NO HIDING PLACE IN CYBERSPACE: ELECTRONIC DISCOVERY FROM NON-PARTIES 2011 Updated Version[1]

David Crerar,

Borden Ladner Gervais LLP[2]

Ryan Purita,

Sherlock Forensics Ltd.[3]

> *It is true that in the modern era defamatory material may be communicated broadly and rapidly via other media as well. The international distribution of newspapers, syndicated wire services, facsimile transmissions, radio and satellite television broadcasting are but some examples. Nevertheless, internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by the features described above, especially its interactive nature, its potential for being taken at face value, and its absolute and immediate worldwide ubiquity and accessibility. The mode and extent of publication is therefore a particularly significant consideration in assessing damages in internet defamation cases.*[4]

An anonymous posting on an internet website defames and destroys a professional reputation. An anonymous entry on an internet chat-room reveals confidential pricing information. A series of anonymous emails threatens physical harm to the recipient. All of these events pose threats to the personal and financial security of the target person or company; all demand immediate remedy; and all found legal causes of action. Happily, our robust and adaptive legal system

---

1 This paper reflects developments in the law and the internet to January 1, 2011.
The writers thank Duncan Finley for his assistance in this update, and James Katz and Stephanie Lewis of BrazeauSeller for their helpful insights on this topic.
Earlier versions of this paper were published in the course materials for the Continuing Legal Education Society of BC course *Electronic Evidence and eDiscovery 2006*, on April 27, 2006, and in *the Advocate* (1 November 2006), vol.64, p.781.

2 David Crerar is a partner in the Commercial Litigation department at Borden Ladner Gervais LLP, and serves as an adjunct professor at the University of British Columbia Faculty of Law. In addition to media and defamation law, Mr. Crerar practices and has published in the areas of commercial litigation, pensions and banking litigation, and protection of trade secrets.

3 Ryan Purita is one of a handful of security professionals in private practice in British Columbia, and one of only 400 in Canada, who holds the Certified Information Systems Security Professional (CISSP), Internet Systems Security Architect Professional (ISSAP) and Information Systems Security Management Professional (ISSMP) certifications. The CISSP designation is the only designation awarded ANSI accreditation under the ISO/IEC 17024 standard, and the only globally recognized security certification. Mr. Purita is also one of only four EnCase Certified Skilled Examiners in British Columbia, and one of eleven in Canada. The EnCE Certification is recognized by courts in Canada and the US, and by law enforcement, corporations and government as the world's leading credential in Computer Forensics.

4 *Barrick Gold Corp. v. Lopehandia* (2004), 239 DLR (4th) 577 (Ont CA) at para.34, per Blair J.A.

provides means of obtaining evidence about the identity of the sender, despite the anonymous source and technical complexities, from non-party sources.[5]

This paper will strive to provide a practical overview of the means to obtain orders for electronic discovery from non-parties such as internet service providers ("ISPs") and website hosts. It will not wade into the valid and vigorous debate about whether the law should recognize and preserve the internet as a sacred sphere of anonymity different from more traditional modes of communication.[6] For the purposes of this paper, we note that Canadian courts have not been dazzled by the vast and novel realm of the internet, but have successfully adopted common law principles, as applied to traditional communications, rather than to carve out a distinct area for this vast and novel electronic realm. Examples can be seen in appellate decisions on jurisdiction[7] and limitation periods[8] with respect to internet communications that neither depart significantly from the existing common law principles nor treat the internet as *sui generis*.

This paper will start with a brief technical overview of the form and creation of electronic evidence that may be held by non-party custodians. It will then review the technical steps for obtaining the evidence on which to base an application to have a non-party disclose electronic evidence. The paper will then set out the civil procedure rules that apply to obtaining non-party discovery, and review how the developing case law has treated those discovery rules. Continuing with the practical logistics of such an application, the paper will then discuss the typical order for non-party discovery. It will then set out some pitfalls and roadblocks impeding non-party discovery, including what effect city-wide wireless and Wi-Fi communications may have on the prospects of plaintiffs seeking redress for civil wrongs based in electronic communications. Finally, the paper will suggest some possible means of circumventing these roadblocks.

---

5 This paper will use the term 'non-party' instead of the confusing and ambiguous term 'third-party' which at times is used to refer to non-party witnesses, and at times is used to refer to litigants added as defendants by existing defendants.

6 For worthy literature in this debate see, for example, Jonathan T. Feasby, "Who was that Masked Man?" (2002) 1:1 Canadian Journal of Law & Technology; L.B. Lidsky, "Silencing John Doe: Defamation & Discourse In Cyberspace" 49 Duke L.J. 855, and generally, The Canadian Internet Policy and Public Interest Clinic Website at http://www.cippic.ca/online-anonymity-and-john-doe-lawsuits/.

7 *Bangoura v. Washington Post* (2005) 258 DLR (4th) 341 (Ont CA), application for leave to appeal dismissed with costs 16 February 2006, SCC Bulletin 2006, p.247.

8 *Carter v. B.C. Federation of Foster Parents Assn.* (2005), 257 DLR (4th) 133 (BCCA).

I. INTERNET PROTOCOL ADDRESS

The primary means of identifying the poster of an anonymous internet communication is through the internet protocol address (the "IP Address") which in effect leaves a fingerprint of the anonymous communicator in the communications surveyed in this paper.

The IP Address can be analogized to a postal address, telling the server to which IP Address the communication should be sent.[9] Many internet-based communications will within themselves record the IP Address of both sender and recipient of the communication. In the recent case of *Warman v. Fournier* the Ontario Superior Court of Justice Divisional Court defined the IP Address, and explained its utility in the forensic process:

> An IP address is a unique identifier for a computer on the internet. It is assigned to a computer by a subscriber's internet service provider (an "ISP") when the subscriber signs on to the internet. The Message Board did not capture the IP of a new user when a new user account was created. It did, however, record and store the IP address for each message posted, including those of the eight John Doe defendants. With the IP address of each message and the time of the message (disregarding an issue as to the accuracy of the Message Board's software clock, which is not relevant to this appeal), the Respondent can, at a minimum, seek the identity of the subscriber who was assigned the particular IP address at the time of the message from the relevant ISP.[10]

As set out below, the IP address is usually not visible, but hidden within the message. Happily, it is usually easy to retrieve this information, as set out below. A further complication is that a given ISP subscriber will not have a fixed IP Address for life, but, instead, ISPs generally assign a given IP Address to a given internet user for a limited period of time; a given internet user may be assigned many IP Addresses in a year, and those IP Addresses may be in turn recycled and assigned to other users. As will be set out below, this complication is also not at all fatal to the reliability of an order ordering disclosure of such information in order to identify the sender.

---

[9] As set out further below, the word "protocol" is used to denote an agreed-upon format for transmitting data between two computing devices.

[10] *Warman v. Fournier* (2010) 100 OR 648 (SCJ) at para. 5.

II. NON-PARTY CUSTODIANS OF ELECTRONIC EVIDENCE

i. Internet Service Providers

When the would-be plaintiff needs to learn the source of an anonymous email to combat its harmful effects, the best source of information will be the ISP. The largest ISPs in British Columbia are Bell Canada, Telus Inc., Shaw Communications Inc. and Rogers Communications Inc. The ISPs are the most fertile source of non-party disclosure in internet defamation cases. They have access to customer subscription information for their customers, as well as records of each email sent by their customer if hosting is provided by the ISP. Furthermore, as they tend to be well-established companies in the wild and woolly world of the internet, with a sense of corporate responsibility and usually an in-house legal department, there is greater legal certainty and stability in attempting to obtain this information from an ISP.

ii. Email Account Providers

Companies that provide email accounts are another potential source of information. The leading examples of such providers are Google, Yahoo! and Hotmail.[11] In theory, these companies and ISPs should have the same information about the customers who obtain email addresses via their internet services. But practically speaking, they are less likely to be useful or reliable sources of information. Although most of these providers have express policies forbidding the use of anonymous or false names when obtaining addresses or email addresses, these companies do not seek to verify the identity provided by the customer in the on-line application form. As they do not generally charge a fee for issuing an email account, they have no accurate billing records with names and addresses. For these reasons, such providers are less fruitful sources for electronic discovery.

It is also possible to obtain further information from emails by utilizing search engines such as Google. Often times an individual may post their email on a forum or personal website with as contact information. In the latter case, you may be able to obtain registrant information on the

[11] e.g. “sharper@hotmail.com“, “arthurmeighen@yahoo.ca“, “jsthompson@aol.com“.

owner of the website providing further clues to the identity of the individual in control of that email address.

Commercial sites such as US People search or http://emailfinder.com/Emailfinder.com will for a fee provide information on the owners of an email address. They derive this information from public records and online phone book resources.

iii. Host Websites

The third potential source of information about the origin of an electronic communication is the host website on which the offending communication has been posted. Chatrooms, bulletin boards and other similar webpages exist to allow users to express views and share information – fertile grounds for communications of legal consequence. The administrators, societies and companies that host such sites will often have information about the source of the postings and emails sent to their sites. Typically, web hosts will have the following information available to them:

- The IP address of the visitor.
- Operating system and browser settings.
- Path taken by visitor (entry and exit website pages for example).
- Referral information. This information is passed along when one clicks on a link. So if the user clicks on a website from a Google search, it will record that the visitor originated from a Google search.

Ultimately, different website hosts will have different information. It is up to the host to turn on an electronic logging function to track information about visitors, and to choose what information to log. An applicant's ability to obtain information from website hosts will thus vary significantly.

