"Revenge Porn", Tort Law, and Changing Socio-Technological Realities: A Commentary on *Doe 464533 v ND*

Yuan Stevens*

Table of Contents

Introduction

How can Canadian tort law capture unforeseen breaches of privacy that occur due to technological change? This is one question at the heart of a recent Ontario Superior Court decision, *Jane Doe 464533 v. D. (N.)*.[1] The case concerned what is colloquially known as "revenge porn", where the defendant publicly shared a sexual video of the plaintiff without consent. Legal experts celebrated the Court's initial decision to find the defendant liable for public disclosure of private facts.[2] While the *Doe* decision is of limited precedential value, it nonetheless serves as a fruitful site of exploration as Canadian courts invariably respond to cases dealing with breaches of privacy facilitated by emerging technology. Indeed, understanding such decisions in light of ever-changing technological and social norms demonstrates that Canadian courts should not adopt the tort of public disclosure of private facts, but should instead embrace a reasonable expectation of privacy test for invasion of privacy claims.

---

* B.C.L/LL.B Candidate, McGill University Faculty of Law. This paper was originally a term paper written for a course taught by Professor Margaret Somerville. The author wishes to thank Professors Robert Leckey, Angela Campbell, Peter Szigeti, Lara Karaian, Chris Hunt, and Amar Khoday for their very helpful comments on this project.

1 2016 ONSC 541, 2016 CarswellOnt 911 (Ont. S.C.J.) [*Doe*].

2 Michelle McQuigge, "Experts applaud ruling against man who posted ex's explicit video online", *CBC News* (27 January 2016), online: <http://www.cbc.ca/news/canada/toronto/explicit-video-ruling-1.3422694>.

Why should a reasonable expectation of privacy test inform the overarching invasion of privacy tort? To answer this question, Part I summarizes the facts and judicial history of the *Doe* decision, and canvasses the legal framework for personal privacy rights in Canada. Part II demonstrates that the tort of public disclosure of private facts is ill-equipped to confront unforeseen breaches of privacy that occur due to technological and social change. Specifically, the requirement that the publicized matter concern the *private* life of another suffers from significant conceptual shortcomings. Instead, the distinction between "private" and "public" can be understood as a matter of degree in context. The tort's requirement of "highly offensive" furthermore acts as a limiting qualifier that ultimately undermines the basis for the action; namely, that invasions of privacy are an affront to one's dignity. Instead, whether public disclosures of private facts violate entrenched normative standards should be one factor in an invasion of privacy claim. To this end, all Canadian jurisdictions ought to adopt a reasonable expectation of privacy test to assess invasions of privacy, and can look to the both the writing of privacy expert Helen Nissenbaum and English courts to decide the contours of this standard. While such analysis draws considerably on the work of other privacy experts,[3] this case comment offers critical synthesis in this evolving area of law, and serves as a platform for further scholarly inquiry.

1. BACKGROUND AND LEGAL CONTEXT

1.1 The Facts of *Jane Doe 464533 v. D. (N.)*

The facts of the *Doe* decision are simple. The case arose out of a civil liability claim based on the actions the defendant, ND, who publicly shared a sexually explicit video of the plaintiff, Jane Doe, without her consent.[4] Jane alleged that ND pressured her into making the sexual video, and promised that no one else would see the video before she sent it to him.[5] She eventually learned that ND had posted the video on the user submissions section of a pornography website, calling it: "college girl pleasures herself for ex boyfriends [*sic*] delight."[6] ND posted the video the same day he received it.[7] The video was up for approximately three weeks before he removed it. It is unknown how many times the video was viewed, downloaded, copied onto media storage devices, and potentially shared.[8] Jane eventually sought compensatory and punitive damages as well as a permanent injunction to prevent any further such conduct by ND.[9]

---

3 In particular, I draw on the work of Chris Hunt, Helen Nissenbaum, and Nicole Moreham.

4 *Doe, supra* note 1 at paras. 6 and 8.

5 *Ibid,* at para. 7.

