

ONTARIO

**SUPERIOR COURT OF JUSTICE
DIVISIONAL COURT**

BETWEEN:

RICHARD WARMAN

**PLAINTIFF
(Respondent)**

AND:

CONSTANCE WILKINS-FOURNIER and MARK FOURNIER

**DEFENDANTS
(Appellants)**

AND:

**JOHN DOES 1-8 (AKA Klinxx; SaskBigPicture; Droid1963; conscience; Faramir; Peter
O'Donnell; Padraigh; and HR-101)**

DEFENDANTS

**FACTUM OF THE INTERVENOR
CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC**

I. Scope of Intervention

[1] CIPPIC has been granted leave to intervene as an amicus curiae intervenor in this appeal. CIPPIC takes no stand on the merits of the case at bar. Its intervention is primarily focused on the need to ensure that privacy and anonymity are given due consideration within the discovery process.

II. Introduction

[2] This appeal raises vital issues relating to the appropriate balance our law strikes between important policy objectives such as facilitating protection of private rights through the discovery process and preserving privacy and online anonymity. In support of this conclusion, CIPPIC intends to address the following issues:

- (a) The role of privacy within the discovery process;
- (b) Challenges posed by anonymity in discovery;
- (c) The proper test for protecting anonymity in discovery

III. Legal Analysis and Argument

A. Privacy in the discovery process

i. Jurisdiction to consider privacy in discovery

[3] Courts have consistently recognized an inherent jurisdiction to protect privacy rights within the discovery process. In criminal discovery, privacy is a live and salient factor that even the section 7 right of an accused to make full answer and defence must be balanced against (*R. v. McNeil*, *R. v. B.(E.)*). In civil suits, courts have contrived various mechanisms to protect privacy of parties in the discovery process, including privilege (*Bean v. Manufacturers Life Insurance*), implied undertakings (*Juman v. Doucette*), screening procedures (*D.P. v. Wagg*) and inherent jurisdiction (*Carter v. Connors*).

Bean v. Manufacturers Life Insurance Co., [2005] 43 C.C.L.I. (4th) 311 (Ont. S.C.), para. 14; *Carter v. Connors*, [2009] 2009 NBQB 317 (N.B. Q.B.), para. 33; *D.P. v. Wagg*, [2004] 71 O.R. (3d) 229 (Ont. C.A.), paras. 14-16; *Juman v. Doucette*, [2008] 1 S.C.R. 157 (S.C.C.), paras. 24-25; *R. v. B.(E.)*, [2002] 57 O.R. (3d) 741 (Ont. C.A.), leave to appeal refused, [2002] S.C.C.A. No. 94 (S.C.C.) at para. 29; *R. v. McNeil*, [2009] 1 S.C.R. 66, 2009 SCC 3, (S.C.C.), paras. 20 and 37-38

[4] The important values furthered by the discovery process will typically outweigh any privacy interest in information being sought, favouring disclosure of all relevant information. This appropriate balance is implicit within most discovery processes, and need not be assessed in the majority of cases. Yet those privacy interests exist in all circumstances, as does the Court's inherent obligation to protect them. As noted in *McNeil*:

Implicit in the Crown's broad duty to disclose the contents of its file under *Stinchcombe* are not the absence of any residual expectation of privacy, but rather the following two

assumptions. The first is that the material in possession of the prosecuting Crown is relevant to the accused's case. Otherwise, the Crown would not have obtained possession of it. The second assumption is that this material will likely comprise the case against the accused. As a result, the accused's interest in obtaining disclosure of all relevant material in the Crown's possession for the purpose of making full answer and defence will, as a general rule, outweigh any residual privacy interest...

Nor is this obligation to balance privacy limited to criminal discovery, as *Juman* makes clear:

discovery is an invasion of a private right to be left alone with your thoughts and papers, however embarrassing, defamatory or scandalous...Yet a proper pre-trial discovery is essential to prevent surprise or "litigation by ambush", to encourage settlement once the facts are known, and to narrow issues even where settlement proves unachievable...The answers and documents are compelled by statute solely for the purpose of the civil action and the law thus requires that the invasion of privacy should generally be limited to the level of disclosure necessary to satisfy that purpose and that purpose alone.

