

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES



In the Matter of)
)
)

BASIC RESEARCH, L.L.C.,)
A.G. WATERHOUSE, L.L.C.,)
KLEIN-BECKER USA, L.L.C.,)
NUTRASPORT, L.L.C.,)
SOVAGE DERMALOGIC LABORATORIES, L.L.C.,)
d/b/a BASIC RESEARCH, L.L.C.,)
OLD BASIC RESEARCH, L.L.C.,)
BASIC RESEARCH, A.G. WATERHOUSE,)
BAN, L.L.C.,)
d/b/a KLEIN-BECKER USA, NUTRA SPORT, and)
SOVAGE DERMALOGIC LABORATORIES,)
DENNIS GAY,)
DANIEL B. MOWREY,)
d/b/a AMERICAN PHYTOTHERAPY RESEARCH)
LABORATORY, and)
MITCHELL K. FRIEDLANDER)

PUBLIC

DOCKET NO. 9318

**REPLY TO COMPLAINT COUNSEL'S PARTIAL AND SUPPLEMENTAL
RESPONSES TO RESPONDENTS' EMERGENCY MOTION REQUIRING THE
COMMISSION TO PROVIDE RESPONDENTS WITH ELECTRONIC FILES AND
REQUEST FOR EXPEDITED RULING**

Respondents Basic Research, LLC, and Ban, LLC, (collectively "Respondents"), pursuant to this Court's request made on March 1, 2005, hereby submit their Reply¹ to Complaint Counsel's Partial and Supplemental Responses to Respondents' Emergency Motion requiring the Commission to immediately produce to Respondents all electronic files² that show who accessed Respondents' confidential information while it was improperly and illegally

¹ This Reply only addresses Respondents' entitlement to the electronic files that show who accessed Respondents' confidential information during the time that Complaint Counsel had it posted on the FTC's Website. Respondents will soon be filing a Motion for Order to Show Cause that directly addresses the merits of this egregious breach of the Protective Order.

² A sample of an electronic file that would provide such information, obtained from the FTC's website at <http://www.ftc.gov/ftc/logfile.htm>, is attached hereto as Exhibit A.

posted on the FTC's website, www.ftc.gov ("FTC Website"). Due to the continuing harm that Respondents suffer with each day that passes, Respondents also respectfully request that this Court issue an Order on this matter on an expedited basis. In support thereof, Respondents state as follows:

I. INTRODUCTION AND RELEVANT BACKGROUND

Complaint Counsel violated the Protective Order entered in this case when Complaint Counsel posted Respondents' highly confidential information on the FTC's website. Respondents immediately brought this breach to the Court's attention on February 18, 2005, when Respondents filed their Emergency Motion Requiring the Commission to Provide Respondents with Electronic Files Showing Who Accessed Respondents' Confidential Information While It Was on the Commission's Website ("Emergency Motion"). Complaint Counsel provided a Partial Response to the Emergency Motion on February 18, 2005 ("Partial Response") and a Supplemental Response to the Emergency Motion ("Supp. Response") (collectively, "Responses"), with supporting declarations of Lauren Kapin, Joshua Millard, and James Reilly Dolan, on February 25, 2005. On March 1, 2004, this Court invited Respondents to submit a Reply in order to address the issues raised in Complaint Counsel's Responses. We now respond.

Foremost, Complaint Counsel should not be able to take refuge in the FTC's internet privacy policy in order to shield the identities of third parties who acquired or viewed Respondents' confidential information on the FTC's website. While Respondents appreciate the FTC's professed respect for the privacy of internet users, the paramount interest here must be the protection of Respondents' confidential information as protecting third parties' privacy in this case will only elevate and enhance the harm Respondents have already suffered as a result of the

FTC's wrongful disclosures.³ Under the Uniform Trade Secrets Act ("UTSA"), a party who material changes its position after it acquires another's trade secrets without reason to know that they have been acquired wrongfully will not be held liable for the misappropriation. *See* UTSA, § 1(2)(ii)(C) (2005). Further, an injunction against such a person may be denied and Respondents may only be able to obtain a reasonable royalty for the continued use of their trade secrets. *Id.* § 2(b) (2005). Thus, Respondents have an affirmative duty to notify all persons who accessed Respondents' confidential information on the FTC's website that such information was wrongfully disclosed and is confidential. If the Court denies this Emergency Motion, people who acquired Respondents' information from the FTC's website will be able to use it with impunity as Respondents have no alternative means of discovering their identities. Accordingly, this Emergency Motion is Respondents' last and only chance to stop the misuse of their confidential information.