6 *Ibid,* at para. 8.

7 *Ibid.*

8 *Ibid,* at para. 10.

1.2 The Court's Initial Decision and Reasoning

The Ontario Superior Court ("the Court") initially ruled in Jane's favour. Stinson J., writing for the Court, noted ND to be in default and concluded that the common law should evolve to recognize the tort of public disclosure of private facts. He emphasized the practical need for the tort, and observed that technology has increasingly "enabled predators and bullies to victimize others by releasing their nude photos or intimate videos without consent."[10] Justice Stinson recognized the overarching lack of an available common law remedy and case law for "victims" whose sexual or intimate images had been distributed without their consent.[11]

Justice Stinson concluded that there are both established and developing legal grounds to provide civil recourse in such circumstances, and relied heavily on the landmark Ontario Court of Appeal decision, *Jones v Tsige*.[12] The Court of Appeal determined that Ontario law ought to recognize the tort of intrusion upon the seclusion of another's private affairs or concerns.[13] The court in *Tsige* established its decision in the principle that the right to privacy is both "integral to our social and political order" [14] as well as "grounded in . . . physical and moral autonomy" that is "essential for the well-being of the individual."[15] The court in *Tsige* turned to jurisprudence before the Supreme Court of Canada, recommending that the common law develop in a manner consistent with *Charter* values.[16] It also emphasized that recent technological change poses a particularly significant threat to privacy protection.[17]

The courts in both *Tsige* and *Doe* essentially adopted the respective actions of "intrusion upon seclusion" and "public disclosure of private facts" established

---

9 *Ibid,* at para. 1.

10 *Ibid,* at para. 16, likely referring to cases of Rehtaeh Parsons and former judge Lori Douglas, both of whom were victims of the non-consensual sharing of sexual images or videos in which they were depicted. See e.g. "Rape, bullying led to N.S. teen's death, says mom", *CBC News Nova Scotia* (9 April 2013), online: <http://www.cbc.ca/news/canada/nova-scotia/rape-bullying-led-to-n-s-teen-s-death-says-mom-1.1370780> and "Judge Lori Douglas's offer to retire early accepted by judicial panel", *CBC News Manitoba* (24 November 2014), online: <http://www.cbc.ca/news/canada/manitoba/judge-lori-douglas-s-offer-to-retire-early-accepted-by-judicial-panel-1.2846980>.

11 *Doe, supra* note 1 at paras. 18-19.

12 2012 ONCA 32, 2012 CarswellOnt 274 (Ont. C.A.) [*Tsige*].

13 *Ibid,* at paras. 65 and 70.

14 *Ibid,* at para. 68.

15 *Ibid,* at para. 40, affirming, *inter alia*, *R. v. Dyment,* 1988 CarswellPEI 73, 1988 CarswellPEI 7, [1988] 2 S.C.R. 417 (S.C.C.) at 427 [*Dyment*].

16 *Ibid,* at para. 45, affirming, *inter alia*, *R.W.D.S.U. v. Dolphin Delivery Ltd.*, 1986 CarswellBC 411, 1986 CarswellBC 764, [1986] 2 S.C.R. 573 (S.C.C.) at para. 46; *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c.11[*Charter*].

17 *Tsige, supra* note 12 at paras. 67-68.

in the *Restatement of Torts (Second)*, which persuasively restates common law trends and recommendations for American courts.[18] Justice Stinson adopted a modified version of the tort of public disclosure of private facts as follows:

> "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of publication a) would be *highly offensive* to a reasonable person, and b) is not of legitimate concern to the public."[19]

Justice Stinson held that the cause of Jane's action had been made out. ND had "made public an aspect of the plaintiff's private life" when he posted "a privately-shared and highly personal intimate video recording of the plaintiff" on the internet.[20] Further, Justice Stinson found that a "reasonable person would find such activity, involving unauthorized public disclosure of *such a video* to be *highly offensive*" and that "[i]t is readily apparent that there was no legitimate public concern in him doing so."[21] Justice Stinson, analogizing Jane's harm to sexual battery, granted injunctive relief and awarded her $50,000 for general damages, $25,000 for aggravated damages, and $25,000 for punitive damages, including both the costs of the action and the motion on a full-indemnity basis.[22]