III. CREATION AND RETRIEVAL OF ELECTRONIC RECORDS

i. Creation

When a user writes an email on that user's computer, the user will typically author the email on an email programme such as Outlook or Eudora.[12] The user then enters in information such as the recipient of the email, the subject, and the body text of the email.

Once the sender has entered this information and tells the programme to send out the email by hitting "Send" or "Email", a series of events takes place which gets the email from the user's computer to the recipient. Consider the following example:

- Jane composes a message using her preferred email programme. For this example, Jane's computer's IP address is "1.2.3.4".

- She then types in the e-mail address of "John" and enters in a subject, types the body of her email and hits "Send".

- Jane's email programme formats the message according to the RFC internet e-mail format and uses the Simple Mail Transfer Protocol ("SMTP") to send the message to the local mail transfer agent ("MTA"). For example, if Jane's ISP is Shaw, the MTA is "SHAWMAIL".[13]

- The email programme then adds a "trace field" and labels the message "Received:" This field identifies the system that sent the email by either its IP address, its host name or both. In this case, "Received: by 1.2.3.4" is appended to the email. This indicated that Shawmail received an email from 1.2.3.4 – Jane's IP address.

- The MTA looks at the destination address provided in the SMTP protocol (not from the message header), in this case john@telus.net.

---

[12] These programmes, such as Outlook, Eudora, and Lotus Notes, are known as "mail user agents" ("MUA").

[13] Electronic mail, like other aspects of the internet, has a "universally accepted" method of travelling the internet, referred to as a "Request for Comments" ("RFC"). These RFCs are an agreed-upon process dictating how emails are to behave in cyberspace. This protocol allows emails to be sent to and received from different devices and operating systems without needing to know its internal operations or workings. The RFC, for example, makes the delivery of an email message from a Macintosh computer to a computer running a Windows operating system possible.

- A modern internet e-mail address is a string in the form of "emailaddress@isp.something". The part before the "@" symbol is the local part of the address, often the username of the recipient, and the part after the "@" sign is a domain name.

- The MTA locates this domain name in the Domain Name System ("DNS") to find the mail exchange servers accepting messages for that particular domain (e.g. telus.net).

- The DNS server for the telus.net domain, ns.telus.net, responds with an MX record that lists the mail exchange servers for that domain. In this case, the MX record is mx.svc.telus.net, which is a server run by John's ISP, Telus.

- Shawmail sends the message to mx.svc.telus.net using SMTP, which then delivers it to John's mailbox.

- When John opens his email account, has his email account open, or presses the "RECEIVE" button in his email programme, it will contact mx.svc.telus.net, typically through "Post-Office Protocol" ("POP"), and receive any emails waiting.[14]

The email leaves a "trace field" at each step of the process. First, Jane's IP address of 1.2.3.4 is appended to the message header as it is being sent to her mail exchange server. When her mail exchange server passes the email along to the next exchange server, it would append its own IP address to the field. Further, each step of the process is recorded as meta-data within the email itself. Every step of the way, each server that receives the email message attaches its own "trace field" before delivering it to the next MTA. If the user who initiates an email uses a proxy server (a server that acts on behalf of the client), or the email bounces off several servers (relays) before reaching its final recipient, each server that handles the message will append its own "trace field" to that message.

ii. Retrieval

In order to crack the first shell of secrecy of an email communication, one needs to obtain the email's header information, which sets out its technical path from sender to recipient, as was described above. Generally, on an email received on the Outlook email programme, one can

[14] For example, "POP3" is an agreed-upon method of translating and transmitting data for emails.

obtain the email header by opening the email on the recipient computer, and then selecting "view" and then "options".[15]

While the header information looks at first like hieroglyphics, closer inspection provides clues and comprehension. As an example, we will translate the following header information:

Received: from p00m165.mxlogic.net ([66.179.109.165]) by smtp.enerflex.com (Lotus Domino Release 6.5.4) with ESMTP id 2005090622094656-165787 ;

Tue, 6 Sep 2005 22:09:46 –0600

Received: from unknown [66.163.179.88] (HELO web35209.mail.mud.yahoo.com) by p00m165.mxlogic.net (mxl_mta-2.12.1-01) with SMTP id 9086e134.2317155248.66902.p00m165.mxlogic.net (envelope-from <hoodedfang@yahoo.com>);

Tue, 06 Sep 2005 22:09:45 -0600 (MDT)

D Received: (qmail 53421 invoked by uid 60001); 7 Sep 2005 04:09:40 -0000

DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=s1024; d=yahoo.com; h=Message-ID: Received:Date:From:Subject:To:MIME-Version:Content-Type:Content -Transfer-Encoding; b=gHUKdGAV/w3cfPU+cuukKXnzFhepTuhxoq3XH8pj/2PBay0cj17pXBtciKaQiojSrWx7RcEYho Gdf3gIC8KSg6qH9s7e8mN3jKayHabAGGEsTihrlMakhfiZDw28UDP7V+ABu7FZ2BvY9F4H00 Gdf3gIC8KSg6qH9s7e8mN3jKayHabAGGEsTihrlMakhfiZDw28UDP7V+h03DG2QPKizn/DcWSMoAFRjN8= ;

Message-ID: <20050907040940.53419.qmail@web35209.mail.mud.yahoo.com>

B, C Received: from [24.71.223.140] by web35209.mail.mud.yahoo.com via HTTP; Tue, 06 Sep 2005 21:09:40 PDT

Date: Tue, 6 Sep 2005 21:09:40 -0700 (PDT)

From: Joe Vigilante <hoodedfang@yahoo.com>

Subject: Our CEO is a Criminally Insane Coprophagist!!!

To: klau@concept.com, barry@concept.com, dstewart@concept.com, dleurs@concept.com, hsmith@concept.com, joecool@concept.com,

[15] In the case of Outlook, one must right-click on the email and select "Options" this will display the emails headers. All mail clients are different. One must consult the manual in order to see how to reveal the headers. For example in Hotmail, one needs to view the emails in Full or Advanced by going to "Options" and then "Mail Display Settings".

MIME-Version: 1.0

X-Spam: [F=0.0021795594; B=0.500(0); S=0.010(2005081001);
MH=0.550(2005090619); R=0.150(s79/n448); SC=none; spf=0.500]

A X-MAIL-FROM: <hoodedfang@yahoo.com>

X-SOURCE-IP: [66.163.179.88]

X-MIMETrack: Itemize by SMTP Server on WEBSVR01/EMFG(Release 6.5.4|March
27,

2005) at 09/06/2005 10:09:47 PM, Serialize by Notes Client on Don
Petersen/EMFG/Enerflex(Release 6.5.2|June 01, 2004) at 07/09/2005 10:28:21 AM

Content-Transfer-Encoding: 8bit

Content-Type: multipart/mixed; boundary="0-1412591497-1126066180=:53408" --0-
1412591497-1126066180=:53408

Content-Type: multipart/alternative; boundary="0-873457478-1126066180=:53408" --
0-873457478-1126066180=:53408

Content-Type: text/plain; charset=iso-8859-1

Content-Transfer-Encoding: quoted-printable

From the sample header information, we can determine the following (the letters correspond to those marked on the left column in the excerpt above):

(A) the email was sent from a web mail account identified as hoodedfang@yahoo.com.

(B) the email was delivered from a Yahoo web server with the address 35219.mail.mud.yahoo.com.

(C) the email passed through a Shaw cable-owned proxy server, IP 24.71.223.140 on Tuesday, 6 September, 2005 at 21:09:40 p.m. Pacific Daylight Time.

(D) the email was received on 7 September 2005 at approximately 04:09:40 a.m. Calgary time.[16]

One may also be able to obtain non-electronic clues from the date and time the email was sent, especially where a series of tortious emails may indicate a pattern. The date and time may help in determining the time zone in which the sender is located. Further, if all the emails come at a particular hour, on a weekday, it may be possible to infer what time zone the sender is in and whether the sender is sending the emails from work.

The IP address (here, 24.71.223.140) allows the next step of sleuthing. There are various internet reverse-lookups that allow one to identify the company and server that have been assigned a given IP address. The most useful common database currently on the internet is maintained at www.ipchecking.com, but one may also use a non-profit site such as arin.net.[17] Slotting the IP address into the field at the top of the homepage yields a response indicating that Shaw Communications Inc. holds that particular IP address (along with a broad range of IP addreses numbered from 24.64.0.0 to 24.71.255.255):

(a) ipchecking.com information on 24.71.223.140:
NetRange: 24.64.0.0 – 24.71.255.255
CIDR: 24.64.0.0/13
OriginAS:
NetName: SHAW-COMM
NetHandle: NET-24-64-0-0-1
Parent: NET-24-0-0-0-0
NetType: Direct Allocation
NameServer: NS8.SO.CG.SHAWCABLE.NET
NameServer: NS7.NO.CG.SHAWCABLE.NET

[16] The same information can be obtain from an email provider such as Yahoo, or the host of a chat-room or similar website. Because these entities are unlikely to have a reliable record of the identity of the sender, who likely uses a pseudonym, it is likely that an additional forensic step is needed. First, one can obtain an order that the provider reveal the IP address of the sender. That IP address can then in turn be used to determine the ISP used by the sender. One then makes a second application, to compel the ISP to provide information about its customer.