II. ARGUMENT

A. Respondents' Right to Protect Their Trade Secrets Trumps the FTC's Privacy Policy

Complaint Counsel asserts that the FTC cannot provide Respondents with the requested web logs because disclosing the identity of the people who accessed Respondents' confidential documents would violate the FTC's privacy policy.⁴ *Supp. Response*, p. 4. The FTC's website contains a privacy policy that provides, in relevant part,

We [the FTC] automatically collect and store: the name of the domain and host from which you [a person who accesses the FTC website] access the Internet; the Internet protocol (IP) address of the computer you are using; the browser software you use and your

³ Compare Declaration of Joshua Millard, Attachment B to *Supp. Response*, at ¶ 13 (wherein Mr. Millard admitted that he "filed the Motion [Complaint Counsel's Motion for Partial Summary Decision] and its exhibits, and the Statement, in electronic files via email...") with Rule of Practice 4.2(c)(3) ("the electronic copy of each such document containing *in camera* or otherwise confidential material shall be placed on a diskette so labeled, which shall be physically attached to the paper original, and not transmitted by e-mail") (emphasis added).

⁴ A copy of the FTC's privacy policy was attached to the Declaration of Lauren Kapin as Exhibit 2.

operating system; the date and time you access our sites; and the Internet address of the site from which you linked directly to our sites.

We use this information only as anonymous aggregate data to determine the number of visitors to different sections of our sites, to ensure the sites are working properly, and to help us make our sites more useful. We do not use it to track or record information about individuals.

This broad, aspirational statement does not vest any rights in computer users who access the FTC website. Website owners cannot be held liable for breach of contract by disclosing information in a manner contrary to the statements contained in the website's privacy policy. *See Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) ("broad statements of company policy do not generally give rise to contract claims"); *In re Northwest Airlines Privacy Litig.*, No. Civ. 04-126, 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) ("general statements of policy are not contractual").⁵

After September 11, 2001, the National Aeronautical and Space Administration ("NASA") requested passenger data over a three month period from Northwest Airlines in order to conduct research on airline security. *Dyer*, 334 F. Supp. 2d at 1197. Northwest Airlines provided NASA with the requested data, which included passengers' names, addresses, credit card numbers, and travel itineraries. *Id.* This disclosure resulted in multiple lawsuits brought by the passengers, including eight class actions. *Id.* The passengers asserted that Northwest Airlines' disclosure violated their privacy rights and also constituted a breach of contract based on the statements contained in the privacy policy on the Northwest Airlines website. *Id.* Northwest Airlines' privacy policy provided, in relevant part, "When you reserve or purchase travel services through Northwest Airlines nwa.com Reservations, we provide only the relevant

⁵ These two cases are part of the flood of litigation that resulted when Northwest Airlines disclosed passenger data to NASA following September 11, 2001. In order to better understand the court's holding in *Dyer*, the facts underlying the disclosure are taken from both cases.

information required by the car rental agency, hotel, or other involved third party to ensure the successful fulfillment of your travel arrangements.” *In re Northwest Airlines Privacy Litig.*, 2004 WL 1278459 at * 5. The court in *Dyer* held that “broad statements of company policy do not generally give rise to contract claims. As such, the alleged violation of the privacy policy at issue does not give rise to a contract claim.” *Dyer*, 334 F. Supp. 2d at 1200.

Like Northwest Airlines’ privacy policy, the FTC’s privacy policy does not vest any contractual or similar rights in the people who accessed Respondents’ information on the FTC’s website; thus, there is no legal or equitable reason to shield the identity of these people from Respondents.

B. Lack of an *In Camera* Order Has No Relevance to Respondents’ Request for Electronic Files

Complaint Counsel’s suggestion that it be allowed to withhold its web logs until the Court determines whether Respondents’ documents merit *in camera* status is specious. First, whether or not the Court ultimately grants *in camera* status to Respondents’ documents does not alter the fact that Respondents’ documents are *currently* confidential under the Protective Order. Indeed, Rule of Practice § 3.45(e) provides, in relevant part,

If a party includes specific information that has been granted *in camera* status pursuant to §3.45(b) or is subject to confidentiality protections pursuant to a protective order in any document filed in a proceeding under this part, the party shall file two versions of the document. A complete version shall be marked “In Camera” or “Subject to Protective Order,” as appropriate, on the first page and shall be filed with the Secretary and served by the party on the other parties in accordance with the rules in this part.

(emphasis added). Complaint Counsel’s embossment of “Subject to Protective Order” on the cover pages to its Motion for Summary Decision and related exhibits indicates that Complaint Counsel understood this Rule and its applicability to Respondents’ materials. Thus, Complaint Counsel always understood that Respondents’ documents were confidential. Had Complaint

Counsel believed otherwise, it would not have filed its Motion for Summary Decision with the legend: “Subject to Protective Order.” Nor is it inevitable that Respondents’ documents will ever become public because the parties are currently in the process of negotiating factual stipulations that may eliminate the need for these documents to be introduced into evidence, which would then negate any need for an *in camera* order.

