

**July 14, 2000**

**John Mogg  
Director, DG XV  
European Commission  
Office C 107-6/72  
Rue de la Loi, 200  
1049 Brussels  
BELGIUM**

**Dear Mr. Mogg:**

**I understand a number of questions have arisen with regard to my letter to you of March 29, 2000. To clarify our authority on those areas where questions have arisen, I am sending this letter, which, for future ease of reference, adds to and recapitulates some of the text of previous correspondence.**

**In your visits to our offices and in your correspondence, you have raised several questions about the United States Federal Trade Commission's authority in the online privacy area. I thought it would be useful to summarize my prior responses and to provide additional information about the agency's jurisdiction over consumer privacy issues raised in your most recent letter. Specifically, you ask whether: (1) the FTC has jurisdiction over transfers of employment-related data if done in violation of the U.S. safe harbor principles; (2) the FTC has jurisdiction over non-profit privacy "seal" programs; (3) the FTC Act applies equally to the offline as well as online world; and (4) what happens when the FTC's jurisdiction overlaps with other law enforcement agencies.**

### **FTC Act Application to Privacy**

**The Federal Trade Commission's legal authority in this area is found in**

**Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits "unfair or deceptive acts or practices" in or affecting commerce.**

**(1) A deceptive practice is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion. A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition.<sup>(2)</sup>**

**Certain information collection practices are likely to violate the FTC Act. For example, if a web site falsely claims to comply with a stated privacy policy or a set of self-regulatory guidelines, Section 5 of the FTC Act provides a legal basis for challenging such a misrepresentation as deceptive. Indeed, we have successfully enforced the law to establish this principle.<sup>(3)</sup> In addition, the Commission has taken the position it may challenge particularly egregious privacy practices as unfair under Section 5 if such practices involve children, or the use of highly sensitive information, such as financial records<sup>(4)</sup> and medical records. The Federal Trade Commission has and will continue to pursue such law enforcement actions through our active monitoring and investigative efforts, and through referrals we receive from self-regulatory organizations and others, including European Union member states.**

### Backstop Self-Regulation

The FTC will give priority to referrals of non-compliance with self-regulatory guidelines received from organizations such as BBOnline and TRUSTe.<sup>(5)</sup> This approach would be consistent with our longstanding relationship with the National Advertising Review Board (NARB) of the Better Business Bureau, which refers advertising complaints to the FTC. The National Advertising Division (NAD) of NARB resolves complaints, through an adjudicative process, concerning national advertising. When a party refuses to comply with an NAD decision, a referral is made to the FTC. FTC staff reviews the challenged advertising on a priority basis to determine if it violates the FTC Act, and often is successful in stopping the challenged conduct or convincing the party to return to the NARB process.

Similarly, the FTC will give priority to referrals of non-compliance with safe harbor principles from EU member states. As with referrals from U.S. self-regulatory organizations, our staff will consider any information bearing upon whether the conduct complained of violates Section 5 of the FTC Act. This commitment can also be found in the safe harbor principles under the Frequently Asked Question

(FAQ 11) on enforcement.

### GeoCities: The FTC's First Online Privacy Case

The Federal Trade Commission's first Internet privacy case, GeoCities, was based on the Commission's authority under Section 5.<sup>(6)</sup> In that case, the FTC alleged that GeoCities misrepresented, both to adults and children, how their personal information would be used. The Federal Trade Commission's complaint alleged that GeoCities represented that certain personal identifying information it collected on its Web site was to be used only for internal purposes or to provide consumers with the specific advertising offers and products or services they requested, and that certain additional "optional" information would not be released to anyone without the consumer's permission. In fact, this information was disclosed to third parties who used it to target members for solicitations beyond those agreed to by the member. The complaint also charged that GeoCities engaged in deceptive practices relating to its collection of information from children. According to the FTC's complaint, GeoCities represented that it operated a children's area on its Web site and that the information collected there was maintained by GeoCities. In fact, those areas on the Web site were run by third-parties who collected and maintained the information.