BMG Canada v. John Doe, [2005] 4 F.C.R. 81 (F.C.A.), para. 29; **Juman** (S.C.C.), paras. 24-25; **R. v. McNeil** (S.C.C.) at para. 20

[5] That courts need not consider privacy in every disclosure request is merely because the appropriate balance between privacy and discovery is inherent to most discovery processes as developed. In spite of this, the obligation to protect privacy where that balance fails is the default, not the exception to the rule. This is necessary, as discovery processes result either from Court rules of procedure or the common law, and in either case must account for s. 8 of the *Charter*. While the *Charter* does not apply directly, common law developments cannot be inconsistent with *Charter* values. Discovery mandated disclosures governed by rules of civil procedure have force of statute and are more directly subject to s. 8.

Carter (N.B. Q.B.) at paras. 26-28; **D.P. v. Wagg**, (Ont. C.A.) at para. 18

[6] In pursuit of this basic principle, courts have developed various mechanisms to protect privacy in situations where discovery processes become overly invasive. In *R. v. B.(E.)* the Court acted on common law and constitutional values to protect core biographical but highly relevant and probative data in the complainant's diary. In *Bean*, the Court recognized an individual's relationship with her diary as one worthy of protection under common law privilege. In *Franco*, the court prevented disclosure of medical records whose relevancy was in doubt. In *Carter*, the Court found the "evolution of technological science and its proliferation" as raising new challenges for individual privacy. The Court concluded that applications to retrieve electronic data must demonstrate that the probative value of the data outweighs the degree of privacy therein. Rather than lacking jurisdiction to consider privacy in discovery, the Court's obligation to do so is inherent and nascent in *all* such processes. It manifests, in different forms, where new circumstances emerge to threaten unreasonable invasion of personal privacy.

Bean (Ont. C.A.) at paras. 10-14; **Carter** (N.B. Q.B.) at paras. 29, 36; **Franco v. White**, 53 O.R. (3d) 391 (Ont. C.A.) at paras. 61-64; **R. v. B.(E.)** (Ont. C.A.) at paras. 29, 59-60

ii. Simplified Procedures

[7] Rule 76.03 imposes a “high standard of discovery” on litigants in simplified procedures so as to “promote cost-effective litigation and the expeditious resolution of disputes without compromising procedural fairness.” Expedited discovery procedures are measured against the principle that “time and expense of any proceeding should be proportionate to the amount in dispute and the importance of the issues at stake.” This overriding proportionality principle has recently been enshrined in Rule 29.2 of the Ontario *Rules*. Simplified discovery procedures in Ontario have also been amended to allow for oral discovery under this principle of proportionality. While private suits filed under the simplified procedure regime may result in lower monetary damages, the potential invasiveness of the discovery process is equal or greater than that found in regular discovery and the importance of the issues at stake remains significant.

Honourable C.A. **Osborne**, Q.C., “Civil Justice Reform Project: Summary of Findings & Recommendations”, Civil Justice Reform Project, November 2007, at pp. 26-27, 30; **Lillie v. Bisson**, [1999] 46 O.R. (3d) 94 (Ont. C.A.) at paras. 3-4; **Rules of Civil Procedure**, R.R.O. 1990, Reg. 194, as amend., Rules 29.2, 76.03, 76.04(2)

[8] There is no principled reason to exclude privacy considerations from the simplified discovery process. Nor are such considerations currently excluded. Rule 76.03 explicitly excludes privileged documents listed in schedule ‘B’. Presumably, it similarly applies to documents subject to implied undertakings and to the *Wagg* screening process. It should equally allow for considerations of privacy in other contexts. Where such concerns are potentially at issue, “disclosure should not be automatic upon the issuance of a Statement of Claim.”

Warman v. Doe, [2009] 309 D.L.R. (4th) 227 (Ont. S.C.) at para. 15; **Juman** (S.C.C.) at para. 24

iii. Privacy Protections in Discovery

[9] The judicial obligation to weigh privacy against inherently invasive discovery processes operates in a number of ways tailored to the situations in which such concerns arise. Often it can be achieved through rigorous application of relevance standards. Where the balance between privacy and competing interests favours doing so, it may prevent disclosure altogether. Where this balance is threatened, courts have adapted screening processes to ensure competing interests are weighed prior to disclosure. The overriding principle is to ensure that discovery impacts on privacy no more than “strictly required for the purpose of securing that justice be done.”