[17] Many websites (including http://geobytes.com/Geobytes.com, http://checkdomain.com/Checkdomain.com, http://easywhois.com/Easywhois.com) provide such a service. Arin.net is still an useful reverse-lookup. Arin also provides all of the information that the companies provide, but is grouped in separate boxes. For example to see the full information on the owner of an IP address, one must click the name associated. In our example Shaw, clicking on the organization "SHAWC" (http://whois.arin.net/rest/org/SHAWC.htmlhttp://whois.arin.net/rest/org/SHAWC.html) provides the full address and contact deals for the owners. http://ipchecking.com/

RegDate: 1996-06-03
Updated: 2006-02-08

OrgName: Shaw Communications Inc.
OrgId: SHAWC
Address: Suite 800
Address: 630 – 3rd Ave. SW
City: Calgary
StateProv: AB
PostalCode: T2P-4L4
Country: CA
RegDate: 2003-03-05
Updated: 2010-08-06

OrgAbuseHandle: SHAWA-ARIN
OrgAbuseName: SHAW ABUSE
OrgAbusePhone: +1-403-750-7420
OrgAbuseEmail: mailto:internet.abuse@sjrb.cainternet.abuse@sjrb.ca
OrgAbuse

OrgTechHandle: ZS178-ARIN
OrgTechName: IP Admin
OrgTechPhone: +1-403-750-7428
OrgTechEmail: mailto:ipadmin@sjrb.caipadmin@sjrb.ca
OrgTech

(b) Arin.net information on 24.71.223.140:

NetRange 24.64.0.0 - 24.71.255.255
CIDR 24.64.0.0/13
Name SHAW-COMM
Handle NET-24-64-0-0-1
Parent NET24 (NET-24-0-0-0-0)
Net Type Direct Allocation
Origin AS
Nameservers NS8.SO.CG.SHAWCABLE.NET
NS7.NO.CG.SHAWCABLE.NET
Organization Shaw Communications Inc. (SHAWC)
Registration Date 1996-06-03
Last Updated 2006-02-08
Comments
RESTful Link http://whois.arin.net/rest/net/NET-24-64-0-0-1http://whois.arin.net/rest/net/NET-24-64-0-0-1

Name Shaw Communications Inc.
Handle SHAWC
Street Suite 800
630 - 3rd Ave. SW
City Calgary
State/Province AB
Postal Code T2P-4L4
Country CA
Registration Date 2003-03-05
Last Updated 2010-08-06
Comments

RESTful Link
http://whois.arin.net/rest/org/SHAWChttp://whois.arin.net/rest/org/SHAWC
Referral Server rwhois://rwhois.shawcable.net:4321

Network Resources
SHAW-COMM (NET-24-108-0-0-1) 24.108.0.0 - 24.109.255.255
SHAW-COMM (NET-68-144-0-0-1) 68.144.0.0 - 68.151.255.255
SHAW-COMM (NET-24-64-0-0-1) 24.64.0.0 - 24.71.255.255
SHAW-COMM (NET-24-80-0-0-1) 24.80.0.0 - 24.87.255.255
SHAW-COMM (NET-24-76-0-0-1) 24.76.0.0 - 24.79.255.255
SHAW-COMM (NET-70-64-0-0-1) 70.64.0.0 - 70.79.255.255
SHAWIPV6 (NET6-2001-4E8-1) 2001:4E8:: -
2001:4E8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SHAW-COMM (NET-184-64-0-0-1) 184.64.0.0 - 184.71.255.255
SHAW-COMM (NET-174-0-0-0-1) 174.0.0.0 - 174.7.255.255
SHAW-COMM (NET-96-48-0-0-1) 96.48.0.0 - 96.55.255.255
SHAW-COMM (NET-50-64-0-0-1) 50.64.0.0 - 50.72.255.255

Autonomous System Numbers
SHAW-COMMUNICATIONS AS10482 (AS10482)
SHAW-COMMUNICATIONS AS19075 (AS19075)

Function Point of Contact
Admin ZS178-ARIN (ZS178-ARIN)
Tech ZS178-ARIN (ZS178-ARIN)
Abuse SHAWA-ARIN (SHAWA-ARIN)

This new information indicates that the Calgary Shaw proxy server was used to distribute the email. But this information does not guarantee that the email originated in Calgary; it only indicates the location of the ISP's head office (which is Calgary for Shaw). No matter where a sender may be located, any email they send will appear to have originated from Calgary if they use Shaw's proxy server. If the user does not use Shaw's proxy server, the sent email would contain the IP address of the computer that sent it.

The trail does not stop there, however. It may be possible to determine the geographic location of the email sender by city or town, or even as precisely as a radius of a few blocks. This is because most ISPs, generally, will dedicate specific IP addresses to specific geographic areas. Even when the individual IP address is reassigned to another individual user, that IP address may generally be assigned to a user in the same geographic area. Two free computer processes allow the investigator to cross-reference the IP address, extracted from the offending email, with a specific geographic location.

The first is the website geobytes.com. Geobytes includes a free function called "IP Locator" that allows one to identify the city to which an IP address is assigned. For the example above, geobytes.com confirmed that the sender not only used the Shaw Calgary proxy server, but that he or she likely resides in Calgary based on the particular IP address he or she was assigned.

An even more precise tracing process can be carried out with one's own Windows-based computer. First, the investigator can click on "Start" in the lower left hand corner of his or her screen and click on "Run" in the menu. Next, the investigator types in "CMD". This takes the investigator to a text-based black screen with a prompt. The investigators types in "tracert", and then a space, and then the sender's IP Address. The computer will trace each "hop" in the path from the investigator's computer to the ISP's router that serves the area in which the sender's computer is located. By conducting this trace route process to the IP address given in the example above, we can see that the last hop that it makes prior to reaching "24.71.223.140" is rd1so-ge6-0.cg.shawcable.net, which translates to an IP address of "66.63.71.130".[18] The "cg" in the name indicates that it is a Calgary router and that the user is likely in Calgary. Shaw and most ISPs place hints about where their routers are located by including geographic code name such as "cg" or "vc" for Vancouver or "nwmr" for New Westminster. As a final step, one can contact the ISP and ask for the name of the neighbourhood or area the individual router serves. Such information does not reveal any personal details of the sender, but would allow the investigator to determine the approximate geographic location of the computer from which the original email was sent.

IV. PRACTICAL STEPS: CONTACTING THE ISP

i. Contacting the ISP

If one provides the header information to the ISP - specifically the date and time when the email was sent and the sender's IP address - the ISP is usually able to determine which customer sent

[18] The first part of "rd1so-ge6-0.cg.shawcable.net" is the Domain Name System name for the IP address of 66.63.71.130. Human beings remember words more easily than they do numbers. So in order to help people, DNS was instituted: this process essentially turns an IP address into a name. For example, www.cnn.com is the name by which that news website is known, but it does have an IP address; it is this numerical address to which one's computer travels.

the email. An ISP will hold tens of thousands of IP addresses. Rather than assigning each of its customers a unique IP address, ISPs will lend each customer a given IP address for a short period of time, usually between one week and six months.[19] Thus, with the date and the IP address, the ISP is able to cross-reference its records and determine which of its customers had a given IP address at the specific time and date the email was sent.

Once one has obtained the header information, it is advisable to contact the ISP's in-house counsel, describe the concern and urgency, and forward the header information. It will be a simple process for the ISP's technical engineers to determine whether records still exist with respect to the communication in question. The ISP will not advise of the identity of the sender or any further information, but will usually be willing to confirm whether or not the records still exist and whether or not there is a name attached to the transaction. One can thus save one's client the costs of a potentially fruitless application where the record of the communication has been deleted through the expiry of a document retention period.

ii. Privacy concerns

ISPs are restrained by privacy legislation from divulging its customers' personal information to persons seeking it through a casual or formal inquiry. As a result, some ISPs choose to contractually obtain pre-authorization from its customers to release customer information to another party seeking it. For example, the Shaw internet account agreement states that:

> Shaw may disclose any information as is necessary to:
>
> a. satisfy any legal, regulatory or other governmental request;
> b. operate the Services properly;
> c. or protect Shaw or its customers, in accordance with the guidelines set out in Shaw's Privacy Policy.[20]

[19] Practices differ, depending on the individual ISP. Some will change each user's IP address every time the user connects to the internet; some ISPs will not change it at all. Shaw, for example, has given one of the authors the same IP address for almost two years now. Other ISPs change their clients' IP addresses every time there is a new connection. Some ISPs bind their user's MAC address number to an IP address, so that as long as the user's network card's unique identification does not change, neither will the user's IP address.

[20] http://www.shaw.ca/en-ca/AboutShaw/TermsofUse/JointTermsofService. Accessed 13 December 2010.

However, in spite of such terms, generally ISPs will ensure that they preserve good customer relations by exercising an abundance of legal caution; ISPs will insist upon a court order compelling it to release information about the email sender before it will commit to doing so.

At this stage, as throughout the process, practical concerns outweigh legal or technical theory. The immediate concerns focus on the time and location of the electronic communication.

iii. Time concerns

With respect to time, there are three reasons that a party should contact the ISP as soon as possible to ensure that the electronic records are preserved.

First, different ISPs preserve their records for different periods of time. Some ISPs, such as Shaw, retain their back-up records with respect to specific email communications for only a few weeks. If your client requires such information, you must move quickly; if the client has delayed seeking your assistance, the ISP may have already destroyed its logs and back-up tapes.

Second, as with injunctions, a delay in applying to court will undermine the plaintiff's claim that the alleged torts in question pose a serious and urgent threat requiring judicial intervention.