In *Trans Union*, while the FTC did indicate that the respondents in that case should have sought *in camera* treatment of confidential materials at the time they filed their opposition to the FTC’s motion for summary decision, the FTC did not allow a unilateral disclosure of respondents’ confidential information. See *In re Trans Union Corp.*, No. 9255, 1993 FTC LEXIS 310, at *6 (Nov. 3, 1993). To the contrary, the FTC specifically recognized “the serious issues underlying the protection of confidential commercial or financial information[,] the disclosure of which could cause ‘clearly defined serious injury’....” *Id.* at *5, n.4. Because of the “serious injury” that can result from the disclosure of a party’s confidential information, the Commission remanded the respondents’ motion for *in camera* treatment to the Administrative Law Judge assigned to the case for consideration of the merits of the respondents’ motion. *Id.* at *6. In no way does *Trans Union* hold that Respondents’ failure to seek *in camera* status of materials submitted “in evidence” as exhibits to a motion for summary decision or opposition thereto grants Complaint Counsel carte blanche to disclose the confidential information to whomever it pleases. Rather, *Trans Union* indicates that, while a respondent should seek *in camera* status of materials that are to be offered into evidence, failure to do so does not necessarily waive the respondent’s right to seek such protective status at a later time.

In *Dura Lube*, respondents sought *in camera* treatment for the non-public version of Complaint Counsel’s motion for partial summary decision and accompanying memorandum of

law and exhibits, and portions of respondents' opposition to the motion for partial summary decision with corresponding exhibits. See *In re Dura Lube Corp.*, Docket No. 9292, Order on Requests for *In Camera* Treatment, at 5 (Dec. 23, 1999).⁶ The Court in *Dura Lube* did not deny the respondents' request for *in camera* treatment of their documents due to a failure to meet the substantive requirements for *in camera* treatment. Rather, the Court found that the respondents' request for *in camera* treatment did not meet the requirements set forth in the Rules of Practice and in the scheduling order entered in that case. *Id.* at 2. Further, the Court did not deny the request with prejudice, but expressly granted respondents the ability to re-file their request for *in camera* treatment within a specified time in order to allow respondents the opportunity to comply with the applicable procedural rules. *Id.* at 5 ("Respondents shall refile their application for *in camera* treatment in accordance with the standards set forth in Rule 3.45(b) and this Order by January 14, 2000, or expressly withdraw their request by way of pleading.") Thus, the Court in *Dura Lube* did not deny respondents' request for *in camera* treatment based on a substantive lacking in respondents' request, and may have subsequently granted *in camera* treatment as requested; this Order merely required respondents to re-submit their request in the proper technical format with supporting affidavits. *Id.*

The fact that Respondents have not yet sought an *in camera* order protecting the confidential status of their documents has no relevance to the public disclosure that has already occurred or Respondents' request for the FTC's web logs in the Emergency Motion. Further, the language of the Protective Order stating that it "governs the disclosure of information during the course of discovery" neither excuses Complaint Counsel's posting of Respondents' confidential information on the FTC Website nor provides a reason for denying Respondents' request for electronic files.

⁶ A copy of the *Dura Lube* Order is attached hereto as Exhibit B.

C. Difficulties in Identifying Individuals Who Accessed Respondents' Confidential Information is Not Grounds for Denying Respondents' Request for Electronic Files

Complaint Counsel also suggest that an inspection of the FTC's web logs would not be fruitful because "internet service providers maintain a large number of IP addresses that are randomly assigned. In other words, a user may have different IP addresses assigned to them each time they log on." Supp. Response, at pp. 3-4. While it is true that some users of some internet service providers ("ISP's") are randomly assigned Internet protocol ("IP") addresses each time they log on, this is certainly not the case for every user of every ISP. In fact, the FTC's own website states, "Generally, users who have fixed Internet connections (cable modems, private companies, etc.) have fixed IP addresses. Dial-up Internet providers usually give addresses dynamically from a pool when a user dials in to connect (such as a pool of 100 IP addresses per 800 subscribers)." See Russ Smith, *The IP Address: Your Internet Identity* (March 29, 1997), available at www.ftc.gov/reports/privacy3/comments/005-cnet.htm (last accessed March 2, 2005). A copy of *The IP Address: Your Internet Identity* is attached hereto as Exhibit C. Any difficulties Respondents may face once they obtain the electronic files from the FTC are for Respondents to handle as they attempt to limit the harm caused by Complaint Counsel's improper disclosure of Respondents' confidential information.⁷ The possibility that such difficulties may arise is an insufficient basis to refuse Respondents' request for the FTC's web logs.

III. CONCLUSION

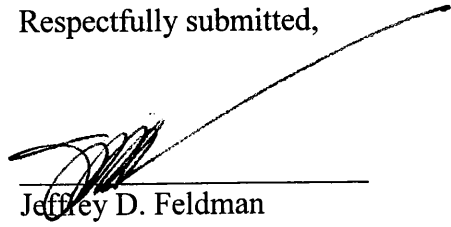
While Respondents' trade secrets have not lost their protected status due to Complaint Counsel's public disclosure of them, Respondents have an affirmative duty to seek out all

⁷ Further, Respondents will be able to issue subpoenas to ISP's in federal district court proceedings in order to compel the ISP's to divulge the name and address associated with each IP address.

persons who may have accessed their confidential information on the FTC's website and attempt to prevent any further disclosure or any misuse of that information. Respondents' sole chance of identifying persons who may possess Respondents' trade secrets lies with the FTC. Without the FTC's web logs, Respondents will never know who has and is using their confidential information and will be powerless to stop this continuing encroachment on their property rights. The FTC suggests that the privacy of third parties who viewed and/or downloaded Respondents' confidential information is paramount. Respondents beg to differ. Privacy, in this instance, would not only shield a wrong, but would allow it to continue. Therefore, Respondents respectfully request that this Court grant Respondents' Emergency Motion and require the FTC to provide Respondents with electronic files that contain sufficient information to allow Respondents to identify who accessed Respondents' confidential information.