Home Office v. Harman, [1983] 1 A.C. 280 (H.L.), per Keith, L.J., at p. 308

[10] Where discovery poses a particular threat to privacy, some concerns may be addressed through rigorous application of relevancy criteria. No special relevancy standard is used, but parties increasingly challenge overbroad disclosures requests otherwise accepted as standard

practice in ‘litigation by avalanche’ discovery. Courts have refused access to entire diaries (*Bean*; *R. v. B.(E.)*), medical records (*Franco*), computer hard drives (noted in *Carter*), or online social network profiles (*Schuster*) on the basis that such requests were overbroad and an unjustified invasion of privacy. The balance between discovery and privacy is often addressed by ordering more tailored disclosure requests to capture only the most relevant of data. As the new *Rules* have narrowed the definition of relevance in discovery, enforcing strict relevance standards may continue to play a role in alleviating such concerns.

Bean, (Ont. C.A.) at para. 15; *Carter*, (N.B. Q.B.) at paras. 35.1, 35-36; *Franco* (Ont. C.A.) at paras. 64-65; *Juman* (S.C.C.) at para. 24; *R. v. B.(E.)* (Ont. C.A.) at para. 40; *Schuster v. Royal & Sun Alliance Insurance Co. of Canada*, [2009] 78 C.C.L.I. (4th) 216 (Ont. S.C.) at para. 39

[11] While relevance remains the “touchstone for determining disclosure and production”, courts will at times impose a balancing test in contexts where the discovery process threatens important social values such as privacy, often as one component of a broader analytical framework. Examples include privilege (*Bean*), Crown disclosure of third party records (*R. v. McNeil*; *R. v. B.(E.)*), disclosure of information protected by implied undertakings (*Juman*), and disclosure of Crown Briefs in civil proceedings (*Wagg*). At times this balancing process is divorced from any broader framework (*Franco*; *Carter*). In most contextual settings, this balance will rarely favour exclusion where criminal innocence is at stake (*McNeil*) and infrequently where evidence is highly probative to a civil action (*Wagg*). Even strong exclusionary rules such as privilege (*R. v. McClure*) and implied undertakings (*Kitchenbaum*) may yield to this balancing of interests. This principled and flexible approach, which Bryant *et. al.* refer to as the “foundation for the law of evidence”, recognizes the balancing of interests that underpins discovery and informs judicial efforts to correct such processes where the balance fails.

A.W. Bryant, S.N. Lederman, and M.K. Fuerst, “The Law of Evidence in Canada”, 3rd Ed., (Markham, ON, LexisNexis Canada Inc., 2009) at ss. 1.80-1.86, 1.95; *Bean* (Ont. C.A.) at para. 14; *D.P. v. Wagg*, [2002] 61 O.R. (3d) 746 (Ont. Div. Ct.), affirm’d [2004] 71 O.R. (3d) 229 (Ont. C.A.) at paras. 12-14; *Juman* (S.C.C.) at para. 32; *Kitchenham v. AXA Insurance Canada*, 2008 ONCA 877 (Ont. C.A.) at para. 64; *R. v. B.(E.)* (Ont. C.A.) at para. 29; *R. v. McClure*, [2001] 1 S.C.R. 445 (S.C.C.) at paras. 41-42; *R. v. McNeil* (S.C.C.) at para. 20

[12] Most judicial frameworks for addressing such concerns are tailored to the specific context that prompted them. With respect to privacy, the inherent invasiveness of the discovery process implicates this important right in a number of contexts, including anonymity.