The settlement prohibits GeoCities from misrepresenting the purpose for which it collects or uses personal identifying information from or about consumers, including children. The order requires the company to post on its Web site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, the settlement also requires GeoCities to obtain parental consent before collecting personal identifying information from children 12 and under. Under the order, GeoCities is required to notify its members and provide them with an opportunity to have their information deleted from GeoCities' and any third parties' databases. The settlement specifically requires GeoCities to notify the parents of children 12 and under and to delete their information, unless a parent affirmatively consents to its retention and use. Finally, GeoCities also is required to contact third parties to whom it previously disclosed the information and request that those parties delete that information as well.<sup>(7)</sup>

### ReverseAuction.com

In January 2000, the Commission approved a complaint against, and consent agreement with, ReverseAuction.com, an online auction site that allegedly obtained consumers' personally identifying information from a competitor site (eBay.com) and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business.<sup>(8)</sup> Our complaint alleged that ReverseAuction violated Section 5 of the FTC Act in obtaining the personally identifiable information, which included eBay users' e-mail addresses and personalized user identification names ("user IDs"), and in sending out the deceptive e-mail messages.

As described in the complaint, before obtaining the information, ReverseAuction registered as an eBay user and agreed to comply with eBay's User Agreement and Privacy Policy. The agreement and policy protect consumers' privacy by prohibiting eBay users from gathering and using personal identifying information for unauthorized purposes, such as sending unsolicited commercial e-mail messages. Thus, our complaint first alleged that ReverseAuction misrepresented that it would comply with eBay's User Agreement and Privacy Policy, a deceptive practice under Section 5. In the alternative, the complaint alleged that ReverseAuction's use of the information to send the unsolicited commercial e-mail, in violation of the User Agreement and Privacy Policy, was an unfair trade practice under Section 5.

Second, the complaint alleged that the e-mail messages to consumers contained a deceptive subject line informing each of them that his or her eBay user ID "will expire soon." Finally, the complaint alleged that the e-mail messages falsely represented that eBay directly or indirectly provided ReverseAuction with eBay users' personally identifiable information, or otherwise participated in dissemination of the unsolicited e-mail.

The settlement obtained by the FTC bars ReverseAuction from committing these violations in the future. It also requires ReverseAuction to provide notice to consumers who, as a result of receiving ReverseAuction's e-mail, registered or will register with ReverseAuction. The notice informs these consumers that their eBay users IDs were not about to expire on eBay, and that eBay did not know of, or authorize, ReverseAuction's dissemination of the unsolicited e-mail. The notice also provides these consumers with the opportunity to cancel registration with ReverseAuction and have their personal identifying information deleted from ReverseAuction's database. In addition, the order requires ReverseAuction to delete, and refrain from using or disclosing, the personal identifying information of eBay members who received ReverseAuction's e-mail but who have not registered with ReverseAuction. Finally, consistent with prior privacy orders obtained by this agency, the settlement requires ReverseAuction to disclose its own privacy policy on its Internet site, and contains comprehensive record keeping provisions to allow the FTC to monitor compliance.

The ReverseAuction case demonstrates that the FTC is committed to using enforcement to buttress industry self-regulatory efforts in the area of online consumer privacy. Indeed, this case directly challenged conduct that undermined a Privacy Policy and User Agreement protecting consumers' privacy, and that could erode consumer confidence in privacy measures undertaken by online companies. Because this case involved the misappropriation by one company of consumer information protected by another company's privacy policy, it also may have particular relevance to the privacy concerns raised by the transfer of data between companies in different countries.

Notwithstanding the Federal Trade Commission's law enforcement actions in GeoCities, Liberty Financial Cos., and ReverseAuction, the agency's authority in some areas of online privacy is more limited. As noted above, to be reachable under the FTC Act, the collection and use of personal

information without consent must constitute either a deceptive or unfair trade practice. Thus, the FTC Act likely would not address the practices of a Web site that collected personally identifiable information from consumers, but neither misrepresented the purpose for which the information was collected, nor used or released the information in a way that was likely to cause substantial injury to consumers. Also, it currently may not be within the FTC's power to broadly require that entities collecting information on the Internet adhere to a privacy policy or to any particular privacy policy.<sup>(9)</sup> As stated above, however, a company's failure to abide by a stated privacy policy is likely to be a deceptive practice.

Furthermore, the FTC's jurisdiction in this area covers unfair or deceptive acts or practices only if they are "in or affecting commerce." Information collection by commercial entities that are promoting products or services, including collecting and using information for commercial purposes, would presumably meet the "commerce" requirement. On the other hand, many individuals or entities may be collecting information online without any commercial purpose, and thereby may fall outside the Federal Trade Commission's jurisdiction. An example of this limitation involves "chat rooms" if operated by noncommercial entities, *e.g.*, a charitable organization.