1.3 Procedural Developments: A Learning Opportunity

In January 2017, the Court dismissed Jane's motion for leave to appeal from its previous decisions, which set aside both the finding of ND's liability and Justice Stinson's previous assessment of damages.[23] Such decisions offer fascinating glimpses into key pressing procedural issues before the Court, yet an explanation of the Court's latest reasoning is unwarranted for this comment's purposes. However, the Court's dismissal did indeed overturn the Court's establishment and interpretation of the tort of public disclosure of private facts.

Despite these procedural developments, the *Doe* decision affords Canadian jurists a rich learning opportunity. Out of Commonwealth and American jurisdictions, Canadian courts have been particularly cautious in their adoption of personal privacy torts.[24] We therefore have the dual benefit and challenge of crafting our privacy tort(s) in light of those who have come before us,

---

[18] *Restatement (Second) of the Law of Torts* § 652D (1977) [*Restatement*]; Meg Kribble, "Secondary Sources: ALRs, Encyclopedias, Law Reviews, Restatements, & Treatises", *Harvard Law School Library* (guide), online: < http://guides.library.harvard.edu/c.php?g = 309942&p = 2070280 > .

[19] *Doe, supra* note 1 at para. 46, modification shown by underlining, emphasis added.

[20] *Ibid,* at para. 47.

[21] *Ibid,* emphasis added.

[22] *Ibid,* at paras. 53-65.

[23] *Jane Doe 464533 v. D. (N.)*, 2017 ONSC 127, 2017 CarswellOnt 163 (Ont. S.C.J.). at 101. 102.r shared material and y accessedlikely inge ation ing employee eamil es. s codified in the ical need for

particularly with a commitment to capturing unexpected breaches of privacy made possible by emerging technologies and social change.

1.4 Canadian Privacy Law

Everyone in Canada has the right to freedom from unreasonable search and seizure under section 8 of the *Charter*.[25] The *Criminal Code* was amended in 2014 to include a new offence of "publication of an intimate image without consent",[26] which was not available to Jane when she brought her claim to court.

Canada also has a complex "patchwork" set of private sector,[27] public sector,[28] and sector-specific[29] privacy laws.[30] Four common law provinces (Manitoba, British Columbia, Saskatchewan, and Newfoundland and Labrador) currently have legislation that establishes a tort of invasion of privacy, and each are similar to one another.[31] Specifically, all four statutes refer to the importance of the nature and degree of the plaintiff's privacy entitlement, which is circumscribed by what is "*reasonable* in the circumstances."[32] The personal right to privacy under Quebec law is explicitly protected by arts. 3 and 35-37 of the *Civil Code of Quebec*[33] and s. 5 of the *Quebec Charter of Human Rights and Freedoms*.[34]

The Intimate Image Protection Act came into force in Manitoba in January 2016, and expressly created a new tort of nonconsensual distribution of intimate images.[35] The *Act* defines an intimate image as one that has been recorded in circumstances that gave rise to a "*reasonable expectation of privacy*" in the picture or recording at the time it was distributed.[36]

---

[24] Chris D.L. Hunt, "Privacy in the Common Law: A Critical Appraisal of the Ontario court of Appeal's Decision in *Jones v Tsige*" (2012) 37:2 Queen's L.J. 665 at 667.

[25] *Charter, supra* note 16.

[26] *Criminal Code*, R.S.C. 1985, c. C-46, as amended at s. 162.1.

[27] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[28] *Personal Health Information Protection Act*, S.O. 2004, c. 3, Schedule A; *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31; *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

[29] See e.g. *Consumer Reporting Act*, R.S.O. 1990, c. C.33.

[30] Lisa R. Lifshitz, "A New Tort is Born! Ontario Recognizes its First Privacy Tort", *Business Law Today* (March 2012) 1, online: < https://www.americanbar.org/publications/blt/2012/03/keeping_current.html > .