IV.Challenges posed by anonymity in discovery

[13] Preservation of online anonymity is an important public policy objective. Anonymity is a defining feature of the internet, and as personal lives are increasingly lived – and recorded – in electronic venues, the range of activities that can be linked to anonymous identities will

accordingly grow. Online anonymity raises special challenges, as it relies on the auspices of an intermediary whose interests may not align with those of the anonymous Doe. The nature of anonymity is such as to allow for privacy in a public space – it facilitates sharing or discussion without identity. It will often act as a gateway to revealing personal life choices, and can raise a serious risk to privacy, as well as to free expression, and should be accorded due protection.

i. Privacy in Online Anonymity

[14] In *Irwin Toy v. Doe*, the court stated that without appropriate safeguards in the discovery process, “the anonymity of the internet could be shattered for the price of the issuance of a spurious Statement of Claim and the benefits obtained by the anonymity lost in inappropriate circumstances.” Behind the veil of online anonymity, much may be hidden. It is “possible to learn where one works, resides or shops...financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed.” The Supreme Court recently noted in *R. v. Morelli* the degree to which our lives are increasingly captured and recorded online and in electronic format. Anonymous online activity in particular can now include political discussions, social interactions, or diary-like blog postings recording intimate personal details. This phenomenon is making it “difficult to defend against the loss of individual privacy.” Anonymity is an important social value, underpinned by ss. 8 and 2(b) of the *Charter*, to be protected diligently in discovery in spite of this increasing electronic presence.

BMG, (F.C.A.) at para. 4; ***Carter*** (N.B. Q.B.) at paras. 29, 31-33; ***Irwin Toy Ltd. v. Doe***, [2000] O.T.C. 561 (Ont. S.C.) at para. 17; ***R. v. Morelli***, 2010 SCC 8 (S.C.C.) at paras. 2-3

[15] Debates over protection of online anonymity typically focus on disclosure of online identifiers such as IP addresses, Email addresses, as well as customer name and address information that accompanies them. Courts that view such identifiers in isolation find there is little or no expectation of privacy in the identifiers themselves, stating no one expects names or the fact an individual has an Email or Internet or message board subscription to be kept personal. What these courts ignore is the context in which such identifiers are released – it is not just the Email address or name that is revealed, but the link between that identifier and the “wealth of personal information” already associated with it. Such data, while perhaps not highly private in itself, rapidly becomes at the point of identification “the means by which a biographical core of personal information is assembled” and as such attracts reasonable expectations of privacy.

R. v. Cuttell, [2009] 247 C.C.C. (3d) 424, 2009 ONCJ 471 (Ont. C.J.) at paras. 20-27; ***R. v. Friers***, 2008 ONCJ 740 (Ont. C.J.) at paras. 23-24; ***R. v. Kwok***, [2008] 78 W.C.B. (2d) 21 (Ont. C.J.) at para. 35; ***R. v. Tessling***, [2004] 3 S.C.R. 43 (S.C.C.) at paras. 23-25

[16] Some courts have held that reasonable expectations of privacy in online identifiers exist, but are vitiated by intermediary terms of use. In such cases, the ISP or other intermediary includes in its terms of use a broad disclaimer informing users that personal information may be disclosed in some circumstances in response to allegations of wrongdoing. Typically, the specific conditions under which such disclosures will be made is left open. Under such circumstances, it remains reasonable for users to expect their information to be kept private absent extreme circumstances. In addition, online terms of use documents are similar to form contracts – seldom read in detail, and expected to be reasonable. A subjective expectation that the intermediary will disclose “only in very limited circumstances” may survive such conditions.

Irwin Toy (Ont. S.C.) at paras. 10-11; *McVicker v. King*, 2010 U.S. Dist. LEXIS 18864, (Pa. Dist. Ct.) at p. 15; *R. v. Cuttell*, (Ont. C.J.) at paras. 28-37; *R. v. Tessling*, (S.C.C.) at paras. 38-42

[17] From a policy perspective, it is troubling that non-negotiable contracts with intermediaries should vitiate reasonable expectations of privacy at a societal level. The legal norm is that privacy will not be invaded until some preliminary proof of wrongdoing has been provided and screened. This concept of pre-authorization is at the core of s. 8 jurisprudence in the criminal context. It is the “mutual understanding” between anonymous users and intermediaries found in *Irwin Toy* to be “implicit” in such internet usage. Users would not take the trouble to adopt online pseudonyms if they did not expect anonymity (*R. v. Friers*). Clearly anonymity should not be absolute – privacy rarely is. But users would not expect to be identified simply upon request or allegation of wrongdoing without any verification. For this reason, courts have required parties seeking identification to meet an evidentiary standard before permitting disclosure of identifying documents.