Each day that passes increases the harm suffered by Respondents, harm that can only be remedied by acting quickly and attempting to prevent third parties from using Respondents' trade secrets. Therefore, Respondents also respectfully request that this Court issue an Order granting Respondents' Emergency Motion on an expedited basis.

Respectfully submitted,



Jeffrey D. Feldman
Todd M. Malynn
Gregory L. Hillyer
Christopher P. Demetriades

Feldman Gale, P.A.
Miami Center, 19th Floor
201 South Biscayne Blvd.
Miami, Florida 33131
Tel: (305) 358-5001
Fax: (305) 358-3309

**Attorneys for Respondents Basic Research, LLC,
A.G. Waterhouse, LLC, Klein-Becker USA,
LLC, Nutrasport, LLC, Söavage Dermalogic
Laboratories, LLC and Ban, LLC**

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was provided to the following parties this 3rd day of March, 2005 as follows:

(1) One (1) original and two (2) copies by Federal Express to Donald S. Clark, Secretary, Federal Trade Commission, Room H-159, 600 Pennsylvania Avenue, N.W., Washington, D.C., 20580;

(2) One (1) electronic copy via e-mail attachment in Adobe® “.pdf” format to the Secretary of the FTC at Secretary@ftc.gov;

(3) Two (2) copies by Federal Express to Administrative Law Judge Stephen J. McGuire, Federal Trade Commission, Room H-104, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580;

(4) One (1) copy via e-mail attachment in Adobe® “.pdf” format to Commission Complaint Counsel, Laureen Kapin, Joshua S. Millard, and Laura Schneider, all care of lkapin@ftc.gov, jmillard@ftc.gov; richardson@ftc.gov; lschneider@ftc.gov with one (1) paper courtesy copy via U. S. Postal Service to Laureen Kapin, Bureau of Consumer Protection, Federal Trade Commission, Suite NJ-2122, 600 Pennsylvania Avenue, N.W., Washington, D.C., 20580;

(5) One (1) copy via U. S. Postal Service to Elaine Kolish, Associate Director in the Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580

(6) One (1) copy via United States Postal Service to Stephen Nagin, Esq., Nagin Gallop & Figueredo, 3225 Aviation Avenue, Suite 301, Miami, Florida 33131.

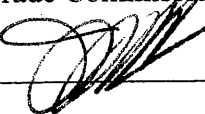
(7) One (1) copy via United States Postal Service to Richard Burbidge, Esq., Jefferson W. Gross, Esq. and Andrew J. Dymek, Esq., Burbidge & Mitchell, 215 South State Street, Suite 920, Salt Lake City, Utah 84111, Counsel for Dennis Gay.

(8) One (1) copy via United States Postal Service to Ronald F. Price, Esq., Peters Scofield Price, A Professional Corporation, 340 Broadway Centre, 111 East Broadway, Salt Lake City, Utah 84111, Counsel for Daniel B. Mowrey.

(9) One (1) copy via United States Postal Service to Mitchell K. Friedlander, 5742 West Harold Gatty Drive, Salt Lake City, Utah 84111, *Pro Se*.

CERTIFICATION FOR ELECTRONIC FILING

I HEREBY CERTIFY that the electronic version of the foregoing is a true and correct copy of the original document being filed this same day of March 3, 2005 via Federal Express with the Office of the Secretary, Room H-159, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.





RECYCLED PAPER



TO REORDER CALL 954-846-9399

FEDERAL TRADE COMMISSION



Privacy Policy for FTC Website

Sample Log File Entry Collected for Statistical Purposes

www.companyname.com - - [29/Jun/2000:13:36:21 -0400]
"GET /bcp/menu-auto.htm HTTP/1.0" 200 16245
"http://www.ftc.gov/ftc/consumer.htm" "Mozilla/4.72 [en] (Win95; U)"

www.companyname.com (or 123.456.78.90) - This is the host name (or IP address) associated with the requestor (visitor). In this case (.com), the requestor is coming from a commercial address. Depending on the requestor's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[29/Jun/2000:13:36:21 -0400] - This is the date and time of the request.

"GET /bcp/menu-auto.htm HTTP/1.0" - This is the location of the requested file

200 - This is the status code (200 = OK). In this instance the request was filled.

16245 - This is the file size (in bytes) of the requested file.

"http://www.ftc.gov/ftc/consumer.htm" - This indicates the last site (or page) the visitor visited, i.e., the site/page that referenced (linked to) the requested file.