The third reason to move swiftly arises from a legal precedent that is based upon faulty technical information. In *BMG*, a leading case, the Federal Court of Appeal stated, in *obiter dicta*, that as IP addresses are reassigned, the passage of time will make the connection between an IP address and a given user less reliable:

> If there is a lengthy delay between the time the request for the identities is made by the plaintiffs and the time the plaintiffs collect their information, there is a risk that the information as to identity may be inaccurate. Apparently this is because an IP address may not be associated with the same individual for long periods of time. Therefore it is possible that the privacy rights of innocent persons would be infringed and legal proceedings against such persons would be without justification. Thus the greatest care should be taken to avoid delay between the investigation and the request for information. Failure to take such care might well justify a court in refusing to make a disclosure order.[21]

[21] *BMG Canada Inc. v. John Doe*, [2005] 4 FCR 81 at para. 43.

With all respect to the Court, which can only rely upon the evidence before it, this technical description is incorrect, as set out above, in Part I of this paper. ISPs assign IP numbers to computers as they sign on to the internet.[22] Each IP number is as unique as a house address. If a crime is committed at an address on January 1, 2005 and on January 2, 2005 the occupant changes house addresses, it does not mean that, 20 years later, that crime did not take place at the original address on January 1, 2005. Certainly, over time, the ISP's logs may be lost or deleted, making the gathering of that evidence impossible or difficult. But it does not follow that an email was never sent from that that specific IP address at that specific time. With an accurate time and date of the email, coupled with an accurate IP address, it is very likely that the real sender, and not an innocent third party, will be revealed.

iv. Geographic and jurisdiction concerns

In terms of location, it is beyond the bounds of this paper to set out jurisdictional concerns with respect to the internet. Despite a more liberal approach to jurisdiction, reflecting the seamless international character of internet communications, counsel will need to consider the issues of jurisdiction *simpliciter* and *forum conveniens*.[23] As a primary consideration, one should look ahead to the likely location of the sender to avoid the inefficiency and cost of having to commence an action in one jurisdiction in order to obtain the information from the ISP, only to then have to start a new action in another jurisdiction once the sender's location is revealed. As set out above, the contents of the communication, the identity of the ISP, and the IP address itself may provide clues as to the location of the anonymous sender.

There is an additional complication. ISPs will often insist that the application to compel production be brought in their home jurisdiction. Thus applications against Telus tend to be brought in British Columbia, applications against Shaw tend to be brought in Alberta, and applications against Rogers tend to be brought in Ontario. In theory, an applicant could legitimately launch an action and bring an application in any of those jurisdictions. But, as will be a theme of this paper, the application will proceed much more smoothly if the ISP is not

---

[22] *Warman v. Fournier*, *supra*, at para. 5.

[23] See, for example, *Black v Breeden* (2010) 321 DLR (4th) 659 (CA), leave to appeal to SCC granted [2010] SCCA No 387 (QL); *Barrick*, *supra; Bangoura*, *supra; Braintech* v. *Kostiuk* (1999) 171 DLR (4th) 46 (BCCA), leave to appeal refused (2000) 142 BCAC 314 (SCC); and *Gutnick* v. *Dow Jones & Co.* [2001] VSC 305.

actively opposing the application; indeed, it will be the norm that the ISP does not consent but does not actively oppose the application, leaving that role to its customer. It may well be advantageous to accede to the ISP's request that the application be brought in the jurisdiction of its choosing. As an additional consideration, it will be easier to enforce a document production order, an order resembling a mandatory injunction, in the jurisdiction where the ISP is clearly situated.

V. CIVIL PROCEDURE: *NORWICH PHARMACAL* OR JOHN DOE?

i. Two possible methods

There are two non-exclusive means of applying to court to obtain non-party discovery. The first is known as a *Norwich Pharmacal* order, otherwise known as an equitable bill of discovery, in which the ISP or keeper of the information is the named defendant; the sole purpose of the litigation is to obtain documents concerning the anonymous sender. The second is a more conventional application for non-party discovery under Rules 7-1(18) and 7-5 of the British Columbia *Supreme Court Civil Rules*, brought within an action in which John Doe is the named defendant; after revelation of the sender's true identity, the claim is amended to replace the defendant "John Doe" with the sender's real name.

Both of these methods will now largely be influenced by the recent decision in *Warman v. Fourier*, which expressly applies privacy and freedom of expression considerations to applications to reveal the identity of anonymous senders and posters of internet communications. *Warman* and related cases will be discussed below, in Part VI of this paper.

ii. *Norwich Pharmacal*: suing the ISP

a. The law of *Norwich Pharmacal* orders

The *Norwich Pharmacal* application finds authority in the eponymous House of Lords decision

of *Norwich Pharmacal Co. v. Customs & Excise Commissioners*.[24] Lord Denning described in remedy in a later case as one that "enables a person, who has been injured by wrongdoing to bring an action to discover the name of the wrongdoer."[25] *Norwich Pharmacal* was a claim for patent infringement with respect to a chemical that the plaintiff was importing into the United Kingdom. The Customs & Excise Commissioners were obliged to keep records of the persons who imported the chemical in question into the country. The plaintiff sought an order that the Commissioners provide the names of the importers. Any importers not identified by the plaintiff as authorized importers would presumably be in breach of patent. The House of Lords allowed the novel order. The Lords noted that where a party has become mixed up with the wrongful acts of another (albeit through no fault of its own) so as to facilitate the wrongdoing, that party has an obligation to assist the wronged person by giving him full information about the identity of the wrongdoer.

As shown in the *Norwich Pharmacal* case itself, the equitable bill of discovery requires that the party in possession of the information about the ultimate wrongdoer be itself named as the defendant. The action is thus a brief one, leading directly to the application to have the defendant disgorge its knowledge as to the ultimate wrongdoer. The initial *Norwich Pharmacal* action would then end, and the plaintiff would commence a new action with the freshly-revealed wrongdoer as the defendant.

The test for a *Norwich Pharmacal* order has been variously stated. In British Columbia, the test has seven components. The applicant must show that:

> (i) the plaintiff must show that a *bona fide* claim exists against the unknown wrongdoer;
>
> (ii) the [plaintiff] must establish that the information is required in order to commence an action against the unknown wrongdoer, that is, the plaintiff must establish that disclosure will facilitate rectification of the wrong;

---

[24] [1973] 2 All ER 943. The remedy has been recognized in British Columbia (*Kenney v. Loewen* (1999), 64 BCLR (3d) 346 (SC)); Alberta (*Alberta Treasury Branches v. Leahy* (2000), 270 AR 1 (QB), affirmed (2002) 303 AR 63 (CA), leave to appeal refused (2002), 303 NR 392 (SCC)); Ontario (*Straka v. Humber River Regional Hospital* (2000), 51 OR (3d) 1 (CA); Prince Edward Island (*Re. Johnston and Frank Johnson's Restaurant Limited*, [1980] PEIJ No. 34 (CA); and the Federal Court (*Glaxo Wellcome plc v. Minister of National Revenue* (1998), 162 DLR (4th) 433 (Fed CA)).

[25] *British Steel Corp. v. Granada Television Ltd.*, [1981] 1 All ER 417 (CR) at 439.

(iii) the defendant must be the only practicable source of the information;

(iv) there is no immunity from disclosure;[26]

(v) the plaintiff must establish a relationship with the defendant in which the defendant is mixed up in the wrongdoing. Without connoting impropriety, this requires some active involvement in the transactions underlying the intended cause of action;

(vi) disclosure by the defendant will not cause the defendant irreparable harm; and

(vii) the interests of justice favour granting the relief.[27]

In its 2000 decision in *Alberta Treasury Branches v. Leahy*, the Alberta Court of Appeal set out five components:

(i) Whether the applicant has provided evidence sufficient to raise a valid, *bona fide* or reasonable claim;

(ii) Whether the applicant has established a relationship with the third party from whom the information is sought such that it establishes that the third party is somehow involved in the acts complained of;

(iii) Whether the third party is the only practicable source of the information available;

(iv) Whether the third party can be indemnified for costs to which the third party may be exposed because of the disclosure; some refer to the associated expenses of complying with the orders, while others speak of damages; and

(v) Whether the interests of justice favour the obtaining of the disclosure.[28]The *Leahy* framework omits considerations (ii) (necessity) and (vi) (no irreparable harm) that are present in the British Columbia test, but those matters would also form relevant considerations under the omnibus "interests of justice" consideration of the test.

The Ontario Court of Appeal recently adopted the *Leahy* test in *GEA Group AG v. Flex-N-Gate Corporation*.[29] The Court considered whether 'necessity' should be included as part of the test, whether as a stand-alone element of the test, or under the headings of "only practicable source" or "interests of justice." Ultimately, the Court concluded that while necessity was not a stand-alone component of the test, the applicant must at least show that the order would be necessary

---

[26] This little-considered requirement flows from the specific context of *Norwich Pharmacal*: in that case, the Customs and Excise Commissioners argued that the governing statute required them to keep the information confidential.

[27] *Kenney, supra, a*t para. 33.

[28] *Leahy, supra,* at para. 106.

[29] *GEA Group AG v. Flex-N-Gate Corporation* (2009) 96 OR (3d) 481 at para. 62.

for a prospective action to proceed, although the applicant need not provide a firm undertaking to commence an action upon receipt of the order and information sought.[30]

College of Opticians of British Columbia v. Coastal Contacts Inc., the most recent Supreme Court of British Columbia consideration of *Norwich Pharmacal,* cited the tests from both *Kenney* and *GEA Group AG* as authoritative. The Court did not have to settle on one formulation of the test, as it declined to issue the order, based on the failure of the applicant to attempt to obtain the information sought through other available means.[31]

b. The disadvantages of a *Norwich Pharmacal* application

In choosing which option to employ when applying for non-party discovery, a number of factors should be considered. The disadvantages to choosing the *Norwich Pharmacal* procedure generally outweigh the advantages.