Irwin Toy (Ont. S.C.) at paras. 10-11; *R. v. Friers* (Ont. C.J.) at para. 26

ii. Anonymity and intermediaries

[18] Another feature of online anonymity is that identification data will almost exclusively be under the control of third parties, often with no affinity of interest to the anonymous individual in question. At best, most situations will involve intermediaries intent simply “to get out of the cross-fire as rapidly and cheaply as possible”. In other situations, where intermediaries face potential liability, the motivation to disclose identities and settle may be even stronger.

York University v. Bell Canada Enterprises, [2009] 311 D.L.R. (4th) 755 (Ont. S.C.) at para. 20

[19] *Advicescene v. Law Buzz* is an example where the intermediary defendant discussion board settled the suit against it in part by disclosing the identifiers of its anonymous users. Even in cases where the defendant intermediaries *do* have some affinity of interest, the interests of the anonymous defendants are not fully represented unless the intermediary chooses to consult with them.

Advicescene Enterprises v. Law Buzz Canada, Court File No. CV-09-384447, (Ont. S.C.)

[20] The danger with intermediaries is that they will not in all cases make proper assessments. There have been cases where plaintiffs have “sued everyone in sight”, sometimes merely to get discovery, at other times with a *bona fide* expectation of success. One example is found in *Sheffield*, where the plaintiffs sued 11 anonymous posters to an online discussion, but the comments of 8 did not meet defamation standards. In other situations, there may be uncertain legal issues that do not require identification to resolve. In *Crookes v. Wikimedia*, multiple parties were sued in defamation for posting hyperlinks to an original defamatory article. The issue of whether linking in this manner can even constitute publication under defamation laws is still being appealed. Had the identities of any anonymous Does who posted such a link online been disclosed “automatically”, it would have been a disproportionate and unnecessary invasion of privacy. Intermediaries are not courts of law, and cannot assess the validity of such claims.

Crookes v. Wikimedia Foundation, [2009] 96 B.C.L.R. (4th) 315, 2009 BCCA 392 (B.C.C.A.), leave to appeal pending, [2009] S.C.C.A. No. 448 (S.C.C.); ***Juman*** (S.C.C.) at paras. 24; ***Sheffield Wednesday Football Club Ltd. v. Hargreaves***, [2007] EWHC 2375 (U.K. Q.B.) at paras. 19-20

[21] The potential scope of defamation claims such as those in *Crookes* and *Sheffield* pose a great risk to online privacy. Any online blogger posting a link to a questionable article may have their anonymity revealed, either through intermediary cooperation or by an automatic disclosure process. Without an appropriate screening process:

for the out-of-pocket cost of issuing a statement of claim...the gate is swung open to investigate the private information...of the examinee in pursuit of allegations that might in the end be found to be without any merit at all.

Juman (S.C.C.) at para. 24

iii. Anonymity and other discovery processes

[22] Online anonymity raises similar challenges to other areas where courts have found a need to adjust the discovery process in order to protect privacy. Where privacy is threatened and the degree of relevance or probative value of the information being sought is in question, courts have in the past found it necessary to delay disclosure until a clearer case for disclosure can be established. In extreme cases, where the discovery process may result in a serious invasion of privacy, s. 8 values may require the granting of a temporary injunction to prevent the irreparable harm that would result from disclosure until primary issues are resolved (*CMRRA/SODRAC*). In addition, courts have tended to delay disclosure where disclosure would tend to capture private information of low probative value along with more relevant, necessary information (*R. v. B.(E.)*, *Franco*; *Carter*, *Schuster*).