Finally, there are a number of full or partial statutory exclusions from the FTC's basic jurisdiction over commercial practices that limit the FTC's ability to provide a comprehensive response to Internet privacy concerns. These include exemptions for many information intensive consumer businesses such as banks, insurance companies and airlines. As you are aware, other federal or state agencies would have jurisdiction over those entities, such as the federal banking agencies or the Department of Transportation.

In cases where it does have jurisdiction, the FTC accepts and, resources permitting, acts on consumer complaints received by mail and telephone in its Consumer Response Center ("CRC") and, more recently, on its Web site.<sup>(10)</sup> The CRC accepts complaints from all consumers, including those residing in European Union member states. The FTC Act provides the Federal Trade Commission equitable power to obtain injunctive relief against future violations of the FTC Act, as well as redress for injured consumers. We would, however, look to see whether the company has engaged in a pattern of improper conduct, as we do not resolve individual consumer disputes. In the past, the Federal Trade Commission has provided redress for citizens of both the United States and other countries.<sup>(11)</sup> The FTC will continue to assert its authority, in appropriate cases, to provide redress to citizens of other countries who have been injured by deceptive practices under its jurisdiction.

### Employment Data

Your most recent letter sought additional clarification concerning the FTC's jurisdiction in the area of employment data. First, you pose the question whether the FTC could take action under Section 5 against a company that represents it complies with U.S. safe harbor principles but transfers or uses employment-related data in a manner that violates these principles. We want to assure you that we

have carefully reviewed the FTC authorizing legislation, related documents, and relevant case law and have concluded that the FTC has the same jurisdiction in the employment-related data situation as it would generally under Section 5 of the FTC Act.<sup>(12)</sup> That is to say, assuming a case met our existing criteria (unfairness or deception) for a privacy-related enforcement action, we could take action in the employment-related data situation.

We also would like to dispel any view that the FTC's ability to take privacy-related enforcement action is limited to situations where a company has deceived individual consumers. In fact, as the Commission's recent action in the ReverseAuction<sup>(13)</sup> matter makes clear, the FTC will bring privacy-related enforcement actions in situations involving data transfers between companies, where one company allegedly has acted unlawfully vis a vis another company, leading to possible injury to both consumers and companies. We expect this situation is the one in which the employment issue is most likely to arise, as employment data about Europeans is transferred from European companies to American companies that have pledged to abide by the safe harbor principles.

We do wish to note one circumstance in which FTC action would be circumscribed, however. This would occur in situations in which the matter is already being addressed in a traditional labor law dispute resolution context, most likely a grievance/arbitration claim or an unfair labor practice complaint at the National Labor Relations Board. This would occur, for example, if an employer had made a commitment in a collective bargaining agreement regarding the use of personal data and an employee or union claimed that the employer had breached that agreement. The Commission would likely defer to that proceeding.<sup>(14)</sup>

### Jurisdiction Over "Seal" Programs

Second, you ask whether the FTC would have jurisdiction over "seal" programs administering dispute resolution mechanisms in the United States that misrepresented their role in enforcing the "safe harbor" principles and handling individual complaints, even if such entities were technically "not for profit." In determining whether we have jurisdiction over an entity that holds itself out as a non-profit, the Commission closely analyzes whether the entity, while not seeking a profit for itself, furthers the profit of its members. The Commission has successfully asserted jurisdiction over such entities and as recently as May 24, 1999, the United States Supreme Court, in California Dental Association v. Federal Trade Commission, unanimously affirmed the Commission's jurisdiction over a voluntary nonprofit association of local dental societies in an antitrust matter. The Court held:

The FTC Act is at pains to include not only an entity "organized to carry on business for its own profit," 15 U. S. C. §44, but also one that carries on business for the profit "of its members." . . . . It

could, indeed, hardly be supposed that Congress intended such a restricted notion of covered supporting organizations, with the opportunity this would bring with it for avoiding jurisdiction where the purposes of the FTC Act would obviously call for asserting it.

In sum, determining whether to assert jurisdiction over a particular "non-profit" entity administering a seal program would require a factual review of the extent to which the entity provided economic benefit to its for-profit members. If such an entity operated its seal program in a manner that provided an economic benefit to its members, the FTC likely would assert its jurisdiction. As a separate point, the FTC likely would have jurisdiction over a fraudulent seal program that misrepresents its status as a non-profit entity.