First, ISPs, understandably, blanch at being named as a defendant. In this, we return to the theme that it is in the applicant's best interests not to provoke the ISP into actively fighting the application; naming it as a defendant may well be the tipping point.

Second, one must always launch two successive actions: the first against the ISP (or other source) and the second against the actual sender.

Third, as seen above, the test for *Norwich Pharmacal* application may be more complicated and onerous than would be an ordinary application for non-party discovery under the *Supreme Court Civil Rules*. This difficulty may have increased under the recent Federal Court of Appeal decision in *BMG Music Inc. v. John Doe.*[32] In *BMG*, the plaintiff applied for an order that certain ISPs, including Shaw, Telus, Bell and Rogers, provide the names of some 29 internet users, who allegedly downloaded music in breach of copyright through "peer-to-peer" file-sharing programmes. The Trial Court declined to order production, citing in part on privacy

[30] *GEA Group AG, supra,* at para. 84-85.
[31] *College of Opticians of British Columbia v. Coastal Contacts Inc.* (2010) 5 BCLR (5th) 365 (SC) at paras. 16-17.
[32] *Supra*.

concerns over the personal information about the file-sharing of Jane and John Does. The Court injected a new element into the test: the applicant must also show that "the public interests in favour of disclosure [must] outweigh the legitimate privacy concerns."[33] The Court of Appeal also elevated privacy concerns as a significant consideration in future applications:

> Thus, in my view, in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action. However, caution must be exercised by the courts in ordering such disclosure, to make sure that privacy rights are invaded in the most minimal way.[34]

Fourth, the complexity of the *Norwich Pharmacal* procedure has increased as different courts at different levels in different jurisdictions have attempted to strike a balance between protection of privacy and the assurance that wronged parties will be able to pursue valid claims. Presumably in an attempt to increase certainty in matters of non-party discovery, the Ontario Court of Appeal, concurring with the Alberta Court of Appeal, recently stated that civil procedure laws must take primacy over *Norwich Pharmacal* procedure if both modes can achieve the same result:

> [Pre-action discovery of non-parties] is not intended nor should it be permitted to serve as a substitute for the normal discovery regime mandated by the *Rules of Civil Procedure*. As noted by the Alberta Court of Appeal in *B.(A.)*, at para. 16: "[a] Norwich order is not intended as a device to circumvent the normal discovery process which can effectively achieve the same result…"[35]

Fifth, recent decisions from British Columbia and Ontario have pronounced the *Norwich Pharmacal* order as "an intrusive and extraordinary remedy that must be exercised with caution."[36] The courts note that an improperly granted *Norwich Pharmacal* order has the potential to harm innocent individuals through the release of confidential information. Further, it inherently places the defendant in possession of confidential information in the doubly awkward position of being a litigation defendant, as well as an involuntary releasor of confidential information about a party with whom it may have an ongoing business or personal relationship.

---

33 *BMG, supra,* at para.15(e)(e).
34 *BMG, supra,* at para.42. The appeal was dismissed without prejudice to the applicant to reapply.
35 *GEA Group AG, supra,* at para. 104.
36 *College of Opticians, supra,* at para. 18, citing *GEA Group AG, supra,* at para. 85.

Accordingly, as noted above, recent authorities require proof of some degree of necessity before granting the order.[37]

Sixth, recent decisions have emphasized that the *Norwich Pharmacal* order is a discretionary one: and courts are willing to exercise that discretion against granting the order, not only because of its intrusive and extraordinary nature, as stated above, but also because it is, ultimately, an equitable remedy. This was emphasized in a recent English decision in which the Court declined to reveal the identity of authors of certain internet postings: *Sheffield Wednesday Football Club Limited et al. v. Neil Hargreaves*.[38] The Court concluded that even if an applicant passes the test for a disclosure order, the court retains the discretion to decline the order. Factors relevant to the exercise of this discretion include the strength of the applicant's case, the seriousness of the defamatory allegations, whether the allegations are part of a defamatory campaign, whether the posters have breached their user agreement with the website, and whether the website has a stated confidentiality policy. In *Sheffield,* the court concluded that while the applicants had satisfied the *Norwich Pharmacal* test, the majority of the postings were of such a trivial nature, and more in the nature of a joke than defamation, that no disclosure should be ordered, as such disclosure would be "disproportionate and unjustifiably intrusive".[39] The court further indicated that had the website posted a confidentiality policy for the benefit of its posters, the more defamatory publications may have been protected from disclosure as well.[40]

As a related and final point, even if a party is able to prove that it has a valid claim, all of the enumerated *Norwich Pharmacal* tests provide courts with the discretion to determine that such an order is not in the public interest. At this stage in the analysis courts will consider *Charter* rights such as freedom of expression and privacy, in addition to general policy arguments. As noted above, the Federal Court of Appeal raised privacy concerns as a significant consideration in future applications for non-party discovery in *BMG Music Inc. v. John Doe*.[41]

---

[37] *GEA Group AG*, *supra*, at para. 85; *College of Opticians*, *supra*, at para. 43.
[38] [2007] EWHC 2375 (QB)
[39] *Supra*, at para.17.
[40] *Supra*, at para.18.
[41] *BMG*, *supra*, at para.42. The appeal was dismissed without prejudice to the applicant to reapply.

As set out further, below, in adjudicating an application for an order that the defendants produce the names of anonymous internet posters on a message board, the Ontario Superior Court of Justice recently held that the *Charter* rights of both freedom of expression and privacy are engaged.[42] Although *Warman* does not fall under the traditional *Norwich Pharmacal* line of cases, being brought under the ordinary rules of court governing disclosure,[43] the link that the court makes between the aforementioned *Charter* rights and internet anonymity may play a greater role in defeating the extraordinary, intrusive, discretionary, and equitable remedy of a *Norwich Pharmacal* order than it would an ordinary application for non-party disclosure under the rules of court.[44] Thus, applicants should be wary to the possibility that a court may exercise its discretion to reject a *Norwich Pharmacal* application in spite of a holding that there is a legitimate claim. This possibility becomes more likely if the facts suggest that the respondent or non-party had a legitimate expectation of privacy, or if an important freedom of expression issue is present.

c. The advantages to a *Norwich Pharmacal* application

The advantages to pursuing non-party discovery via a *Norwich Pharmacal* order are hypothetical, limited, and generally overwhelmed by the disadvantages set out above.

Theoretically, the *Norwich Pharmacal* application provides the plaintiff with more control of the process; once the ISP has provided the information about the sender, the plaintiff may consider whether or not it wishes to launch the second action against that wrongdoer. This is helpful, for example, when there is a fear that the sender of the offending communication might be revealed to be, for example, the son of the CEO of the defamed company, or a trade competitor that may be in fact keen to enter into litigation as an extension of a war in the market place. Further, the defendant John Doe could keep the action alive even if the plaintiff did not wish to proceed – an unlikely but possible scenario. By proceeding via *Norwich Pharmacal*, one avoids this risk, and can decide whether or not to commence proceedings against the newly revealed sender.

---

42 *Warman*, *supra*, at para. 15.

43 The application for production was brought under Rule 30.06 of Ontario's *Rules of Civil Procedure*, rather than under the equitable principles from *Norwich Pharmacal.*

44 It is conceded that for practical purposes the *Charter* may equally apply to applications for discovery under a province's civil rules in applications to unmask with anonymous internet posters, as it did in *Warman*, *supra*.

Ultimately, *Norwich Pharmacal* is a more important authority in England, which has traditionally barred discovery from "mere witnesses". As a result of this comparatively limited regime for pre-trial discovery, *Norwich Pharmacal* orders still play an important role in English procedure. In contrast, under the post-1976 British Columbia Rules of Court and its new *Supreme Court Civil Rules*, discovery from non-parties is neither rare nor difficult to compel. There is no need to rely upon the *Norwich Pharmacal* procedure, except insofar as some precedents for non-party electronic discovery are framed as *Norwich Pharmacal* applications.

iii. Discovery rules: suing John Doe

The more practical approach is to commence an action naming as the defendant the pseudonymous "John Doe", John Doe standing in for the ultimate sender of the offending email. The notice of civil claim briefly sets out the date and contents of the offending communication, alleging a specific cause of action such as breach of confidence or defamation. As it is not practicable to take further steps in the action (including serving the notice of civil claim itself) until one can identify John Doe, it is then appropriate to launch immediately into an application under Rules 7-1(18) and 7-5 of the British Columbia *Supreme Court Civil Rules* to obtain documents and information relating to the offending communication.[45] The application is launched with a notice of application, supported by affidavits. In order to expedite the process, a draft order, ideally one approved in advance by the ISP, ought also to be included. These materials will usually be served together with the notice of civil claim.

The test under Rule 7-1(18) is reasonably simple to meet.[46] The applicant must satisfy the court that the application is not a mere "fishing expedition", and that the non-party has a document in its possession relating to a matter in issue.[47] Alternately or concurrently, the party may proceed under Rule 7-5, seeking to obtain information from the non-party rather than documents. Again, the test is not onerous. The applicant must show, through affidavit evidence, that:

---

[45] Rule 30.10 of Ontario's *Rules of Civil Procedure* provide defamed persons with a mechanism for non-party discovery. In Nova Scotia, it is Rules 14.12 and 18.12 of the *Civil Procedure Rules*.

[46] While Rules 7-1(18) and 7-5 changed in number, they did not change in substance when British Columbia's new Supreme Court Civil Rules were adopted. As the wording is almost exactly the same, the authors expect that its interpretation will not change.

[47] *Dufault v. Stevens* (1978) 86 DLR (3d) 671 (BCCA) at para. 10.

(a) the matter in question in the action to which the applicant believes that the evidence of the proposed witness may be material; and[48]

(b) that the proposed witness

(i) has refused or neglected on request by the applicant to give a responsive statement, either orally or in writing, relating to the witness' knowledge of the matters in question, or

(ii) has given conflicting statements.

Where an ISP has stated that it will not provide the information without a court order, the test will be satisfied.

Once the order is obtained, and the true identity of the sender is revealed, the claim is amended to substitute the true defendant's name in place of John Doe, and the litigation proceeds without further delay.

VI. *CHARTER* CONCERNS AND COMPLICATIONS: *WARMAN*

The procedural distinctions above are diminished by the new leading decision of *Warman v. Fournier*. Even more importantly, *Warman* confirms that *Charter* principles of freedom of expression and privacy will play an important role in judicial decisions as to whether to release documents and information concerning anonymous internet posters.

In *Warman*, the plaintiff launched a defamation claim against Constance Wilkins-Fournier, Mark Fournier, and eight anonymous John Does who allegedly posted defamatory content on an internet message board operated by the Fourniers. The plaintiff sought an order under Rule 30.06 of the Ontario *Rules of Civil Procedure* to compel the Fourniers to produce all documents in their possession relating to the identities of the John Does.

After considering the importance of privacy and freedom of expression rights in such applications, the Court set down a list of required considerations:

[48] Rule 7-5(3)(b) is not relevant for the purposes of this paper.

(1) whether the unknown alleged wrongdoer could have a reasonable expectation of anonymity in the particular circumstances;

(2) whether the Respondent has established a *prima facie* case against the unknown alleged wrongdoer and is acting in good faith;

(3) whether the Respondent has taken reasonable steps to identify the anonymous party and has been unable to do so; and

(4) whether the public interests favouring disclosure outweigh the legitimate interests of freedom of expression and right to privacy of the persons sought to be identified if the disclosure is ordered.[49]

Apart from expressly adding privacy and freedom of expression to the overall balancing of whether the order would benefit the public interest, the Court primarily protects the interests of privacy and freedom of expression by raising the requirement that the plaintiff show not merely that he has a *bona fide* claim, but a *prima facie* claim. This is not as daunting, however, as it may seem. The Court held that in a defamation case, the applicant need only prove the affirmative aspects of his own case, and need not defeat in advance any defamation defences that the defendant might be anticipated to raise. For example, even where the subject website contains political debate which may well be protected by the defences of fair comment or responsible communication on a matter of public interest – defences that have been greatly strengthened recently by the Supreme Court of Canada[50] – the applicant need only show a *prima facie* case of defamation: that the words are false, that they refer to the plaintiff, and that they would tend to lower the applicant's reputation in the eyes of right-minded persons.[51] In the words of the Court, "[f]or such purpose, a plaintiff is required to establish only the elements of defamation within its control."[52]

In the end, the *Warman* Court concluded that the motions judge failed to take into consideration the importance of freedom of expression, or whether the applicant had established a *prima facie*

---

49 *Warman, supra,* at para. 34.

50 *WIC Radio Ltd. v. Simpson* [2008] 2 SCR 420 (fair comment); and *Grant v. Torstar Corp.* [2009] 3 SCR 640; *Quan v. Cusson* [2009] 3 SCR 712 (responsible communication).

51 *Grant v. Torstar Corp.* [2009] 3 SCR 640 at para.28.

52 *Warman, supra,* at para. 43. Interestingly, *A.B. v. Bragg Communications Inc.* (2010) 293 NSR (2d) 222 (SC), discussed below, after applying *Warman*, suggests that the applicant may have to rebut anticipatorily potential defences to an otherwise *prima facie* defamatory posting, such as fair comment: see para. 21.

case of defamation.[53] The Court ordered that the matter be remitted to a different motions judge for reconsideration based upon the newly-pronounced *Warman* principles.[54]

Warman is important in British Columbia for two reasons.

First, it unequivocally states that courts must consider an anonymous internet poster's freedom of expression and privacy rights under the *Charter* in cases that consider whether a knowledgeable party is compelled to reveal the poster's identity.[55] The Divisional Court considered and applied the decisions in *BMG* and *Irwin Toy*.[56] The Court found that *Charter* values were engaged by the plaintiff's application for disclosure. The Court looked to the law of the US, and noted that the First Amendment protected the right to publish anonymously as a component of freedom of speech.[57] At the same time, the Court noted that a claim in defamation also seeks to protect the privacy concerns of the plaintiff. The judicial challenge is to balance the interests of each of the parties.

Second, with respect to cases about internet anonymity, *Warman* follows the Federal Court of Appeal's holding in *BMG*[58] by blurring the line between *Norwich Pharmacal* applications and applications for production of documents and information under ordinary civil procedure rules. Notwithstanding that the application was brought under ordinary rules of court, the Court employed *Norwich Pharmacal* principles in its analysis,[59] and observed that *Norwich Pharmacal*

---

53 *Warman, supra,* at para. 45.

54 *Warman, supra,* at para. 46. The matter was heard and reserved on December 7, 2010, before the Honourable Madam Justice Blishen.

55 *Warman, supra,* at para. 44.

56 *Irwin Toy v. John Doe* (2000) 12 CPC (5th) 103 (Ont SCJ)

57 *Warman, supra,* at para. 17, citing *McIntyre Ohio Elections Commission,* 514 US 334 at paras. 3-4 (1995).

58 *BMG, supra,* at para. 32.

59 *BMG, supra,* at paras. 26-30. Rule 30.06 of Ontario's *Rules of Civil Procedure* applies to discovery from parties to an action, while Rule 30.10 applies to discovery from non-parties, making it Ontario's equivalent to Rule 7-1(18) of British Columbia's *Supreme Court Civil Rules*. However, the fact that *Warman* is not brought under Rule 30.10 does not necessarily distinguish it from British Columbia cases regarding non-party discovery. At para. 32 of *Warman,* Justice Wilton-Siegel states that it would be illogical to apply different principles to the discovery of parties and the discovery of non-parties, when a non-party can be made a party for "the price of issuing a statement of claim".

is an equitable remedy and thus can be applied flexibly on a case-by-case basis depending on the facts, no matter how the application was made.[60]

This blurring continues in other jurisdictions: the Supreme Court of Nova Scotia recently applied *Warman* in *A.B. v. Bragg Communications Inc.,* in form and substance, applying *Norwich* principles to an application for non-party discovery under the Nova Scotia *Civil Procedure Rules*.[61]

No British Columbia court has cited or approved *Warman*, but it is likely that future applicants who wish to unmask anonymous internet posters using Rules 7-1(18) or 7-5 will face arguments imported from *Charter* and *Norwich Pharmacal* jurisprudence.

That being said, it may well be that *Warman* will not significantly limit internet disclosure applications, for several reasons.

First, although *Warman* establishes that courts must consider whether the John Doe poster has a reasonable expectation of privacy, in most cases this enquiry will be answered in the negative. *York University v. Bell Canada Enterprises*, a *Norwich Pharmacal* application to compel the identities of the anonymous authors of defamatory emails, highlights two reasons why privacy concerns will not usually defeat the judicial quest for truth.[62] First, the court reviewed the privacy statements and service agreements of the respondent ISPs Bell and Rogers, and noted that those terms contemplated disclosure: "[a] Bell customer can reasonably contemplate, therefore, that his or her identity may be disclosed by order of the court in the event he or she engages in unlawful, abusive or tortious activity."[63] Accordingly, "the internet service customer(s) who published the communications could not have a reasonable expectation of privacy in relation to the use of the internet for the purpose of publishing defamatory

---

60 *Warman*, *supra*, at para. 28.

61 *A.B. v. Bragg Communications Inc.* (2010) 293 NSR (2d) 222 (SC).

62 *York University v. Bell Canada Enterprises* (2009) 99 OR (3d) 695 (SCJ), at para. 2. The anonymous email in question, sent by the elegantly-named "York Faculty Concerned about the Future of York University" accused the University President of committing "an outrageous fraud" by appointing a Dean who was allegedly not a distinguished scholar: para. 6. The Court found that each of the five *Norwich Pharmacal* criteria had been satisfied on the facts, and granted the order: paras. 25-38.

63 *York University*, *supra*, at para.34.

statements."[64] Second, no one appeared in court to oppose the *York University* application, and the Court noted that it may be appropriate for the ISP to give notice to its customer that it has received such an application, as the customer may wish to consider and assert his privacy and expressive and other interests.[65] Where the anonymous poster has received notice of the application, and elects not to contest the application or assert privacy rights, judicial concern for such interests may reasonably abate. And as set out below, an applicant should, as a matter of good practice, both ethically and strategically, ensure that the ISP does forward the application materials on to its customer to thus provide notice.

Further, the fact that technological advances in the form of the internet offers more secure and surreptitious avenues for tortious activity should not displace the well-established liberal approach to non-party document production where such production is relevant to the claim; in the case of internet defamation, few things are more relevant than the identity of the defendant. The internet does not lessen the importance of documents and facts to the truth-finding process of litigation; and the social importance of that process; to do so would allow the proverbial tail to wag the proverbial dog.

Finally, and as a related point, the fact that the poster seeks to take advantage of the broad avenues for anonymity afforded by the internet should not grant that person greater privacy rights than those enjoyed by litigants in more traditional contexts: the poster of a defamatory advertisement in a newspaper does not enjoy a presumption of rights to privacy or anonymity. Indeed, some courts have found that the very fact that the defendant has sought to hide his identity from the plaintiff to be a factor inclining the court towards an order disclosing the defendant's identity.[66] Indeed the recent cases have recognized that anonymity should generally prompt the granting of disclosure orders, rather than prompt greater protection for the anonymous poster. As stated in *Warman*:

> There is no compelling public interest in allowing someone to libel and destroy the reputation of another, while hiding behind a cloak of anonymity. The requirement

---

64 *York University*, *supra*, at para.39.
65 *York University*, *supra*, at paras. 24 and 38.
66 *Hogan v. Great Central Publishing Ltd.* (1994) 16 OR (3d) 808 (Gen Div), cited in *York University, supra,* at para. 19.

> to demonstrate a *prima facie* case of defamation furthers the objective of establishing an appropriate balance between the public interest in favour of disclosure and legitimate interest of privacy and freedom of expression.[67]

Similarly, the Court in *A.B. v. Bragg Communications Inc.*, concluded that

> In view of a *prima facie* case of defamation, in the absence of any suggestion of a compelling interest that would favour anonymity (such as fair comment), the expectation of anonymity in these circumstances is not a reasonable one. Anonymity is not an automatic shield for defamatory words. ... Defamatory speech does not lose its character as defamation simply because it is anonymous. In these circumstances, where a *prima facie* case of defamation is established, no public interest beyond the general right of freedom of expression is offered in support of maintaining the author's anonymity, I am satisfied that the public interest favour of disclosure prevails.[68]

Time will tell whether British Columbia courts will follow *Warman* generally, or whether the courts will interpret *Warman* to see in the development of the internet a greater judicial protection of those who desire anonymity under the cloak of technology.

VII. ADDITIONAL LEGAL AUTHORITIES

Reported decisions under either the *Norwich Pharmacal* or non-party discovery rules are scarce, even after fifteen years of widespread internet and email use. The following precedents are in addition to those already discussed, above.

a. Ontario

In *Irwin Toy Ltd. v. Joe Doe* the offending communication contained private and confidential electronic files as well as defamatory comments.[69] The forensic investigations identified an internet protocol address traced to refer to a subscriber of iPrimus Canada, an ISP. The ISP could not consent to the application, but did not oppose the application. Wilkins J. observed the lack of jurisprudence on this issue and set down some guiding principles:

---

[67] *Warman*, *supra*, at para. 42.
[68] *York University*, *supra*, at paras. 21-22.
[69] (2000) 12 CPC (5th) 103 (SCJ).

1. generally the ISP ought to preserve internet confidentiality. The ISP is under no obligation to voluntarily disclose the identity of the holder of an internet protocol address.

2. an order will not automatically flow against the custodian of such information upon the provision of a statement of claim. Instead the court must scrutinize such applications such as not to shatter the presumptive anonymity of the internet based upon a potentially spurious claim. An applicant ought to be able to show that the communication was *prima facie* capable of being correctly construed as tortious (whether defamatory, or in breach of confidence).[70]

3. a plaintiff facing an anonymous email will likely be without a remedy unless it can discover the holder of the IP address.

4. the court must consider whether there it would be unfair to oblige the ISP to disclose the identity of the subscriber.

5. under the operative Ontario rule, 31.10, the applicant must show that it has been unable to obtain the information from other persons whom the applicant is entitled to examine for discovery. In such an application, this test would almost always be satisfied.

6. thus generally in such applications, the test may be distilled to allow an order where the applicant shows in its materials a *prima facie* case that John Doe has committed the torts alleged in the action.[71]

Although the *Irwin Toy* principles have been superseded by the principles set out in *Warman, supra,* the *Warman* Court noted that its conclusions were consistent with those in *Irwin Toy,* as well as those in *York University, supra,* and *Sheffield Wednesday Football Club, supra.*

---

[70] In British Columbia, the court would not likely require such proof in a statement of claim. A notice of civil claim setting out the cause of action, coupled with an affidavit in support of the application, should be more than adequate to set out a *bona fide* or *prima facie* case.

[71] *Irwin Toy Ltd. v. Joe Doe, supra,* at para.18.

The *Irwin Toy* Court concluded that the applicant Irwin Toy had satisfied the principles set out above. It demonstrated on a *prima facie* basis that the communication was capable of being correctly construed as defamatory, and that the electronic files were private and confidential. The plaintiff would likely be without a remedy unless it could discover the holder of the IP address. Finally, there would be no unfairness in ordering the ISP to disclose the identity of the subscriber.

b. New Brunswick

In the facts leading to the more brief New Brunswick Court of Queen's Bench decision of *Loblaw Companies Ltd. v. Aliant Telecom Inc.*[72], an email containing confidential information was sent to Loblaws employees. The email was traced to a Yahoo! account and a IP address with the ISP Aliant Telecom. As indicated by the style of cause, the plaintiff proceeded by way of a *Norwich Pharmacal* action, naming the ISP Aliant and Yahoo! as the defendants themselves, rather than John Doe. The New Brunswick Rules of Court in effect codify the *Norwich Pharmacal* principles. As the applicant established a *prima facie* case for relief against the defendant, as the applicant had made reasonable enquiries but had been unable to identify the intended defendant, and as it was likely that the defendants had information identifying the intended defendant, the order was granted.

In *Doucet v. Brunswick News*, the applicant brought a *Norwich Pharmacal* application under Rule 32.12 of the New Brunswick Rules of Court, requesting that the respondent media organizations provide "all information in its possession regarding the identity of the person or persons who posted comments on the "Letters to the Editor" section of a website."[73] The anonymous letter to the editor accused Doucet, a firefighter of being a goon who endangered members of the public. The media organizations did not oppose the application. The Court applied *Leahy*, and granted the order, albeit with a narrower scope: as an order for "all information" might affect the privacy of others, the Court accordingly only ordered release of sufficient information to identify the author.

[72] [2003] NBR (2d) (Supp.) No. 32.
[73] (2010) 363 NBR (2d) 61 (QB)

c. Nova Scotia

In *A.B. v. Bragg Communications Inc.*, the applicant sought from the respondent ISP the identity of an owner of an IP address.[74] The anonymous author had created a fake Facebook profile, attacking the applicant's physical appearance, weight, and sexual history. The applicant relied upon the Nova Scotia Civil Procedure Rules. The Court reviewed and applied *Warman*, and noted the necessity of considering the interest and freedom of expression. It concluded that where only general rights of freedom of expression are raised in the face of a *prima facie* defamation, the order should issue.[75]

In brief oral reasons, the Court in *Mosher v. Coast Publishing Ltd.* ordered the respondents Google and *The Coast* newspaper to disclose information that might assist the applicants in discovering the identity of anonymous internet posters.[76]

d. Orders

Apart from the decisions surveyed above, courts across Canada regularly grant such disclosure orders, issuing brief or no written reasons.[77]

VIII. THE APPLICATION

i. Affidavits in support

An application will usually be supported by two affidavits: one from the client setting out the

---

[74] *A.B. v. Bragg Communications Inc.* (2010) 293 NSR (2d) 222 (SC).

[75] *A.B. v. Bragg Communications Inc.*, *supra*, at para.22.

[76] 2010 NSSC 153

[77] See, for example, the following orders for applications brought under a *Norwich Pharmacal* procedure: *York University v. Google* (14 May 2009) (Ont SCJ), referred to in *York University*, *supra*, at para. 3; *Best Buy Canada Ltd. v. Shaw Cable Systems G.P.*, (25 July 2003) Vancouver Registry No. S033807; *Jordan v. Rogers Telecom Inc.* (15 October 2005) Toronto, Court File No.05-CV-297837PDI; and the following orders for applications brought under non-party discovery rules in "John Doe" applications: *Philip Services Corp. v. John Doe* (24 June 1998), Hamilton Court File No. 4592/98; *Ontario First Nations Partnership v. John Doe* (3 June 2002), File No. 02-CV-229617-CM3 (Ont SCJ); *Canadian Blood Services v. John Doe* (17 June 2002), No. 02-CV-20980 (Ont SCJ).

For further authorities see the Australian decision in *Resolute Ltd. & Anor v. Warnes*, [2000] WASC 35, and the English decisions in *Totalise Plc. v. Motley Tool Ltd.*, [2001] EWCA Civ. 1987 at para. 8, and *Takenaka (UK) Ltd. v. Frankl* (11 October 2000) (QB), referred to in [2001] EWCA 348 at para.3.

material background facts and the harm suffered, and the second from a computer forensics expert setting out the technical paper trail by which the tortfeasor is traced to the ISP.

The affidavit of the plaintiff or representative of the corporate plaintiff should set out the following:

(a) evidence that the email in question is tortious (for example, a corporate policy with respect to confidential information: a company standard-form contract signed by all employees with respect to confidential information, or the like could be attached to show the court that there is a *prima facie* or good claim);

(b) the extent to which the offending email or post was distributed;

(c) the nature and extent of the harm caused by the communications;

(d) the party's reasonable attempts to determine the identity of the sender, through avenues other than the ISP;

(e) the necessity of obtaining the information from the ISP;

(f) the party's willingness to compensate the ISP for all costs associated with the application and the request. Such an assurance may require an undertaking to indemnify the ISP for any proceedings brought, for example, by its customer as a result of the release of that customer's identity.

The technical affidavit should set out the following:

(a) the expertise of the affiant;

(b) confirmation that the affiant has direct knowledge of the forensic investigation, or the grounds for his belief in the facts alleged if carried out by an associate;[78]

(c) the electronic communication in question;

(d) the header information and other revelations through technical forensics;

(e) the deciphering of the header and other electronic information;

[78] See *BMG*, *supra*, at paras. 13, 15(b) and 21, for admonitions against hearsay evidence. In *BMG*, much of the forensic affidavit was ignored as hearsay, as the affiant had not himself carried out the investigations: "major portions of these affidavits are based upon information which Mr. Millin gained from his employees. Accordingly they consist largely of hearsay.... Mr. Millin gives no reason for his beliefs."

(f) an explanation of the IP address, and how it was traced to the respondent ISP;

(g) further information to be garnered and likely conclusions to be drawn from the header information or technical information;

(h) the assumptions on which those conclusions are based;

(i) the reliability of that further information, and the possibility that there may be other explanations for those conclusions;

(j) why the respondent is likely in possession of information about the identity of the sender;

(k) why other potential sources of information about the identity of the sender are likely unhelpful or limited (e.g. as Yahoo does not keep customer billing records and does not take steps to determine whether a given subscriber is using an actual name or address, a request to Yahoo would likely be unhelpful).

ii. The order

It is recommended that the ISP be consulted in advance on the terms of the order. Again, the ISP is likely to take no position nor actively oppose the application if it is satisfied with the terms of the draft order. A typical order is as follows:

> THIS COURT ORDERS THAT:
>
> 1. The Respondent TELUS Communications Inc. disclose to the Plaintiff, within 7 days of receipt of this Order by it, the last known name and mailing address of its subscriber which it believes was assigned the IP address 216.232.136.253 on or about Thursday, September 16, 2004 at 9:55 a.m.;
>
> 2. The Plaintiff pay to TELUS Communications Inc. its administrative costs, including, without limitation, in-house legal fees, related to compliance with this Order forthwith in the amount of $110.00; and
>
> 3. Costs of this application be in the cause.

iii. Service of application materials

The application materials should be served upon the ISP. The ISP will likely have a policy and a practice in place whereby it then forwards those materials on to its customer. Where the communication in question is an email, the plaintiff may also wish to email a copy of the materials to the email address where the offending email originated.

Multiple means of attempted service provide two advantages. First, some John Does, upon receiving notice of the application, will realize that the revelation of his identity is imminent, and turn themselves in.[79] The cost of the application is thus avoided. Second, the more reassurance the applicant can provide to the court that the would-be defendant has likely learned of the application, the more willing the court may be to grant the order. The plaintiff's counsel will wish to advise the court of these attempts to responsibly serve the would-be defendant, although the plaintiff should provide the caveat that given the transitory nature of email accounts, service is certainly not guaranteed.

In any case, it is unlikely that John Doe will reveal himself by attending in chambers to oppose the application. John Doe might dispatch a lawyer to speak on his behalf and attempt to retain his anonymity while simultaneously opposing the plaintiff's application.[80]

IX. PITFALLS, DEAD ENDS AND BLACK HOLES

Of course, such applications do not always end with a neat unmasking of the tortious sender. There are ample means by which a John Doe sender of a defamatory or otherwise tortious email can attempt to evade detection. In other cases, the path may grow cold simply because of John Doe's innocent technological arrangements.

In our wireless age, the wireless router is the most common distorter of the tracing of a tortious email sender through an IP address. Such routers are inexpensive, retailing for $50-$200; electronic stores routinely encourage purchasers of laptop computers to purchase such routers.[81] Such routers permit users to, for example, access the internet and send email via the router from anywhere in their homes. When one purchases and sets up such a router, the accompanying manual usually encourages the user to block unauthorized use of the router. If the user does not

---

[79] This suggestion is not naïve; John Does have actually identified themselves in files that the authors have been involved in.

[80] In the well-publicised case of *Cohen v. Google Inc.* (NYSC Index No. 100012/09, 17 August 2009), in which an anonymous blogger defamed the plaintiff model Liskula Cohen on the charmingly-named website "Skanks in NYC", the anonymous blogger appeared in court anonymously, by dispatched her lawyer to court to argue for the protection of her privacy: see discussion in *York University*, *supra*, at para. 23.

[81] Popular brands of routers include Linksys, Brother, D-Link Gigafast. Apple products include TimeCapsule and Airport Express.

take these simple steps to prevent use by unauthorized users, any person with a laptop or hand-held device within the router's range (typically, with a domestic router, between 75 and 150 feet) can parasitically access the internet or send an email via the unsecured router. Users of such routers are encouraged to secure their routers to avoid being named in a lawsuit based on the use of their routers to send defamatory email. On a practical level, a neighbour "piggybacking" onto an unsecured router will usually cause the router to deliver the legitimate user's internet and email access at a slower rate.

Based on the authors' experience, individuals traced through IP addresses often claim to have an unsecured router, and suggest that it must have been a neighbour or someone else within the router's range that sent the offending email. While this could be true, based on the authors' experiences, it usually is not. It may be necessary to inspect the person's actual computer, through consent or a court order, to test the IP address user's claim by seeing if there are residual traces of the offending email or communication on the hard drive.

Another dead end arises where the sender of the email uses a public terminal, such as a library or an internet café. It is rare for such institutions to require users to sign in. There is a small chance that the internet café may have credit card records or invoices, or user logs, but this is unlikely. Usually this will result in a dead end.

In the future, such investigations will become more and more difficult. As wireless networks spread and with the expected institution of public Wi-Fi terminals throughout cities, it will become more and more difficult to use IP addresses to trace senders of tortious communications.[82] There is no real way to trace individuals who conduct their activities wirelessly, as the only records they leave are their MAC address and sometimes the name of their computer. Most Wi-Fi spots do not keep logs and, if they do, they tend to keep them for a short time. If it is the case of a user sending out emails, it may be possible to obtain an order against the email-hosting provider which may have a record of IP addresses used by that individual on the computers in that location.

[82] See, for example, the recent proposal by Ontario Hydro to provide wireless internet access to the downtown core of the City of Toronto city wireless: see Jeffrey Hawkins, "Wireless Net access to blanket core", *Globe & Mail* (March 8, 2006).

There remain possibilities, however, for identifying the sender. It is not uncommon for a user to create their email address from home and then use a wireless connection to send out emails. The hosting provider in most cases has the account create an IP address, recording the date, as well as the last logged-in IP address. This information may allow the investigator to trace back to the person who paid for the ISP account, and lead to an enquiry to the ISP. However, where a user employs wireless technology and a temporary email provider, such as mytrashmail.com, tracing becomes almost impossible. The identity of such a user would only be possible if other, non-electronic means, such as closed-circuit camera footage or credit card payment records, were available.

A final potential dead end is the use by the sender of software and websites which render communications anonymous to a degree. Examples of such websites include www.ultimate-anonymity.com, anonymizer.com and Anonymity 4 Proxy at inetprivacy.com. These programmes strip away identifying information concerning the IP address by providing a "proxy" service to subscribing users. Essentially, a proxy service acts on behalf of one's computer system in order to send and receive information to a remote host, hiding the original sender's IP address. There are many different types of "proxy" services offered, some for internet traffic ("HTTP"), some for email ("SMTP"), and all different kinds of each. These sites claim that no logs are kept of the transactions carried out, so any subpoenas or orders would be fruitless. In many cases, however, even though these sites do not record the examples of individual access to the site, almost all websites log information for statistical purposes such as how many "hits" they get, what pages people most visited, how many received error messages, and the like. Obtaining these logs from the website provider (if such logs exist) and correlating access times and when emails were sent could provide evidence that a given user used that particular service at a particular time. The next challenge is convincing these providers to recognize a Canadian order or subpoena. Many of these providers reside in countries that do not recognize such orders, or in which domestication and enforcement of those orders is difficult.

X. LAST DITCH ATTEMPTS TO AVOID A DEAD END

Where one hits a dead end, there remains some hope of identifying the sender of the email. It is important with respect to the following that legal practitioners consider their ethical obligations and not expose themselves to allegations of improper behaviour.

If one is unable to determine the identity of a sender of a tortious communication, it may be possible to employ other methods. For example, it may be possible to convince the sender to send another email, allowing for another source of investigative data. The obvious means to obtain this evidence is to simply reply to the original offensive email, and hope that the sender responds. Alternatively, the investigator could perform what is called a "bug". To do so, the investigator must send an email to the original sender that entices the sender into clicking a link to a website. The following is an example of such a link: http://checkthislinkout.mycontrolledwebsite.com/something.html The link resides on a website controlled by the investigator. If the original email sender clicks on that link, the investigator is then able to obtain the computer's internal IP address. Through use of Java or ActiveX code on the "mycontrolledwebsite.com" page, the investigator can defeat all anonymous proxy servers the sender may use to send the email, because the Java/ActiveX code is executed on the originating machine and not on the proxy server.

Alternatively, the investigator could include in the email a picture for the original sender to click on; embedded in the email code is something to the following address: <IMG SRC="http://www.mycontrolledwebsite.com/secretpicture.jpg"> . If a sender opens the email and displays it in html format, the sender's computer would go to www.mycontrolledwebsite.com/secretpicture.jpg". When this occurs, the investigator can obtain the IP address of the original sender. This IP address would be the original sender's actual IP address reflecting the computer that looked at the email.

XI. CONCLUSION

A person posting a defamatory advertisement in a newspaper would enjoy no immunity from disclosure, and to the writers it seems just that a person who defames another via the internet would be treated in the same manner. *Norwich Pharmacal* orders and Rules 7-1(18) and 7-5 of British Columbia's *Supreme Court Civil Rules* allow a defamed party to pursue such a claim. Recent cases have magnified the spotlight on privacy interests and freedom of expression, complicating what a defamed person must do to seek redress. However, so long as a plaintiff acts swiftly and takes technical care in pursuing an action, the judicial processes set out above offer a potential remedy and hope.