9, 2012 motions hearing. *See* May 9, 2012 Order, ECF No. 226.

End of Document

TAB E

STATEMENT OF COMMISSIONERS ORSON SWINDLE AND THOMAS B. LEARY CONCURRING IN PART AND DISSENTING IN PART

in ReverseAuction.com, Inc., File No. 0023046

ReverseAuction.com, Inc., a company that offers auction services on the Internet, became a member of eBay, a popular Internet auction site, and was thereby granted access to the e-mail addresses, eBay user IDs, and feedback ratings of other eBay members. When registering as a member, ReverseAuction agreed to abide by eBay's privacy agreement, which prohibits members from using the personal identifying information of any eBay member obtained through eBay's web site for the purpose of sending unsolicited commercial e-mail. In Count One of the complaint, the Commission alleges that ReverseAuction violated Section 5 of the FTC Act by using other eBay members' user IDs, feedback ratings, and e-mail addresses for the purpose of sending those members unsolicited commercial e-mail, in contravention of its agreement with eBay. The complaint pleads alternative theories in support of the Section 5 violation in Count One: that ReverseAuction engaged in deception by falsely representing to eBay that it would abide by the privacy agreement, Complaint ¶ 16; or that ReverseAuction's use of the eBay member information for the purposes of sending unsolicited commercial e-mail was an unfair practice. Complaint ¶ 17.

We join our colleagues in support of the deception theory in Count I. ReverseAuction represented to eBay that it would not use the information it obtained about other members to send unsolicited commercial e-mail. ReverseAuction, however, sent unsolicited e-mails promoting its auction site to eBay members using e-mail addresses harvested from eBay's site. ReverseAuction thereby deceived eBay directly and, in doing so, also misled other members of the eBay community who believed that all participants in the eBay marketplace would abide by the same privacy rules.

We recognize that the Commission's decision to proceed against the deception alleged in Count One could be construed as placing the Commission in the position of enforcing eBay's privacy policy. Nevertheless, we want to emphasize that our decision to challenge ReverseAuction's deception is an effort to buttress, not supplant or detract from, initiatives of private parties (like eBay) who develop and implement their own privacy arrangements. We further believe that it is in the public interest for the Commission to pursue the deception allegation in Count One because such deceptive conduct undermines consumer confidence in the nascent electronic marketplace at a critical point in time and may thereby inhibit its development.

We do not, however, support the unfairness theory in Count One. The Commission has no authority to declare an act or practice unfair unless it "causes or is likely to cause *substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. ¶ 45(n) (emphasis added). The statutory requirement of

substantial injury is actually derived from the Commission's own Statement of Policy, issued in 1980. The Commission explained at that time that, "[t]he Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm . . . Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair." Letter from the Commission to the Consumer Subcommittee of the Senate Committee on Commerce, Science, and Transportation, *Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction*, 4 Trade Reg. Rep.(CCH) ♦ 13,203 (Dec. 17, 1980), reprinted in *International Harvester, Inc.*, 104 F.T.C. 949, 1070-76 (1984).

We do not say that privacy concerns can never support an unfairness claim. In this case, however, ReverseAuction's use of eBay members' information to send them e-mail did not cause substantial enough injury to meet the statutory standard.

Consumers do not have a substantial privacy interest in the e-mail addresses and other information that ReverseAuction harvested since consumers had already agreed to make this information available to millions of other eBay members (albeit with restrictions on using it for commercial solicitations). Moreover, a substantial portion of this information is available without restriction to non-members who visit eBay's web site. Merely obtaining consumers' e-mail addresses without their explicit consent and sending them e-mail solicitations does not cause substantial injury.

The injury in this case was caused by deception: that is, by ReverseAuction's failure to honor its express commitments. It is not necessary or appropriate to plead a less precise theory.

Industry self-regulation and consumer preferences, as expressed in the marketplace, are the best and most efficient ways to formulate privacy arrangements on the Internet and in commerce generally. Because proliferation of the kind of deceptive conduct in which ReverseAuction allegedly engaged could undermine consumer confidence in such privacy arrangements, we believe that it is appropriate to pursue this matter under a deception theory. The unfairness theory, however, posits substantial injury stemming from ReverseAuction's use of information readily available to millions of eBay members to send commercial e-mail. This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not. We are troubled by the possibility of an expansive and unwarranted use of the unfairness doctrine.

For the reasons discussed above, we dissent from the unfairness allegation contained in Paragraph 17 of the Complaint.