[31] *Tsige, supra* note 12 at para. 52; *Privacy Act*, R.S.M. 1987, c. P125; *Privacy Act*, R.S.B.C. 1996, c. 373; *Privacy Act*, R.S.S. 1978, c. P-24; and *Privacy Act*, R.S.N.L., 1990, c. P-22 [referring to all legislation as *Privacy Acts*].

[32] *Privacy Acts, supra* note 31; Daniel Burnett, "Privacy Torts in Common Law Provinces" (1998) online: < http://www.adidem.org/Privacy_Torts_in_Common_Law_Provinces > , emphasis added [This source is no longer available at this address].

[33] *Civil Code of Québec,* arts. 3 and 35-37 C.C.Q.

[34] *Charter of Human Rights and Freedoms*, C.Q.L.R. c. C-12 s. 5.

[35] *The Intimate Image Protection Act*, S.M. 2015, c. 42, C.C.S.M. c. I87, at s. 11(1) [*IIPA*].

2. CRITICAL REFLECTIONS ON THE *DOE* DECISION

There is no doubt that the court's decision to develop the tort of invasion of privacy in the present case was welcome. Nevertheless, there are difficulties in the *Doe* decision that may undermine the tort's effectiveness for future claims, particularly with respect to unanticipated breaches enabled by new technologies. Privacy and common law expert Chris Hunt came to a similar conclusion in his analysis of *Tsige*.[37] Indeed, two key problems that he analyzed in his critical appraisal of that case are equally problems in this decision and warrant analysis here.

2.1 Public and Private: A Matter of Degree, in Context

The distinction between private and public may best be understood as a matter of degree in context rather than kind; such arguments are not new.[38] Recall that a key element of this tort is the distribution of another's *private* facts.[39] This element of the tort operates as a definitional filter, and is typically contrasted with *public* facts.[40] But when used descriptively, this test offers little clarity due to its assumption that these two concepts are in stark contrast with one another.[41] Instead, any perceived bright line between private and public ought to be reconsidered, because these concepts are not mutually exclusive categories, but are instead generally matters of degree existing on a continuum.[42]

The presumed dichotomy of public versus private can reflect a logical error, notably the "fallacy of bifurcation."[43] Numerous examples illustrate this fallacy. Elizabeth Paton-Simpson, Statutory Officer at the New Zealand Ministry of Justice, pointed to public records in New Zealand, such as birth and death certificates that are always available for public inspection but are also private, since most are never accessed and remain hidden from public view.[44] Information science and privacy expert Helen Nissenbaum particularly observed that new

---

36 *Ibid,* at s. 1(1), emphasis added.

37 Hunt, *supra* note 24.

38 Duncan Kennedy, "The Stages of the Decline of the Public/Private Distinction" (1982) 130 U. Pa. L.R. 1349; Jeff Alan Weintraub & Krishan Kumar, *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy* (Chicago: University of Chicago Press, 1997); Anne Deegan, "The Public/Private Law Dichotomy and its Relationship with the Policy/Operational Factors Distinction in Tort Law" (2001) 18 Q.U.T. Law J.Jl., online: <http://www.austlii.edu.au/au/journals/QUTLawJJl/2001/18.html>.

39 *Doe, supra* note 1.

40 Hunt, *supra* note 24 at 682.

41 *Ibid,* at 682.

42 *Ibid.*

43 *Ibid,* at 683.