"Mozilla/4.72 [en] (Win95; U)" -- This identifies the type of browser software (Netscape 4.72) used to access the page. This information tells the server what design parameters to use in constructing the page. This entry also indicates the visitor was using Windows 95 operating system.

[Contact Us](#) | [Search](#) | [Complaint Form](#) | [FOIA](#) | [Privacy](#) | [Site Map](#) | [Home](#)

Last Updated: Thursday, June 29, 2000



RECYCLED PAPER



TO REORDER CALL 954-846-9399

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
)
 DURA LUBE CORPORATION,)
 AMERICAN DIRECT MARKETING, INC.,)
 HOWE LABORATORIES, INC.,)
 CRESCENT MANUFACTURING, INC.,)
 NATIONAL COMMUNICATIONS CORPORATION)
 THE MEDIA GROUP, INC.,)
)
 corporations, and)
 HERMAN S. HOWARD, and)
 SCOTT HOWARD,)
)
 individually and as officers)
 of the corporations.)

Docket No. 9292

ORDER ON REQUESTS FOR *IN CAMERA* TREATMENT

I.

Before the Court is Respondents' Application for *In Camera* Treatment, filed December 17, 1999. In this motion, Respondents request *in camera* treatment of: (1) the "*in camera*" version of Complaint Counsel's Motion for Partial Summary Decision, Memorandum in Support thereof, and supporting exhibits, filed December 7, 1999; and (2) portions of Respondents' Opposition to the Motion for Partial Summary Decision and supporting exhibits, filed December 23, 1999. In an earlier pleading, Respondents' Request to Reply, Reply in Support of Motion to Exclude Witnesses and Request for In Camera Treatment of Complaint Counsel's Opposition, filed December 6, 1999, Respondents requested *in camera* treatment of materials contained in Complaint Counsel's Opposition to Respondent's Motion to Exclude Witnesses, filed December 3, 1999.

In the pretrial conferences in the instant case, the parties have been advised to comply with the procedures for requesting *in camera* treatment of materials to be submitted in pleadings. In addition, the parties have previously been instructed in the Order on Respondents' Motion to Exclude Witnesses, December 8, 1999:

Under the Commission's Rules of Practice, confidential material does not become "*in camera*" material until the Administrative Law Judge has granted it *in camera* status.

Commission Rule 3.45. The Pretrial Scheduling Order sets forth procedures which counsel must follow for confidential material to be granted *in camera* status.

According to Respondents, Complaint Counsel failed to provide Respondents with notice that Complaint Counsel intended to file or introduce Respondents' confidential materials prior to filing Complaint Counsel's Opposition to Respondents' Motion to Exclude Witnesses and its Motion for Partial Summary Decision. Despite Complaint Counsel's failure to follow the procedures contained in the Pretrial Scheduling Order, Respondents have attempted to comply with the Pretrial Scheduling Order by filing the pending Respondents' Application for *In Camera* Treatment. However, in order for Respondents' Application for *In Camera* Treatment to be considered, Respondents must strictly comply with the Commission's rules on *in camera* treatment.

Because Respondents' pending requests do not comply with the Commission's express rules on *in camera* treatment, they are DENIED WITHOUT PREJUDICE, as described herein.

II.

Pursuant to Commission Rule 3.45(b):

[t]he Administrative Law Judge may order material, or portions thereof, offered into evidence . . . to be placed *in camera* on a finding that their public disclosure will likely result in a clearly defined, serious injury to the person, partnership or corporation requesting their *in camera* treatment. . . . No material . . . may be withheld from the public record unless it falls within the scope of an order issued in accordance with this section, stating the date on which *in camera* treatment will expire, and including: (1) A description of the material; (2) A statement of the reasons for granting *in camera* treatment; and (3) A statement of the reasons for the date on which *in camera* treatment will expire.

16 C.F.R. § 3.45(b). Though the language of Rule 3.45(b) literally applies to information "offered into evidence," Rule 3.45(d) requires that "[p]arties shall not disclose information that has been granted *in camera* status pursuant to § 3.45(b) in the public version of proposed findings, briefs, or other documents." 16 C.F.R. § 3.45(d).

Respondents' Application for *In Camera* Treatment fails to specifically identify or describe the material for which they seek *in camera* treatment, fails to provide evidence to support reasons for granting materials *in camera* treatment, and fails to distinguish between material for which indeterminate *in camera* treatment is sought versus material for which *in camera* treatment for a specific time frame should be sought. A blanket *in camera* order for an entire pleading will not be granted. An application for *in camera* treatment should describe the materials for which *in camera* treatment is sought, provide reasons for granting such materials *in*

camera status, specify the time period for which *in camera* treatment is sought for each document, and attach as exhibits to the application the specific documents for which *in camera* treatment is sought. In addition, to sustain the burden of proof, an application must be supported by proper evidence, such as affidavits, to support all factual issues." See 16 C.F.R. § 3.43.

III.