Groupe Archambault Inc. v. CMRRA/SODRAC Inc., [2005] 53 C.P.R. (4th) 290, 2005 FCA 330, (F.C.A.) at paras. 13, 15; ***Carter***, (N.B. Q.B.) at para. 35; ***Franco*** (Ont. C.A.) at para. 64-65; ***R. v. B.(E.)*** (Ont. C.A.) at para. 40; ***Schuster***, (Ont. S.C.) at paras. 1, 53;

[23] Most judicial protections of online anonymity in discovery to date involve a screening process. Where there is an alleged anonymous wrongdoer, courts are required to delay disclosure of identity until an assessment, by varying standards, of whether the case against her is valid has been completed. While the criminal context is clearly distinct, this is in keeping with the manner in which reasonable expectations of privacy have been protected against allegations of wrongdoing in the past. Indeed, courts have likened the process to a probable cause requirement. Expectations of anonymity are reasonable only until a preliminary case of wrongdoing has been made out. This is the balance that has been struck between competing values such as the need to facilitate private rights enforcement through discovery and privacy.

BMG (F.C.A.); ***Carter*** (N.B. Q.B.) at paras. 26-28; ***D.P. v. Wagg***, (Ont. C.A.) at para. 18; ***Krinsky v. Doe*** 6, 72 Cal. Rptr. 3d 231 (Cal. App. 2008) at p. 33

B. Protecting privacy in discovery

[24] Courts in many jurisdictions have adopted various processes to address the particular issues raised by online anonymity. There are two sets of concerns typically addressed in making such assessments. One is procedural, the other substantive. The test we suggest this Court adopt is as follows.

Process:

- (a) The intermediary, if a party to the proceeding, should disclose the existence of any identifying documents, but should not produce the documents or otherwise identify the users in question;
- (b) The party seeking to identify the individuals in question should take reasonable steps to do so on their own accord and give the anonymous users time to respond;
- (c) The party seeking disclosure should apply to the court to have the anonymous individual's identity disclosed. Reasonable steps should be taken to notify the anonymous Doe and to provide her time to respond or consent to disclosure;

A Court will only order disclosure where:

- (a) The requesting party has demonstrated a prima facie case;
- (b) The balance between the cost and benefit of identifying the individual, weighing competing values such as privacy and free expression and the need to facilitate private rights litigation;

i. Procedure

a) Intermediary as party

[25] Naming the intermediary as a party to the proceeding does not change its fundamental nature as an intermediary. Where the intermediary is named co-defendant, its joinder with other defendants is often essentially for convenience and does not reflect any qualitative difference in its character. The liability of the intermediary will in many cases be severable from that of the anonymous Does. The identities of co-defendant Does will not always be necessary or relevant to the suit against the intermediary, which will revolve around its own actions or inactions. In

such cases, the identifying information should be treated as third party personal information. The intermediary should inform the plaintiff what identifying documents are available.

Sheffield (U.K. Q.B.) at para. 10

b) Attempt self-identification

[26] The party seeking identification should take reasonable steps to do so on its own. In cases where the intermediary has no potential liability, this may preclude its involvement altogether. This will not only be more efficient procedurally, but will avoid the need to rely on exceptional remedies such as Norwich orders.

York (Ont. S.C.) at para. 27

c) Application and notification

[27] If the plaintiff is unable to identify the anonymous users alone, an application should be brought seeking an order from the court to do so. Plaintiffs should make reasonable efforts to inform an anonymous Doe this of such applications to enable her to represent her own interests.

[28] This notification provision “imposes very little burden on a...plaintiff while at the same time giving an anonymous defendant the opportunity to respond.” Meeting this burden can be accomplished by taking steps through the medium in which the anonymous alleged unlawful conduct took place. Posting a notice on a message board may be sufficient. If the medium permits direct contact between users, that should be attempted as well.

Doe v. Cahill, 884 A.2d 451 (Del. Sup. Ct., 2005) at p. 461; *Krinsky* (Cal. App.) at p. 1171

[29] Where no acknowledgement is received from the anonymous defendant, notice may be provided, where possible, through the intermediary. The intermediary will often have ready access to the anonymous Doe, and will be able to notify her of the application with ease. Courts have additionally developed mechanisms to diffuse costs incurred by intermediaries. The notice requirement is not analogous to substitute service, but merely an obligation to take reasonable steps to inform the anonymous user their privacy interests will be at stake in a proceeding. If the anonymous Doe does not respond in time, Courts have proceeded to consider the merits of Norwich/Dendrite applications without the benefit of their presence.