44 *Ibid*; Elizabeth Paton-Simpson, "Private Circles and Public Squares: Invasion of Privacy by the Publication of 'Private Facts'" (1998) 61:3 Mod. L. Rev. at 327.

technologies reveal the fuzziness of such definitions.[45] One excellent question is whether posts or messages on social media websites constitute private or public information,[46] a proper determination of which would likely hinge on such factors as the degree of publicness of any written or shared material. Another example concerns the status of online activity in the workplace such as accessing email and the internet, which was conceived in the early 1990s as personal and inviolate.[47] Yet what was once private in the workplace is increasingly open to monitoring by employers and their representatives.[48] Finally, legislation such as the *USA Patriot Act* has given government agencies far greater leeway to infiltrate a broad variety of spheres previously considered private, including digital bank, telephone, and even library records.[49]

Canadian courts ought to consider Nissenbaum's three dimensions of the public/private distinction, which determines the *degree* of privacy in light of (1) the *actors*, which she divides into government and private actors; (2) the dimension of *realm*, including geographic and abstract spaces that can also be divided into the public and private; and (3) the *type* or *nature* of information, which can be divided into public or personal.[50] Analysis of the third dimension would be particularly helpful in determining the scope and extent of privacy protection when distributed information or material is at issue.[51] This is because it can help courts to determine whether the material at hand was already known to the world at large, or whether it is of legitimate concern to the public.

2.2 Problems with the "Highly Offensive" Standard

Canadian courts should abandon the high offensiveness criterion, which not only compromises the very basis of the action — to recognize invasions of privacy that are an affront to one's dignity — but also threatens to be both overbroad *and* under-inclusive when it comes to technological advancements. Recall that Justice Stinson adopted a modified version of the *Restatement* standard: a defendant will be liable if they disclose matters concerning the private life of another, so long as the act of publication or even *the matter* itself publicized would be "highly offensive to a reasonable person."[52] The court in *Tsige,* echoing the *Restatement,* held that the qualifier of "highly offensive" attempts to act as a limiting principle, excluding claims brought by "individuals

---

45 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010) at 101.

46 *Ibid,* at 102.

47 *Ibid,* at 101.

48 *Ibid.*

49 *Ibid,* at 102.

50 *Ibid,* at 96.

51 *Ibid,* at 96-98.

52 *Doe, supra* note 1 at para. 46, modification shown by underlining.

who are sensitive or unusually concerned about their privacy" and intrusions that are not "significant."[53]

Hunt, drawing on the work of fellow privacy law expert Nicole Moreham, asserted that the high offensiveness standard obscures the fact that protecting privacy is integrally bound up with the dignity of the individual.[54] Moreham defines dignity as the principle that one should respect the intrinsic value of all persons, and seek, insofar as possible, to further their ends as well as one's own.[55] Therefore to treat someone "merely as something to be looked at, listened to, found out about, or reported on" against their wishes is therefore to ignore their right to respect as a person.[56] An individual's subjective sense of dignity is quite plainly too broad and protean a basis upon which to build a legal action (indeed an objective test will always be needed).[57] Yet, Canadian courts ought to inform their development and application of personal privacy tort law with an understanding of the dignitary nature of the privacy interest.[58]

Many decisions of the Supreme Court of Canada already recognize the relationship between privacy and dignity. In the landmark decision of *R. v. Plant,* Sopinka J. held that dignity, integrity, and autonomy underlie the right to informational privacy;[59] that is, the right to communicate or retain all information about a person, as such information is in a fundamental way one's own.[60] While the *Charter* does not apply to common law disputes between private individuals, the Supreme Court has both expounded the principle that the common law should develop in a manner consistent with *Charter* values, and determined that the perseveration of dignity is a core value that underpins the right to privacy.[61]

The high offensiveness standard also has the effect of distracting courts from the dignitary interest at stake in privacy claims, and focuses instead on irrelevant

---

53 *Tsige, supra* note 12 at para. 72.

54 Hunt, *supra* note 24 at 689, citing Nicole Moreham, "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in Finn, J. & Todd, S. (eds), *Law Liberty, Legislation: Essays in Honour of John Burrows Q.C.,* (Wellington: LexisNexis, 2008) at 231.

55 Moreham, *supra,* at 236.

56 *Ibid.*

57 *Ibid,* at 238.

58 *Ibid.*

59 *R. v. Plant*, 1993 CarswellAlta 566, 1993 CarswellAlta 94, [1993] 3 S.C.R. 281 (S.C.C.) at 293, affirmed *R. v. Tessling*, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352 (S.C.C.) at para. 25 [*Tessling*].