The Federal Trade Commission strongly favors making available to the public the full record of its adjudicative proceedings to permit public evaluation of the fairness of the Commission's work, and to provide guidance to persons affected by its actions. *Crown Cork & Seal Co., Inc.*, 71 F.T.C. 1714, 1714-15 (1967); *H.P. Hood & Sons, Inc.*, 58 F.T.C. 1184, 1186 (1961) ("[T]here is a substantial public interest in holding all aspects of adjudicative proceedings, including the evidence adduced therein, open to all interested persons."). See also *RSR Corp.*, 88 F.T.C. 734 (1976), in which the Commission explained:

One reason for the requirement that proceedings of this sort be decided "on the record" is to permit the public to evaluate the fairness and wisdom with which the decisions of public agencies have been made, and to permit affected parties to draw guidance from those decisions in determining their future conduct. . . . [I]n *camera* treatment of certain relevant information may be appropriate where the prospective injury from disclosure outweighs the public interest in full knowledge.

Id. at 734-35.

To clarify, all applications for *in camera* treatment will be evaluated by the standards set forth in Rule 3.45(b) and described in this Order. "The party seeking *in camera* treatment must make a clear showing that 'the information concerned is sufficiently secret and sufficiently material to [its] business that disclosure would result in serious competitive injury.'" *Volkswagen of America, Inc.*, 103 F.T.C. 536, 538 (1984) (quoting *General Foods Corp.*, 95 F.T.C. 352, 355 (1980)); *Hood*, 58 F.T.C. at 1188 (applicant has burden of showing "that the public disclosure . . . will result in a clearly defined, serious injury to the person or corporation whose records are involved"). Whenever an applicant seeks *in camera* treatment, it should demonstrate the necessity thereof by "using the most specific information available." *Bristol-Myers Co.*, 90 F.T.C. 455, 457 (1977).

In *Bristol-Myers*, the Commission outlined six factors to be weighed when determining materiality and secrecy: (1) the extent to which the information is known outside of the applicant's business; (2) the extent to which the information is known by employees and others involved in the applicant's business; (3) the extent of measures taken by the applicant to guard the secrecy of the information; (4) the value of the information to the applicant and its competitors; (5) the amount of effort or money expended by the applicant in developing the information; and (6) the ease or difficulty with which the information could be properly acquired

or duplicated by others. *Bristol-Myers*, 90 F.T.C. at 456-57. The likely loss of business advantages is a good example of a "clearly defined, serious injury." *General Foods*, 95 F.T.C. at 355. To warrant *in camera* treatment, an application must include a complete analysis and evidence in support of these factors.

A determination that information should be accorded *in camera* treatment does not end the inquiry. The next step is to determine the duration for which material will be held *in camera*. Again, the applicant has the burden of proof on this issue. In making this determination, the distinction between trade secrets and ordinary business records is important since ordinary business records are granted less protection than trade secrets. *See Hood*, 58 F.T.C. at 1189. "Trade secrets" are primarily limited to secret formulas, processes, and other secret technical information. *Hood*, 58 F.T.C. at 1189; *General Foods*, 95 F.T.C. at 352. "Ordinary business records" includes names of customers, prices to certain customers, and costs of doing business and profits. *Hood*, 58 F.T.C. at 1189. (Although Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. § 46(f), prohibits the Commission from publishing "trade secrets and names of customers," this provision does not apply to adjudicative proceedings. *Hood*, 58 F.T.C. at 1185, 1186 n.1).

Applicants seeking indefinite *in camera* treatment must demonstrate "at the outset that the need for confidentiality of the material is not likely to decrease over time." *E.I. DuPont de Nemours & Co.*, 1990 FTC LEXIS 134, *2 (April 25, 1990)(quoting 54 Fed. Reg. 49,279 (1989)). Commission Rule 3.45(b)(3) requires:

[An] expiration date [for an *in camera* order] may not be omitted except in unusual circumstances, in which event the order shall state with specificity the reasons why the need for confidentiality of the material, or portion thereof at issue is not likely to decrease over time, and any other reasons why such material is entitled to *in camera* treatment for an indeterminate period.

16 C.F.R. § 3.45(b)(3). The applicant has the burden of proof to demonstrate these "unusual circumstances." Accordingly, requests for indefinite *in camera* treatment must include evidence to provide justification as to why the document should be withheld from the public's purview in perpetuity and why the requestor believes the information is likely to remain sensitive or become more sensitive with the passage of time. *See DuPont*, 1990 FTC LEXIS 134 at *2.

In addition, there is a presumption that *in camera* treatment will not be provided to information that is three or more years old. *See, e.g., General Foods*, 95 F.T.C. at 353; *Crown Cork & Seal*, 71 F.T.C. at 1715.

IV.

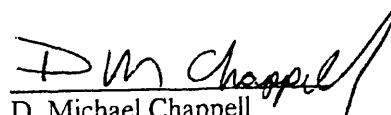
IT IS HEREBY ORDERED that Respondents shall refile their application for *in camera* treatment in accordance with the standards set forth in Rule 3.45(b) and this Order by January 14, 2000, or expressly withdraw their request by way of pleading.