### Privacy in the Offline World

Third, you note that our prior correspondence has focused on privacy in the online world. While online privacy has been a major concern of the FTC as a critical component to the development of electronic commerce, the FTC Act dates back to 1914 and applies equally in the offline world. Thus, we can pursue offline firms that engage in unfair or deceptive trade practices with regard to consumers' privacy.<sup>(15)</sup> In fact, in a case brought by the Commission last year, FTC v. TouchTone Information, Inc.,<sup>(16)</sup> an "information broker" was charged with illegally obtaining and selling consumers' private financial information. The Commission alleged that Touch Tone obtained consumers' information by "pretexting," a term of art coined by the private investigation industry to describe the practice of getting personal information about others under false pretenses, typically on the telephone. The case, filed April 21, 1999, in federal court in Colorado, seeks an injunction and all illegally gained profits.

This law enforcement experience, as well as recent concerns about the merging of offline and online databases, the blurring of distinctions between online and offline merchants, and the fact that a vast amount of personal identifying information is collected and used offline, make clear that significant attention to offline privacy issues is warranted.

### Overlapping Jurisdiction

Finally, you pose the question of the interplay of the FTC's jurisdiction with that of other law enforcement agencies, particularly in cases where there is potentially overlapping jurisdiction. We have developed strong working relationships with numerous other law enforcement agencies, including the federal banking agencies and the state attorneys general. We very often coordinate investigations to maximize our resources in instances of overlapping jurisdiction. We also often refer matters to the appropriate federal or state agency for investigation.

I hope this review is helpful. Please let me know if you need any further information.

Sincerely,

Robert Pitofsky

1. 15 U.S.C. § 45. The Fair Credit Reporting Act would also apply to Internet data collection and sales that meet the statutory definitions of "consumer report" and "consumer reporting agency."
2. 15 U.S.C. § 45(n).
3. See GeoCities, Docket No. C-3849 (Final Order Feb. 12, 1999) (available at [www.ftc.gov/os/1999/9902/9823015d%26o.htm](http://www.ftc.gov/os/1999/9902/9823015d%26o.htm)); Liberty Financial Cos., Docket No. C-3891 (Final Order Aug. 12, 1999) (available at [www.ftc.gov/opa/1999/9905/younginvestor.htm](http://www.ftc.gov/opa/1999/9905/younginvestor.htm)). See also Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Part 312 (available at [www.ftc.gov/opa/1999/9910/childfinal.htm](http://www.ftc.gov/opa/1999/9910/childfinal.htm)). The COPPA Rule, which became effective last month, requires operators of Web sites directed to children under 13, or who knowingly collect personal information from children under 13, to implement the fair information practice standards enunciated in the Rule.
4. See FTC v. Touch Tone, Inc., Civil Action No. 99-WM-783 (D.Co.) (filed April 21, 1999) at [www.ftc.gov/opa/1999/9904/touchtone.htm](http://www.ftc.gov/opa/1999/9904/touchtone.htm). Staff Opinion Letter, July 17, 1997, issued in response to a petition filed by the Center for Media Education, at [www.ftc.gov/os/1997/9707/cenmed.htm](http://www.ftc.gov/os/1997/9707/cenmed.htm).
5. Indeed, the FTC recently filed a complaint in federal district court against a TRUSTe sealholder, Toysmart.com, seeking injunctive and declaratory relief to prevent the sale of confidential, personal customer information collected on the company Web site in violation of its own privacy policy. The FTC learned of this possible law violation directly from TRUSTe. FTC v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS (D.Ma.) (filed July 11, 2000) (available at [www.ftc.gov/opa/2000/07/toysmart.htm](http://www.ftc.gov/opa/2000/07/toysmart.htm)).
6. GeoCities, Docket No. C-3849 (Final Order Feb. 12, 1999) (available at [www.ftc.gov/os/1999/9902/9823015d%26o.htm](http://www.ftc.gov/os/1999/9902/9823015d%26o.htm)).
7. The Commission subsequently settled another matter involving the collection of personal information from children online. Liberty Financial Companies, Inc., operated the Young Investor website which was directed to children and teens, and focused on issues relating to money and investing. The Commission alleged that the site falsely represented that personal information collected from children in a survey would be maintained anonymously, and that participants would be sent an e-mail newsletter as well as prizes. In fact, the personal information about the child and the family's finances was maintained in an identifiable manner, and no newsletter or prizes were sent. The consent agreement prohibits such misrepresentations in the future and requires Liberty Financial to post a



privacy notice on its children's sites and obtain verifiable parental consent before collecting personal identifying information from children. Liberty Financial Cos., Docket No. C-3891 (Final Order Aug. 12, 1999) (available at [www.ftc.gov/opa/1999/9905/younginvestor.htm](http://www.ftc.gov/opa/1999/9905/younginvestor.htm)).