60 *Tsige, supra* note 12 at para. 41, affirming *Tessling*, *supra* note 59 at para. 23.

61 See e.g. *R. v. Saeed,* 2016 SCC 24, 2016 CarswellAlta 1145, 2016 CarswellAlta 1146 (S.C.C.); *R. v. Fearon*, 2014 SCC 77, 2014 CarswellOnt 17202, 2014 CarswellOnt 17203 (S.C.C.); *R. v. Gomboc*, 2010 SCC 55, 2010 CarswellAlta 2269, 2010 CarswellAlta 2270 (S.C.C.); *R. v. Golden*, 2001 SCC 83, 2001 CarswellOnt 4253, 2001 CarswellOnt 4301 (S.C.C.); *Dyment*, supra note 15.

considerations. For example, New Zealand courts satisfying the highly offensive element have scrutinized the *tone* of the publicity, analyzing whether it cast the plaintiff in a positive or embarrassing light.[62] In the case of *Andrews v Television New Zealand,* the court there held that the broadcast of detailed car crash footage did not meet the standard of "highly offensive", despite the plaintiffs having a reasonable expectation of privacy with respect to the conversations at the time.[63] In essence, the broadcast was not highly offensive because it did not make the plaintiffs "look bad."[64] Moreham compellingly argues that the defendant's decision to turn a private trauma into a public spectacle was the crux of the issue, and not whether the tone of the feature presented the plaintiff in a positive or negative light.[65] If privacy is fundamentally linked to dignity then all breaches would be highly offensive to a reasonable person.[66] By including the highly offensive requirement, courts relying on the initial *Doe* decision are likely to focus on inappropriate questions, distracting from the dignitary nature of the privacy interest.

The high offensiveness standard is liable to be both overbroad and under-inclusive regarding new circumstances made possible by emerging technologies. One critical problem in the *Doe* decision: Justice Stinson never clarified the test for high offensiveness. Indeed, the Court merely held that a judge can find both the act of publication or *the material itself* highly offensive in order to constitute an invasion of privacy.[67] It is startling that the court retained the latter element. This benchmark in *Doe* can effectively operate as an appeal to a judge's instinctive feeling about what material ought to be publicly shared or not,[68] and what deserves protection under Canadian privacy law. It is not difficult to see that by deciding that the publicized matter is itself highly offensive, judges make value-laden determinations of the societal acceptance of all kinds of material—whether it involves, for example, nude images or videos shared through electronic means, or conversations of a sexual nature that occurred in the digital sphere. By affording judges such significant leeway in the determination of high offensiveness, the tort of public disclosure of private facts allows judges to find liability concerning the sharing of *any* sort of material that they might not approve of. For these reasons, future courts should reject the inclusion of the high offensiveness standard.

The highly offensive threshold is also insufficient insofar as it leads to under-inclusivity with respect to technological development, but courts can begin to

---

62 Moreham, *supra* note 54 at 241, citing *Andrews v. Television New Zealand*, [2006] NZHC 1586 (N.Z.H.C.) [*Andrews*].

63 *Andrews*, *ibid.*.

64 Moreham, *supra* note 54 at 241.

65 *Ibid.*

66 *Ibid,* at 243.

67 *Doe*, *supra* note 1 at para. 46.

68 Moreham, *supra* note 54 at 246.

remedy this by considering contextual factors. Indeed, clarification in the *Restatement* states that "[t]he protection afforded to the plaintiff's interest in [their] privacy must be relative to the customs of the time and place, to the occupation of the plaintiff, and to the habits of [their] neighbors and fellow citizens."[69] Nissenbaum cogently argued that judges should consider examining the *level of commonness* of using such technology in a given context; if such use is *known*; and whether the particular use of the technology in question *violates or conforms* to relevant context-specific norms.[70]