IT IS FURTHER ORDERED that the deadline set forth in the Second Revised Scheduling Order for filing motions for *in camera* treatment of proposed trial exhibits is extended to January 14, 2000. Such motions shall comply with the standards set forth in Rule 3.45(b) and this Order.

Should Respondents choose to refile their Application for *In Camera* Treatment, the Court will issue an appropriate order to grant or deny *in camera* treatment of confidential information contained in (1) Complaint Counsel's Opposition to Respondent's Motion to Exclude Witnesses, (2) Complaint Counsel's Motion for Summary Judgment, and (3) Respondents' Opposition to Complaint Counsel's Motion for Summary Judgment. The parties will then be instructed to refile public versions and *in camera* versions in accordance with Commission Rule 3.45(e). The Secretary of the Commission is hereby requested to withhold from public disclosure all documents previously filed as *in camera* versions until a final order is issued.

Because the Commission's rules do not contemplate the filing of an *in camera* version of a pleading until the Administrative Law Judge has granted *in camera* treatment to confidential materials, when filing applications for *in camera* treatment or responses thereto which include or specifically describe information for which a party is seeking *in camera* treatment, the parties are instructed to serve the Office of Administrative Law Judges, and to serve each other, copies of such pleadings, but not to file such pleadings with the Office of the Secretary. Once the Court has granted or denied *in camera* treatment of the information for which *in camera* treatment is sought, the parties shall then file with the Secretary an *in camera* version and a public version of the application for *in camera* treatment or any response thereto.

It is SO ORDERED.


D. Michael Chappell
Administrative Law Judge

Dated: December 23, 1999



RECYCLED PAPER



TO REORDER CALL 954-846-9399

The Consumer.Net Privacy Policy

"Opt-In ... Let the Consumer Decide"

No information is sold or released to anyone about visitors to this site or customers of Consumer.Net without consent. In other words, no information is released to anyone unless you tell us it is OK.

Aggregate reports for web site visitors are generated. These reports do not contain any personally identifiable information.

Internet 'cookies' are not used except for demonstration purposes on the Internet Privacy Analysis page.

When visiting any Internet site your unique address called an "IP address" is recorded. Consumer.Net does not release any information about the collection of this address to any third party. Consumer.Net archives the log files in order to create aggregate statistical reports, detect errors at the web site, and for security reasons. A full explanation of the IP address and examples of the log file that captured when visiting a web site are found here. To see your IP address and see the results of a trace click here. IP reports for advertisement clicks are shared with the advertiser. However, they usually have this information already since it is captured by their server when you click an ad. No additional information associated with any specific user is provided to the advertiser. For more information on IP addresses see the paper authored by Russ Smith of Consumer.net: *The IP Address: Your Internet Identity.*

No Images, files, or cookies are downloaded from third party servers.

'Redirects' or the logging of clicks for external links is only done for advertisements. This is indicated by link to a URL such as '/redirect.asp?url= ...' The external URL is clearly marked in the "url=" portion. An example of the information collected when clicking on an ad is shown here.

For more information see the Internet Privacy issues page at this site or contact privacy@consumer.net. Consumer.Net customers may also verify their personal information that is on record at Consumer.Net. To have personal information removed from the Consumer.net database contact this e-mail address or see the contact page for the mailing address and telephone number.

The IP Address: Your Internet Identity

by

Russ Smith of Consumer.Net
March 29, 1997

Abstract

The Internet, sometimes called the network of networks, is based upon one simple principle: transferring information from one computer to another. In order to do this each computer needs an identity which is called the "Internet Protocol address" or "IP address." It is similar to a telephone number or street address. The IP address is **personally identifiable information** that is automatically captured by another computer when any communications link is made over the Internet. This includes visiting web pages, sending or receiving e-mail, visiting newsgroups, or using a chat room. Often, a user's IP address is automatically sent to a third party when visiting a web site using banner ad networks or, under certain circumstances, opening an e-mail message. This usually occurs before there is any opportunity to review a privacy policy. The amount of information available about users from their IP addresses varies greatly depending on how they are connected to the Internet and other information that may be available. Logging the IP address is also essential in system security for tracing unauthorized use and computer break-ins. As fixed Internet connections increase, more and more users can be traced directly from their IP address. To see a demonstration of IP address tracing visit <http://consumer.net/analyze/>.

IP Addresses and Domain Names

Computers connected to the Internet must speak the "Internet language" called the "Internet Protocol" or simply "IP." Each computer is assigned a unique address somewhat similar to a street address or telephone number. Under the current system there are four numbers that range from 0 to 255 (Example: 206.156.18.122). Every computer, whether it functions as a web site, is being used by a web surfer, is a mail server, and/or is used for any other function, has an IP address so it can communicate across the Internet. Communication is accomplished by sending pieces of information called "packets" that include the IP address of the destination computer.

Up to this point, domain names have not yet been mentioned because they are not needed for the Internet to work! An *optional* feature of the

Internet is to use domain names. With this system I can tell users to visit www.consumer.net rather than 206.156.18.122. If there are several computers in a network they can be grouped under a domain and could be given 'friendly' names for convenience such as: computer1.consumer.net, computer2.consumer.net, etc. This has the added convenience of keeping the same computer names even when the IP addresses change or if the computers move to a different physical location. Again, this naming is optional and is not always done. As a side note, the underlying IP addresses have no intrinsic value but the optional domain names can be worth thousands of dollars and have been the subject of many court cases.

The Domain Name System (often called DNS) is the system where the IP addresses are converted into names. When www.consumer.net is entered by a user into a browser a (somewhat hidden) process converts that name into 206.156.18.122. This allows the user to connect to the proper web site and usually involves a domain registration service that is funded by domain name fees.

How are IP Addresses Distributed?

Every transfer of information over the Internet must include the capture of the IP address. Some examples of automatic logging are: visiting a web site, sending or receiving e-mail, using a chat room, or reading and posting to newsgroups. A common situation that causes IP addresses to be distributed to a third party is when visiting a web site **and** that site participates in banner ad networks where the ads are served from a third party site. This third party site retrieves the IP address when it sends the ad. This information is used to measure the number of ad views and calculate click-through rates.

Transferring IP addresses to a third party can also be accomplished by sending a web page via e-mail. When the user opens the attachment (if they are connected to the Internet) the e-mailed web page could make a request to a web site anywhere on the Internet (such as requesting an image file). This transfers the user's IP address to that web site along with the date and time that the user opened the message. An Internet cookie can also be placed on the user's system at that time. Several advertisers already engage in this practice. This method could also be used to defeat anonymous e-mail.

How Can Users be Traced from their IP Addresses?

Once an IP address is captured several methods can be used to trace the user. These tools can be found at <http://consumer.net/tracert.asp>.

- Determine who owns the network. IP addresses are distributed in blocks to network providers or private companies. By searching IP registration databases it is possible to determine who owns an IP address block. Databases are available on the Internet for the Americas, Europe, and Asia-Pacific regions. Sophisticated computer break-ins sometimes include an attempt to erase the IP addresses captured by the log files to prevent this type of lookup.
- Perform a "reverse lookup." This converts the IP address into a computer name [Example: convert 206.156.18.122 into www.consumer.net]. This is used to determine if a computer is part of a registered Internet domain.
- Conduct a Traceroute. When information packets travel through the Internet they pass through several computers in a hierarchical fashion. Normally packets pass from the user to their Internet Service Provider (ISP) until it reaches the user's "backbone" provider. It then transfers to the destination "backbone" provider down to the ISP of the destination computer and finally to the intended recipient. It is often possible to determine an approximate physical location of an IP address in this fashion. It is also possible to determine the computer's ISP and/or network provider even if the computer itself is not part of a domain. This is usually how junk e-mail or "spam" is traced.
- Review domain registration information via the "WHOIS" databases. Domain registration information is available via the Internet by performing a WHOIS on the domain name portion of the computer name [Example: for www.consumer.net perform WHOIS CONSUMER.NET to obtain the registration information].
- Search the Internet for the IP address and/or computer name. It is often possible to find matches from users making public postings on discussion boards or from web sites that leave their log files open to the Internet. Of course, web site owners and/or banner networks could have additional non-public information based on activities at their web sites.

Generally, users who have fixed Internet connections (cable modems, private companies, etc.) have fixed IP addresses. Dial-up Internet providers usually give addresses dynamically from a pool when a user dials in to connect (such as a pool of 100 IP addresses per 800 subscribers).

Internal network procedures also affect the amount of information that can be gleaned from an IP address. If a proxy sits between the users and the Internet all of the users appear to come from one computer. In these cases, users can only be traced as far as the proxy unless additional information is known. The computer names can also sometimes be

used to gather additional information. One major provider's computer names usually include the nearest big city of the user. Some networks simply use the e-mail address in the computer name [Example: russ.consumer.net has e-mail address russ@consumer.net].

Ambiguities in user identification by IP address are reduced by the use of "Internet cookies." These are text files that gives users a unique identity. Cookies would essentially become unnecessary if everyone had fixed IP addresses.

Privacy Policy Implications

As of March 1998 the vast majority of privacy policies, both in the public and private sectors, fail to properly explain IP address collection as the collection of **personally identifiable information**. Sites such as FTC.GOV and CONSUMER.GOV have incorrect information concerning this issue. These policies indicate that only a domain name is captured. Some commercial web sites (such as VISA.COM) have copied this incorrect information and made it part of their own policy. Other industry privacy policy templates, such as those offered by the Direct Marketing Association and the Information Industry Association, overlook IP address collection.

A site's policy must also be coordinated with the policies of third parties that capture IP addresses from their site visitors (such as banner ad networks). Sometimes the banner ad network's policy is more important since it has the potential to track users across several sites rather than activity at a single site.

© 1998 Russ Smith