Mobilisa, Inc. v. Doe 1, 217 Ariz. 103 (Ariz. Ct. App. 2007) at paras. 29-30; *York* (Ont. S.C.) at paras. 21-24, 38

[30] The benefits of a notification requirement cannot be understated. It speaks directly to the lack of affinity of interest between intermediaries and anonymous Does. As in *Motley Fool*:

the court must be careful not to make an order which unjustifiably invades the right of an individual to respect for his private life, especially when that individual is in the nature of things not before the court... there are many situations in which...the protection of a person's identity from disclosure may be legitimate...It is difficult to see how a court can

carry out this task if what it is refereeing is a contest between two parties, neither of whom is the person most concerned

The concern is more pressing where the intermediary has *not*, as the ISPs in *Motley Fool* did, undertaken contractually to protect user anonymity. While part of this concern can be mitigated by vesting the ultimate decision to disclose with the Court, as with other *ex parte* motions, anonymous Does should have the opportunity to present their own interests in such proceedings. Indeed, in many cases, the Doe may wish to consent to the identification, precluding the need for any proceeding at all. Where the Does do not respond, the time delay will be slight, as court imposed deadlines for responding can be as short as 20 days. It is for such reasons that, in other similar contexts, the courts have held that notification of those whose privacy rights are implicated is essential (*Juman, McNeil, Wagg*).

Juman (S.C.C.) at para. 52; *Mobilisa* (Ariz. Ct. App. 2007) at paras. 29-30; *Totalise v. Motley Fool Ltd.*, [2003] 2 All E.R. 872, [2001] EWCA 1897 (U.K. C.A.); *R. v. McNeil* (S.C.C.) at para. 27; *Wagg* (Ont. C.A.) at para. 50

ii. Substantive Requirements

[31] Before anonymous identities can be disclosed, the seeking party will typically have to meet two requirements. First, she will have to demonstrate that her claim against the anonymous Doe meets certain standards. Second, she must convince the court that the balance between competing interests favours such disclosure in her particular case.

a) Proof of wrongdoing

[32] Courts have imposed various standards in situations where anonymity is at stake. Some have required the plaintiff to demonstrate a *bona fide* claim, others a *prima facie* case, and still others the capacity to survive a motion for summary judgment.

Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231 (Ct. App. 2008) at pp. 1167-1173

[33] In *BMG*, the Federal Court of Appeal held that an applicant seeking the identity of an anonymous Doe need only demonstrate a *bona fide* intent to pursue the litigation to its completion. This is intended to filter illegitimate complaints aimed at preventing suits filed for the primary purpose of identifying anonymous Does.

BMG (F.C.A.) at para. 34; *McVicker* (Pa. Dist. Ct.) at p. 16; *York* (Ont. S.C.) at paras. 13-16, citing *GEA Group AG v. Ventra Group Co.*, [2009] 96 O.R. (3d) 481 (Ont. C.A.)

[34] When considering this standard in the context of online anonymity, other courts have held that a higher standard of evidence demonstrating a *prima facie* case is required to protect the important *Charter* values at stake in such cases. Thus *York* states that “the requirement to establish a *prima facie* case against the customer before obtaining a court order is a reasonable balance”. Most U.S. courts have found that a *prima facie* standard, requiring more than mere

good intentions to sue, is the lowest standard considered acceptable for protecting anonymity. U.K. courts have additionally adopted a *prima facie* standard with respect to anonymous communications. It is in keeping with s. 8 values that a party seeking to use the state's apparatus to invade a reasonable expectation of privacy should demonstrate some concrete foundation for doing so. Otherwise, anonymity and privacy may be too easily set aside in cases that lack minimal merits. In most cases involving online anonymity, a *prima facie* case is simple to assess as the character of the act can be made out (defamatory statement, copyright infringement, etc.). This standard has been met in many cases.