Judges will undoubtedly find such contextual analysis particularly useful in the context of new technology. Consider the following seemingly innocuous types of technical systems: closed-circuit television (CCTV) used in public spaces, radio frequency identification (RFID) increasingly installed in consumer and government service items, the mining of large aggregated databases, the use of thermal imaging to detect heat patterns emanating from residences, and facial recognition software.[71] Nissenbaum reminds us that judges cannot generalize from the observation that certain uses of technology in certain contexts are commonplace, accepted, and supported, in order to conclude that all such uses will *not* violate the right to privacy.[72] In other words, judges cannot merely assess how common a given technology is and how familiar people are with them, but must instead analyze whether its use in a particular *context*, in a particular *way* is *so* unusual as to indicate that the publication has violated standing societal conventions.[73] In so doing, judges are far better equipped to assess invasions of privacy through their discretion and wisdom, paired with determining both relevant norms and eventually which cases constitute reasonable analogies and which do not.[74]

2.3 A Promising Standard: Reasonable Expectation of Privacy

Canadian courts should determine invasions of privacy through a standard that prioritizes such detailed contextual analysis as the reasonable expectation of privacy test. More specifically, this test is sensitive to the plaintiff's own views in order to respond to the essentially subjective nature of privacy.[75] And as mentioned above, the test must also comprise an objective facet to avoid a tort that is insupportably broad.[76] The current approach in English law satisfies each of these criteria.

---

69 *Restatement, supra* note 18.

70 Nissenbaum, *supra* note 45 at 235.

71 *Ibid.*

72 *Ibid.*

73 *Ibid,* at 234-235.

74 *Ibid,* at 235.

75 Hunt, *supra* note 24 at 686.

76 *Ibid.*

Hunt compellingly argues that Canadian courts' efforts are in fact better served by following the influence of the newer, more principled developments in England than by adopting the bifurcated and categorical analysis of the American model.[77] Indeed, English courts — cautious in their recognition and development of the tort of invasion of privacy[78] — have rejected the "highly offensive" approach in favour of the reasonable expectation of privacy test.[79]

English courts employ what functions as a subjective-objective analysis. They consider all the circumstances relating to the particular individual — including their expectations in relation to the information or activity in question — and use the objective element to assess whether, in the circumstances, these expectations are reasonable.[80] The test, taken here from the English Court of Appeal decision, *Murray v Express Newspapers,* can include analysis of elements such as :

1) the *attributes* of the claimant,
2) the *nature of the activity* in which the claimant was engaged,
3) the *place* at which it was happening,
4) the *nature* and *purpose* of the intrusion,
5) the *absence of consent* and whether it was *known* or could be *inferred*,
6) the *effect* on the claimant, and
7) the *circumstances* in which and 8) the *purposes* for which the *information came into the hands* of the *publisher*.[81]

Courts could incorporate Nissenbaum's contextual factors regarding emerging technologies into the second element, which evaluates the nature of the activity in which the defendant was engaged.

The benefits of adopting the reasonable expectation of privacy test are numerous. First, the reasonable expectation of privacy test offers Canadian courts a far more effective analytical toolkit with which to assess invasions of privacy facilitated by technological and social change than does the bifurcated and categorical *Restatement* approach. By first framing the inquiry from the plaintiff's perspective, this test allows judges to take stock of the plaintiff's subjective expectations, thereby responding to the underlying, subjective reasons as to why an invasion of privacy claim can arise[82] — all while particularly

---

77 *Ibid,* at 667.

78 *Ibid,* at 666.

79 See *Campbell v. MGN Ltd.,* [2004] UKHL 22 (U.K. H.L.) at paras. 21-22; *Mosley v. News Group,* [2008] EWHC 1777 (available on QL) (Q.B.) at para. 7; *LNS v. Persons Unknown,* [2010] EWHC 119, [2010] 1 FCR 659 (Q.B.) at para. 55; *Regina ex rel Wood v. Metropolitan Police Commissioner,* [2009] EWCA Civ 414 at para. 34, [2010] 2 LRC 184 (C.A.) at paras. 24-25.

80 Hunt, *supra* note 24 at 687, citing Hilary Delany & Eoin Carolan, *The Right to Privacy: A Doctrinal and Comparative Analysis* (Dublin: Thompson Round Hall, 2008) at 299.

81 *Murray v. Express Newspapers plc.,* [2008] EWCA Civ 446, [2009] Ch 481 (C.A.) at paras. 35-36, emphasis added.

82 Hunt, *supra* note 24 at 687.

keeping in mind the importance of ensuring individual dignity. The objective aspect makes clear to both judges and parties before the court that prevailing social norms are critical markers informing the assessment of whether a claim has been established.[83] In contrast, while judges are also bound to consider social norms under the high offensiveness standard, the two-step reasonable expectation of privacy test explicitly accounts for this factor and thus promotes predictability.

Second, the test is flexible and inherently well-positioned to respond to unforeseen privacy threats arising from technological and social changes,[84] avoiding the problems of being overbroad *and* under-inclusive that characterizes the standard of "highly offensive."

Third, a reasonable expectation of privacy test already exists in Canadian tort law with respect to personal privacy claims. Recall that the four provincial statutes establishing the tort of invasion of privacy *all* refer to the importance of the nature and *degree* of the plaintiff's privacy entitlement, which is circumscribed by what is "*reasonable* in the circumstances."[85] By adopting the reasonable expectation of privacy test, Canadian courts espouse a benchmark that works in concert with a key standard set out across relevant Canadian personal privacy legislation. Further analysis of case law under the various Canadian privacy statutes is beyond the scope of this comment, but is fertile ground for future scholarly research.

Finally, a "reasonable expectation of privacy" is the core legal notion that underpins the analytical framework for privacy violations under the *Charter*. Canadian courts are thus familiar with this concept, and drawing on it in personal privacy claims certainly does not break new ground. And despite the fact that the *Charter* is not directly applicable in private law cases, Canadian judges are required to develop the common law in accordance with *Charter* values. Indeed, there is a growing body of jurisprudence demonstrating the desirability for courts to update the law of personal privacy to reflect both modern circumstances and the values that underlie the *Charter*.[86]

CONCLUSION

This comment has demonstrated that Canadian courts should assess invasion of privacy tort claims by prioritizing contextual analysis. We have much to learn from the *Doe* decision: a bifurcated view of the public/private dichotomy and the highly offensive standard *both* call into question the ability of the invasion of

---

83 *Ibid.*

84 *Ibid,* at 688.

85 *Privacy Acts*, *supra* note 31.

86 *M. (A.) v. Ryan*, 1997 CarswellBC 100, 1997 CarswellBC 99, [1997] 1 S.C.R. 157 (S.C.C.), at paras. 30 and 45; *Carter v. Connors*, 2009 NBQB 317, 2009 CarswellNB 632, 2009 CarswellNB 728 (N.B. Q.B.), at paras. 26-33 and 42.

privacy tort to capture unforeseen privacy breaches facilitated by ever-changing technological and social conditions.

Canadian courts can understand the notions of public and private as matters of degree, by evaluating the publicness of the actor, geographic or abstract space, and type or nature of information at hand. Courts should develop and apply the invasion of privacy tort with a commitment to preserving dignity as a fundamental aspect of the right to privacy. Also, judicial discretion cannot be unfettered: the highly offensive standard adopted by the *Doe* decision is overbroad and ought to be rejected because it enables courts to find liability simply due to holding the publicized material itself to be highly offensive. The high offensiveness threshold is inadequate and also risks being under-inclusive particularly when it comes to technological and social change. Courts can remedy such deficiencies by analyzing how and when technology is used in a certain context, and the unusualness of such usage.

The modern, principled English approach offers a hopeful way forward for Canadian courts, which should lay to rest the conceptually flawed *Restatement* approach. Instead, they should embrace the reasonable expectation of privacy test, which overcomes these problems by enabling Canadian tort law to capture unexpected privacy breaches that will inevitably occur through technological and social change.