8. See ReverseAuction.com, Inc., Civil Action No. 000032 (D.D.C.) (filed January 6, 2000) (press release and pleadings at [www.ftc.gov/opa/2000/01/reverse4.htm](http://www.ftc.gov/opa/2000/01/reverse4.htm)).

9. For this reason, the Federal Trade Commission stated in Congressional testimony that additional legislation probably would be required to mandate that all U.S. commercial Web sites directed toward consumers abide by specified fair information practices. "Consumer Privacy on the World Wide Web," Before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, July 21, 1998 (the testimony can be found at [www.ftc.gov/os/9807/privac98.htm](http://www.ftc.gov/os/9807/privac98.htm)). The FTC deferred calling for such legislation in order to give self-regulatory efforts the opportunity to demonstrate widespread adoption of fair information practices on Web sites. In the Federal Trade Commission's report to Congress on online privacy, "Privacy Online: A Report to Congress," June 1998 (the report can be found at [www.ftc.gov/reports/privacy3/toc.htm](http://www.ftc.gov/reports/privacy3/toc.htm)), the FTC recommended legislation to require that commercial Web sites obtain parental consent before collecting personally identifiable information from children under 13 years old. See footnote 3 *supra*. Last year, the FTC's report, "Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress," July 1999 (the report can be found at [www.ftc.gov/os/1999/9907/index.htm#13](http://www.ftc.gov/os/1999/9907/index.htm#13)), found sufficient progress in self-regulation and, accordingly, chose not to recommend legislation at that time.

In May 2000, the Commission issued a third report to Congress, "Privacy Online: Fair Information Practices in the Electronic Marketplace," (the report can be found at [www.ftc.gov/os/2000/05/index.htm#22](http://www.ftc.gov/os/2000/05/index.htm#22)) which discusses the FTC's recent survey of commercial Web sites and their compliance with fair information practices. The report also recommended (by a majority of the Commission) that Congress enact legislation that would set forth a basic level of privacy protection for consumer-oriented commercial Web sites.

10. See <https://www.ftc.gov/ftc/complaint.htm> for the Federal Trade Commission's online complaint form.

11. For example, in a recent case involving an Internet pyramid scheme, the Commission obtained refunds for 15,622 consumers totaling approximately \$5.5 million. The consumers resided in the United States and 70 foreign countries. See [www.ftc.gov/opa/9807/fortunar.htm](http://www.ftc.gov/opa/9807/fortunar.htm); [www.ftc.gov/opa/9807/ftcrefund01.htm](http://www.ftc.gov/opa/9807/ftcrefund01.htm).

12. Except as specifically excluded by the FTC's authorizing statute, the FTC's jurisdiction under the FTC Act over practices "in or affecting commerce" is coextensive with the constitutional power of Congress under the Commerce Clause, United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). The FTC's jurisdiction would thus encompass employment-related practices in firms and industries in international commerce.

13. See "Online Auction Site Settles FTC Privacy Charges," FTC News Release (Jan. 6, 2000),

available at <http://www.ftc.gov/opa/2000/01/reverse4.htm>.

14. The determination whether conduct is an "unfair labor practice" or a violation of a collective bargaining agreement is a technical one that is ordinarily reserved to the expert labor tribunals who will hear the complaints, such as arbitrators and the NLRB.

15. As you know from earlier discussions, the Fair Credit Reporting Act also gives the FTC the authority to protect consumers' financial privacy within the purview of the Act and the Commission recently issued a decision pertaining to this issue. *See In the Matter of Trans Union*, Docket No. 9255 (March 1, 2000) (press release and opinion available at [www.ftc.gov/os/2000/03/index.htm#1](http://www.ftc.gov/os/2000/03/index.htm#1)).

16. Civil Action 99-WM-783 (D.Colo.)(available at <http://www.ftc.gov/opa/1999/9904/touhtone.htm>) (tentative consent decree pending).