Irwin Toy (Ont. S.C.); *Krinsky v. Doe* 6, 72 Cal. Rptr. 3d 231 (Cal. App. 6th Dist. 2008) at p.19; *Mobilisa* (Ariz. Ct. App. 2007) at para. 23; *Sheffield* (U.K. Q.B.) at para. 12; *York* (Ont. S.C.) at paras. 13, 25, 27

[35] U.S. courts have applied a more rigorous standard, requiring the plaintiff to demonstrate its capacity to survive a motion for summary judgment on all elements not dependent on the anonymous Doe's identity. Some courts have held this standard is necessary to ensure that anonymous free speech is sufficiently protected from undue infringement. It would allow the Doe defendant to present evidence so as to defeat *prima facie* elements of a suit brought against her that are not reliant on her identity.

Krinsky (Cal. App. Dist.) at pp. 1168; *Mobilisa* (Ariz. Ct. App.) at para. 23

[36] As noted in *Krinsky*, "common to most courts...is the necessity that the plaintiff make a *prima facie* showing". Many defamation and similar cases will involve fact scenarios with statements that are defamatory on their face. In such cases, meeting this standard will be no serious bar. A well intentioned suit should not be permitted to intrude on anonymity where, for example, it is clear that defamatory statements do not meet the legal test (*Sheffield*) or where there are serious legal questions to resolve (*Crookes*). In some cases, a *prima facie* standard may not be sufficient. In adopting the summary judgment standard, the court in *Mobilisa* reasoned it may, in a whistleblower or similar case, wish to allow an anonymous Doe to challenge a claim with evidence so as to advance a truth defence against a defamation suit.

BMG (F.C.A.) at para. 34; *Crookes*, (B.C. C.A.); *Sheffield*, (U.K. Q.B.) at paras. 19-20; *Krinsky* (Cal. App. Dist.) at p. 1171 and 1168; *Mobilisa* (Ariz. Ct. App.) at para. 19

b) Balance of competing interests

[37] This last component of the screening process is necessary to ensure the proper balance is struck between competing values. With the appropriate process and standard of proof in place, the balance of competing interests will effectively be set for most cases where anonymous identity is sought to protect private rights in discovery. This final balancing step will be, in most cases, a formality. In extreme cases, it will operate to correct imbalances.

[38] For example, if a *bona fides* standard is selected, and a large number of anonymous Does are sought where there is minimal hope of success, the balance will in many cases weigh against immediate disclosure. In such cases, anonymous Does will have additional potential remedies to correct for an improperly calibrated test, such as moving for summary judgment against the plaintiff (Rules 20, 21) and applying for an interim injunction to protect their identities from irreparable harm (*CMRRA/SODRAC*; *Schuster*). In other cases where a *bona fides* standard may facilitate a means of highly intrusive privacy invasion where probative value to relevant issues is low (*Bean*; *Carter*; *CMRRA/SODRAC*), or where personal information of third parties is involved, this balance may also weigh more heavily against disclosure (*McVicker*, *Carter*). It can similarly be employed where speech deserving higher protection under s. 2(b) is at issue.

Carter (N.B. Q.B.) at paras. 37, 39; **CMRRA/SODRAC Inc.** (F.C.A.) at para. 16; **McVicker** (3rd Cir.) at pp. 16-17; **Bean** (Ont. C.A.); **Schuster** (Ont. S.C.) at paras. 40, 53; **Sheffield** (U.K. Q.B.) at paras. 12, 20; **Rules**, Rules 20, 21

[39] This component can also correct for situations where an adopted standard proves too onerous. In some more complex cases, for example, a plaintiff might find it difficult to prove, with supporting affidavit evidence, a *prima facie* case with respect to all elements of her claim not related to anonymity in order to survive an order for summary judgment. In such cases, a court may find the balance weighs in favour of identifying the anonymous Doe in spite of this.

[40] CIPPIC submits that this test best balances the need to facilitate private rights dispute resolution through the discovery process and the need to preserve privacy and online anonymity.

V. Remedy

[41] CIPPIC takes no position with respect to the outcome of the case at bar. CIPPIC asks for no costs and, in accordance with our intervention order, asks that no costs be awarded against it.

ALL OF WHICH WE RESPECTFULLY SUBMIT,

Tamir Israel

Lawyer for the Intervenor,
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic