



8 June 2009

Ewan Morris  
Law Commission  
PO Box 2590  
Wellington 6140

By email: [privacy@lawcom.govt.nz](mailto:privacy@lawcom.govt.nz)

Dear Mr Morris

**Law Commission Issues Paper 14 - *Invasion of Privacy: Penalties and Remedies*.**

The Society's Privacy Working Party (the working party) is grateful for the opportunity to comment on the Law Commission's issues paper "Invasion of Privacy: Penalties and Remedies" (the issues paper). This submission follows the question and answer format provided for in the issues paper.

**Question 1: Is there value in a tort of invasion of privacy by publicity given to private facts? If so, what is that value?**

Yes. The working party recognises that there is no compelling argument or policy reason to legislate away from the use of tort, and as such favours the status quo.

Britain has experienced strain on existing causes of action, as people seek a remedy for invasion of privacy. A direct remedy avoids that strain. The New Zealand Bill of Rights Act continues to offer protection for freedom of expression.

The concept of "private facts" requires refinement however, it is debatable whether a statutory formulation of the tort is necessary to achieve this. For example, the courts have found that a published record of a criminal conviction is a private fact (*Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716) and that a photograph of a woman's genitals identifiable only to the subject can also be a private fact (*L v G* NP202/00, 21 January 2002).

There is value in having tort law develop alongside legislation to keep pace with technology and changing social values. If a statute becomes obsolete in a fast changing world, or the drafting unintentionally prevents legitimate claims, the courts will be able to continue their cautious evolutionary approach.

**Question 2: Do you think it would be sensible to abolish the tort without replacing it? If it is to be replaced, what should replace it?**

No, for the reasons stated above.

**Question 3: If there is to be a tort, is it better to codify it in statute, or leave it to evolve by case law?**

It would be preferable to leave the tort to evolve by case law. The value of the common law approach is that it will be able to take into account new facts as they arise, which might not be possible in a static statutory codification. The pace at which new scenarios arise from new technologies means that a statute-based formulation may not keep pace.

A public interest defence in claims against the media has not yet developed. There will be cases in which a court is required to weigh the particular facts and principles in order to balance the right of freedom of expression against a right to privacy. The range of variables that might present in a given case does not support a pre-emptive codification in statute.

**Question 4: If there is to be a statute, what should it contain? It would be helpful if you answered the specific questions 5-23 below, but you need not confine yourself to those questions.**

There is no compelling policy reason to constrain the courts' continued development of the common law and the working party does not support the development of a statutory tort. Should a statute be developed the approach used should be principle based, as opposed to a prescriptive approach. Legislation should be formulated only where it would provide greater certainty than a common law approach, and the working party is not satisfied that a statutory formulation, at this stage, would be capable of doing that.

**Question 5: Should the "highly offensive" test remain as a separate element of the tort?**

An objective standard of "highly offensive" is quite onerous for a plaintiff, but could be justified given the value society places on freedom of expression. The Broadcasting Standards Authority's (BSA) use of the phrase "highly offensive" and the Californian "offensive" test could usefully be compared and considered. Any statutory provision would need to take into account the subjective nature of privacy and individuals' expectations.

An alternative approach would be to move away from the "highly offensive" test as a fundamental element of the tort, and to reflect the level of offensiveness in the remedies awarded.

**Question 6: Is "reasonable expectation of privacy" a useful test? Would it be possible in a statute to give more precise definition, or to list considerations to be taken into account in determining whether that expectation exists?**

"Reasonable expectation of privacy" would be a useful test. Rather than list the situations that apply, it may be more useful to list situations where individuals do not have any such expectation, such as in respect of criminal convictions where no suppression orders exist, and no "clean slate" regime applies.

Some jurisdictions make it clear that a public servant's name, job description, salary and other specified information related to their official duties cannot be subject to a privacy claim.

**Question 7: In what circumstances can there be a reasonable expectation of privacy in relation to things which happen in a public place? Is it possible to devise a test to clarify this issue?**

It is probably unwise to attempt to specify when there should be an expectation of privacy in a public place. It is in this respect that the "highly offensive" element of the tort becomes useful. It is difficult to conceive of many situations in which one might claim a public event attracts privacy,

but a “highly offensive” test would provide a remedy to someone like the Briton who attempted suicide in a public place and was captured on CCTV camera. Similarly the publication of images of injured people at a car crash might be found to be highly offensive. The difficulty for the courts in these cases under the current formulation of the tort is whether such images can properly be described as “private facts”.

The BSA approach achieves a reasonable balance, which passes the workability test and seems to achieve fair results.

**Question 8: To what extent is the degree of privacy that public figures can reasonably expect less than that of the general population? Does any reduced expectation of privacy on the part of public figures also apply to their families?**

Part of this discussion will need to consider what constitutes a public figure. A person who puts themselves into the spotlight in order to highlight a particular issue of public concern, such as a whistleblower, or someone whose personal experience of a public service shows a need for inquiry or reform should not necessarily be exposed to the full scrutiny of their private lives.

Similarly, an actor, newsreader, athlete or quiz show contestant ought not to be considered to have relinquished any claim to privacy only by virtue of their vocation or taking up of an opportunity to participate in a public activity.

Consideration should be given to some element of waiver for people who actively court media coverage. This could be inherent in the tort, reflected in any award of damages, or provide ground for estoppel.

Any deviation from the base expectation of privacy for public figures ought to be proportional, and related to their public role and comments. It might be defensible for example for a newspaper to print stories about allegations of drug taking by a sports star who publicly advocated against performance enhancing drugs, but an actor’s drug abuse problems, or dissemination of information about the sports star’s sexuality might not qualify for the defence.

**Question 9: In what circumstances can there be a reasonable expectation of privacy in relation to something which has already been published?**

It is necessary to have a more sophisticated approach to privacy than one which claims “if a fact is capable of being uncovered through legitimate means or research, its publication is not actionable”.

From the earliest judicial consideration of the tort in *Tucker* the potential for privacy to “grow back” over an earlier publication has been acknowledged.

With modern media allowing infinite copies, and indefinite retention of information, that need becomes even more acute. For example a young person with a Bebo page might allow only 6 friends to access that page, but the conduct of those friends might mean that information is available to the world at large for years to come.

The tort might usefully incorporate elements of the law of contract or breach of confidence to address these issues. To whom was information disclosed, and on what basis, ought to influence the extent to which the subsequent publication is actionable. Perhaps a modification of the test in *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47-48, which requires a

consideration of the nature of the information, and the circumstances in which it has been imparted, could inform the availability of the tort, rather than a simple consideration of whether prior publication has occurred.

It may be that damages would differ depending on who published the material. It is unsatisfactory that a newspaper could publish private material in its pages or on its website with impunity, on the basis that a low circulation blog published it first. Much more damage would be done by the former than the latter.

**Question 10: At what time should the expectation of privacy be assessed: the time of the occurrence of the facts in question, or the time of their projected publication?**

At the time of the intended publication.

**Question 11: How far should plaintiff culpability be relevant to reasonable expectation of privacy? Is it possible to frame a statutory test to deal with plaintiff culpability?**

One of the reasons that incremental development through the courts is preferable to a statute is because of the difficulties inherent in developing a statutory test for culpability, and the moral judgement that this would involve. While there are areas in which culpability should be considered, there are difficulties in a statutory “bright line” test. This means that it is better dealt with as a tortious matter.

Further, media outlets need some protection from withdrawal of consent. A documentary crew which invests time and money following a person who has consented to be filmed should not later be liable when the person withdraws consent.

**Question 12: Would it be helpful, in a statute, to give examples of matters which are normally of legitimate public concern?**

Yes, but examples should be neither exclusive nor binding.

**Question 13: Should the statute require only reasonable grounds for belief that the matter is of legitimate public concern, or should the test be an objective one?**

The test should be objective. An objective test favours the individual, as it provides a defence. A “reasonable grounds” test tends to favour the media. This is discussed adequately in 6.71 of the issues paper.

**Question 14: Other than legitimate “public concern”, what defences should there be to a cause of action for publicity given to private facts?**

It should be a defence where the public disclosure is necessary to counter selective facts placed into the public domain by the individual concerned, provided the further private facts are relevant and the disclosure proportional.

**Question 15: What remedies should be available? (paras 6.74-6.82)**

The existing remedies available through the court are satisfactory, and these remedies should be consistent with those available before the BSA and under the Human Rights Review Tribunal.

**Question 16: Is it possible, or desirable, to list considerations to be taken into account in**

**assessing damages?**

The damages regime should be aligned with statutory remedies. A list of damages is in s.66 of the Privacy Act. If the regimes apply different standards and awards it will distort litigant behaviour.

A plaintiff should choose a single forum. A defendant should not face proceedings in the Human Rights Review Tribunal, the Broadcasting Standards Authority and the District Court over the same matter.

**Question 17: Should it be possible to obtain a remedy in this privacy tort (or cause of action) if some or all of the statements made about the plaintiff are untrue?**

No, the affected person should seek a remedy in defamation.

**Question 18: Should wide publicity be required to ground a cause of action or might publication to a small group be enough in some cases?**

Publication to a small group can cause considerable harm in some cases, such as the destruction of relationships. The tort should not require widespread publication.

**Question 19: Should it ever be possible to obtain a remedy for invasion of the privacy of a deceased person?**

No. Actions in tort necessarily lead to (or attempt to lead to) remedial action, which cannot be provided to a dead person.

**Question 20: Should corporations, or other artificial persons, be able to bring an action for invasion of privacy?**

No.

**Question 21: Is it possible to lay down a statutory test to clarify the special position of children?**

It would be very complex legislation that attempted to do so. The position and vulnerability of the plaintiff should be one of the factors to be considered in deciding an award of damages, and could affect the level of offensiveness involved.

**Question 22: Might it ever be possible for a person to succeed in an action for publicity given to private facts if that person was not identified in that publicity? To whom would the person need to be identified?**

A person might have a sense of betrayal on the basis of recognizing themselves in some anonymised description, or other such publication, however it is difficult to characterise that action as a breach of privacy without identification to some third party in some way. That identification might be obscure, and not obvious to all viewers of the disclosed information, but some identification should be required nonetheless.

**Question 23: What mental element should be required to found liability in a defendant?**

In the principal offender, no mental element should be required to be found. However for any

secondary or subsequent offenders, for example republishers, a level of intent should be required, with thought given to possible defences like innocent dissemination.

**Question 24: Should the existing criminal offences relating to disclosure of personal information be examined to see whether they are all still needed? Are there any existing offences that are no longer needed?**

The existing criminal offences should be examined for consistency, and also to see if they are sufficient to cover new technologies. Any obsolete references should be removed.

**Question 25: Are any new criminal offences needed?**

No comment – the working party has not examined areas outside the issues paper.

**Question 26: Is it worthy of consideration whether the Privacy Act 1993 should contain offences?**

This is a subject more suitable for discussion at stage 4 of the review.

**Question 27: Should inconsistencies in the existing criminal offences and penalties be removed? If so, how?**

Yes, if there is evidence that inconsistencies have led to unjust results, and if a sufficient case can be made to justify amending legislation.

**Question 28: Are any other civil remedies in relation to disclosure of personal information needed? If so, should they be obtainable in the courts, or in some other forum?**

In principle, no. One of the aims of law reform is to rationalise the law, not further fragment it. Adding further causes of action will not help achieve this aim.

**Question 29: How useful are the distinctions between public and private places, mass and target surveillance, and overt and covert surveillance, for the purpose of framing laws to control surveillance? Are there any other key distinctions the Commission should consider?**

As the report points out, the distinction between public and private places is not always clear. Individuals do not give up all their reasonable privacy entitlements when they are in a public place. They should continue to enjoy a right to be free from unwanted surveillance. Any limitations on this right should require a high level of justification and the law should reflect this.

The distinctions between targeted and mass surveillance are useful on occasions, provided they are not used to justify the diminution of individuals' reasonable privacy expectations. Sometimes these distinctions 'blur at the edges'. Any changes to the law regarding surveillance need to reflect this.

The working party is more concerned about mass surveillance by the state than market-driven and coincidental surveillance, for example, a location trail produced by the GPS capacity of a mobile phone.

**Question 30: Are there particular surveillance technologies that you are especially concerned about?**

The level of concern generally reflects the perceived degree of intrusiveness of the form of technology at issue. The greater the degree of intrusiveness on the reasonable privacy entitlements of individuals, the greater should be the level of justification preceding the introduction of the particular surveillance technology.

With this in mind, the working party ranks the forms of surveillance technology identified in the report (8.34-37) from most to least intrusive as follows –

- brain scanning (eg, the potential to analyse people's thoughts)
- biometrics (eg, face recognition technology)
- spyware
- location technologies (including RFID and GPS). This is especially the case when used to track the movements of an identifiable individual – other than when there are strong grounds to suspect that they are involved in serious criminal activity.
- networked digital cameras (aka CCTV)

**Question 31: What role do you see for privacy-enhancing technologies in addressing the problems of surveillance? Is there a role for the law in promoting or mandating such technologies?**

The working party recognises the increasing role that privacy-enhancing technologies can play. The law should promote their use provided that the particular technologies are effective in protecting individuals' reasonable privacy entitlements. Enforcement agencies should undertake only surveillance that is allowed by law.

**Question 32: Which of the following types of surveillance are you particularly concerned about? What are your main concerns about these types of surveillance? Which of these types of surveillance do you consider particularly beneficial, and why? (Note that surveillance for intelligence and law enforcement purposes is largely outside the scope of this Review, and that workplace, private investigator and media surveillance are discussed in chapter 12.)**

- **Regulatory (including local government, environmental and traffic regulation)**  
These agencies have broad surveillance powers which have expanded in recent years – the working party is unsure how effective the present privacy safeguards are in practice.
- **Domestic**  
The commentary in paragraphs 8.58-59 of the issues paper highlights the need to review the scope of the current 'domestic affairs' exemption in the Privacy Act (s 56), as part of the Law Commission's upcoming review of the Act.
- **Workplace**  
Existing legal protections have frequently proved ineffective to employee privacy expectations.
- **Media**  
Media – elements of the media appear to be willing to use intrusive forms of surveillance in pursuit of 'a good story'. The existing legal protections (eg, the BSA's privacy jurisdiction) have not proved particularly effective in discouraging major media operators from engaging in intrusive behaviour on occasions.

**Question 33: Should civil liability for certain uses of surveillance devices be provided for by means of a statutory privacy tort or intrusion tort (as discussed in chapter 11), or a statutory surveillance tort? If so, what uses of surveillance devices should the tort cover?**

The working party would not wish to rule out the development of a tort of surveillance/intrusion through the normal process of developing common law, but considers that there is no case for a statutory tort, and there is a case for clarifying the application of the Privacy Act to an individual's personal, family or household affairs (s56 of the Act)<sup>1</sup>

**Question 34: Should civil liability for the use of surveillance devices be based on breach of a statutory duty?**

No. Civil liability for the use of surveillance devices should be based on breaches of the Privacy Act 1993 (as amended). Please see below at Question 49.

**Question 35: Should certain targeted surveillance activities be designated "specified acts" of harassment under the Harassment Act?**

While civil liability matters involving use of surveillance devices should be dealt with by way of changes to the Privacy Act 1993, there is a case for enhancing the Harassment Act by the inclusion of certain targeted surveillance activities as "specified acts" for the purposes of the Act. It should, however, be made clear that these targeted surveillance activities are deemed to be specified acts only where those acts cause the applicant to be in fear for his or her safety, and would cause a reasonable person in the applicant's particular circumstances to fear for his or her safety.

**Question 36: Should certain acts of surveillance be considered to constitute harassment on their own, without a requirement for any further specified act directed at the applicant to occur, for the purposes of seeking a restraining order or bringing a criminal charge under the Harassment Act 1997?**

Yes, if the reference here is to allowing acts of continuous surveillance to be a form of harassment. It should have to be shown that acts of continuous surveillance constitute a pattern of behaviour (rather than simply one or more isolated incidents) before the Act's remedies can be invoked. This may require some further definition of the term "pattern of behaviour".

**Question 37: Should the use of surveillance devices continue to be dealt with under the criminal law by targeting specific uses of surveillance devices in particular circumstances? Alternatively, should these offences be dealt with more generically? If so, how could this be achieved?**

We agree with the Law Commission's view that any new provisions creating criminal liability should be specific and directed at defined uses of certain types of surveillance device. The criminal law needs to be precise. This approach is also consistent with the way in which the criminal law has developed and is developing both in New Zealand and in Australia.

---

<sup>1</sup> Questions 33, 49, 50 and 51

For the avoidance of doubt, these answers to these questions should not be interpreted as opposing the development of a common law tort of intrusion and surveillance.

**Question 38: Are any reforms to the criminal law relating to visual surveillance required, such as:**

- **a new visual surveillance device offence;**

Yes in principle, but all or most of the limitations referred to in paragraph 10.36 of the issues paper should apply to ensure that activities that are not clearly inappropriate are not criminalised;

- **reform of the summary offence for offensive behaviour in a public place or a new offence to cover intrusive visual surveillance in public;**

Generally speaking any new offence should not extend to visual surveillance in public places. Any exceptions (such as filming people seriously injured in traffic accidents) should be tightly circumscribed.

- **an offence against the use of hidden cameras; or**

No, this is best regulated within the framework of the Privacy Act.

- **expansion of the intimate visual recording offence?**

We think that consent to both the original recording and to subsequent distribution should be considered, particularly where the subjects concerned are immature or are vulnerable at the relevant time.

**Question 39: Should any of these matters concerning visual surveillance be dealt with instead by way of civil liability (under a tort or the Privacy Act)?**

Criminal liability should be maintained while civil liability continues to develop.

**Question 40: What should be the scope of any new visual surveillance offences?**

See the responses under question 38. It is important that any new criminal offences be tightly circumscribed. For instance in the case of any new visual surveillance device offence, any offence should be limited to cases of trespass: should apply only where recording is involved; should be generally limited to covert surveillance, and there should be a clear and limited public interest defence.

**Question 41: Does the definition of “private communication” for the purposes of the interception offence require reform?**

Yes, to avoid any uncertainties around “expectations” of privacy concerning the use of emails, texts and cell phone communications. It also makes little sense for there to be inconsistencies with the “no exception” regime operating in relation to the computer misuse offences (see paragraph 10.52).

**Question 42: Should the participant monitoring exception to the interception offence be reformed in any respect?**

Yes. A new approach should be adopted to the rules around participant monitoring – along the lines that currently operate in New South Wales (see paragraph 10.58)

**Question 43: Are any other reforms of the interception offence required?**

Yes. Authorised outside monitoring should not be permitted.

**Question 44: Are any other reforms required in relation to communications privacy?**

There is no compelling reason for the current law to be changed. This subject is dealt with in the Law Commission paper on Search and Surveillance Powers (NZLC R 97).

**Question 45: Should a new offence be created to target the covert use of tracking devices to determine people's locations?**

Yes. The argument that "there is no evidence of the illegitimate use of tracking devices in NZ" is weak. This argument concedes that there should be an offence if there is a problem. It ignores the fact that developments in technology are fast-moving. It also seems odd that to say there is no problem in New Zealand, yet new law has been introduced in Australia.. Any use by law enforcement agencies of new covert monitoring technology should be subject to the same level of judicial oversight as current interception warrant procedures.

**Question 46: Are the computer misuse offences adequate to deal with privacy intrusions from computer hacking and other unauthorised access to computers and digital devices, and the use of spyware and keystroke loggers? Is a specific review of the adequacy of these offences required?**

It would appear from the Law Commission's analysis (see paragraphs 9.20 to 9.30) that the computer misuse offences are adequate to deal with privacy intrusions from computer hacking and other unauthorised access to computers and digital devices, and the use of spyware and keystroke loggers. A review is probably not worthwhile unless it can be shown that one of more of the exceptions (such as the unauthorised insider exception to the offence created by s 252 of the Crimes Act) is causing difficulties.

**Question 47: Should consideration be given to an offence for the unauthorised monitoring or collection of call data? Or should this be dealt with as a matter of civil liability?**

This kind of conduct is already dealt with by way of civil liability and under the Telecommunications (Interception Capability) Act 2004.

**Question 48: Should consideration be given to an offence against RFID skimming in New Zealand?**

This has already been discussed.

**Question 49: Should the application of the Privacy Act to surveillance be clarified? If so, how should this be done?**

The existing privacy principles should be expanded to take into account surveillance to the extent that they do not already do so. (See Paul Roth's views in the issues paper as to the inadequacy of current legislation).

The alternative (a new set of principles) should be considered only if they work properly and easily with the existing set of principles.

**Question 50: Do the privacy principles need any modification in the way they apply to surveillance? If so, how should they be modified?**

Please see answer to question 49.

**Question 51: Is a new set of surveillance principles required, either within the Privacy Act framework or under a new Surveillance Act? If so, what should be the content of these principles, and how should they operate?**

Please see answer to question 49.

**Question 52: Should there be limitations on surveillance of public spaces carried out by both public and non-public agencies?**

Yes in principle, but any offences should be tightly circumscribed to ensure that activities that are not clearly inappropriate are not criminalised.

**Question 53: Should CCTV be regulated under a specific CCTV statute?**

No. A code of practice under the Privacy Act might be appropriate. This might, however, require expansion of the categories of codes that the Commissioner can make.

**Question 54: If not, should CCTV be regulated in any other way such as:**

- the Local Government Act;
- statutory regulations;
- a Code of Practice issued by the Privacy Commissioner;
- voluntary guidelines issued by the Privacy Commissioner; or
- standards developed by Standards New Zealand?

Please see answer to question 53

**Question 55: What are the most important issues that any regulation of CCTV should cover?**

Please see answer to question 53. A cost/benefit analysis might be appropriate in determining the need for regulation.

**Question 56: Are any specific regulatory measures needed in relation to RFID technology?**

This is an emerging technology. The need for any specific regulatory measures in relation to it would need further examination.

**Question 57: Are any other regulatory measures necessary or desirable in relation to surveillance?**

Not as the law currently stands.

**Question 58: Should the Harassment Act 1997 provide for the award of damages?**

No. The Harassment Act concerns personal safety, and provides remedies appropriate to this context (for example, restraining orders).

**Question 59: Are any reforms to the law needed to deal with voyeurism not involving the use of recording devices, including reform of the “peeping and peering” offence in the Summary Offences Act 1981?**

As the paper identifies, the key questions for reform are whether the parameters of the offence are appropriate and whether the penalties are adequate (para.11.24). The working party agrees with the conclusion that the current restriction in the Act to offences limited to peeping and peering at night should be widened by being applicable during the day. The paper notes that if this were the case it should be clarified that only offensive behaviour is targeted, which seems a sensible conclusion.

The paper also raises the question whether the terminology in the offence as to peeping and peering into “a dwelling house” is broad enough to encompass a variety of buildings in which a person resides and has a reasonable expectation of privacy. “Dwelling house” is sufficiently broad in that regard (although it would not apply to, for example, public swimming pools).

The maximum fine, which has not been updated since 1982 (para.11.25) should be reviewed, against provisions in other comparable statutes.

Para.11.26 of the paper notes that peeping tom activity that does not involve recording devices but involves covert observations (such as by drilling holes in a wall, one-way mirrors etc.) is sometimes used in places where people expect privacy. To the extent these are within a “dwelling house” the Summary Offences Act is sufficient. To the extent they take place in, for instance, a swimming pool changing shed, the paper notes a number of other offences (offensive behaviour in a public place, willful damage to property, being on a property without lawful excuse – see para.11.26) which may apply. While these do not directly address the invasion of privacy involved, they provide an adequate remedy.

**Question 60: Are any new criminal offences, or changes to existing offences, needed to deal with specific types of intrusion other than surveillance?**

The question is whether legislation needs to criminalise voyeuristic observation as well as recording. The intimate covert filming provisions of the Crimes Act deal only with use of recording devices. In terms of privacy, while mere observation is unpleasant and uncomfortable, filming allows the intrusion to be “spread” much wider than the individual or individuals undertaking the filming.

If the Summary Offences Act is amended as above, it may not be necessary to extend the Act to covert voyeuristic observation (which may be difficult in any case to prove).

**Question 61: Are any new civil remedies (apart from a possible intrusion tort) needed to deal with intrusion?**

The paper identifies an option of creating a new offence of voyeurism (para.11.27). It identifies that the parameters of such an offence would need to be delineated, and that the potential overlap with the intimate covert filming provisions of the Crimes Act would need to be thought through, including whether intimate covert filming provisions would be treated separately from voyeurism undertaken without the use of a recording device.

The paper does not identify a significant need for defining a particular offence of voyeurism. That may mean it is unnecessary.

**Question 62: Should an express right to sue for breach of statutory duty be created in relation to any statutory provisions relating to intrusion?**

There seems to be no particular need to codify what may already exist in the tort of breach of statutory duty.

**Question 63: Should there be an intrusion tort?**

Paragraphs 11.33 and 11.34 summarise the arguments for and against an intrusion tort. The paper sets out some scenarios under the current law where the Commission believes that there are limitations in the remedies available for “intrusion” (para.11.9 – 11.20). However, the gaps identified are in many cases not sufficiently serious to warrant introduction of an intrusion tort. Given the limited number of actions, and their success rates, in other jurisdictions which have similar rights, an intrusion tort does not seem a particularly pressing need in New Zealand.

In particular, to the extent that any intrusion results in publication, the Broadcasting Standards Authority intrusion principle is available to many complainants. More pressing is ensuring that new media, and in particular the internet (and blog sites), have a remedy equivalent to the Broadcasting Standards Authority.

**Question 64: Should the development of an intrusion tort be left to the common law, or should it be introduced by statute?**

Given the conclusion above, answering this question is not strictly necessary. However, even if the decision is that there should be an intrusion tort, development under common law seems logical, given that the common law has been sufficiently flexible to deal with the disclosure tort as it has arisen. There is not significant clarification, benefit or efficiency in a little used statute that does not attract a significant body of case law, over and above development of a common law tort.

**Question 65: If an intrusion tort is introduced by statute, what should be its elements? Specifically:**

- **Should it refer to intrusions on “solitude and seclusion” and would this necessarily suggest that it applies only in private places?**
- **Should it include intrusions into personal or private affairs and concerns, or should it be limited to intrusions and spatial privacy (unwanted access to a person’s private spaces)?**
- **Should it include examples?**

It would be difficult to establish examples, given the breadth of when the tort might arise, and the likelihood that it would not be well used.

**Question 66: Would your answers to question 5 – 8 and 11 from Chapter 7 differ for the intrusion tort from the answers you gave with respect to the disclosure tort?**

Given the moderate approach suggested, the answers would not differ – although given “intrusion” is more likely to give rise to vexatious claims, the “highly offensive” test discussed at Question 5 should be an essential element of the tort.

**Question 67: If the statute were to give examples of matters of public concern, would the examples for the intrusion tort differ in any respect from those for the disclosure tort?**

If examples were to be included they should be neither exclusive nor binding.

**Question 68: With respect to the intrusion tort, should the statute require only reasonable grounds for belief that the intrusion was for the purpose of obtaining information in the public interest or about matters of legitimate public concern, or should the test be an objective one?**

The test should be objective – and there is no reason for intrusion and disclosure torts to differ in this regard.

**Question 69: Would your answers to Questions 14 – 16, 19 – 21 and 23 from Chapter 7 differ for the intrusion tort from the answers you gave with respect to the disclosure tort?**

No – these should develop concurrently and on the same general basis.

**Question 70: What do you think should be the relationship between the disclosure and intrusion torts if both were to be put on a statutory basis?**

The working party argues against the creation of distinct statutory disclosure and intrusion torts. While it might give greater scope for recognising differences between them (as identified in para.11.56 of the paper) it is likely there would be considerable overlap between intrusion and subsequent disclosure, making distinct torts difficult in practice. Rather, one tort would be more useful and easier to manage.

**Question 71: Should there be a mechanism for dealing with intrusion at a lower level as an alternative to proceeding through the courts? If so, what form should this take? Should intrusion and disclosure both be dealt with at the same level?**

Even if a tort is separately recognised, there is not sufficient benefit in giving an entry level approach to enforcement, such as giving the Privacy Commissioner jurisdiction in relation to intrusion more generally. If the matter is sufficiently serious, it should be dealt with by the courts. The paper does not identify enough specific issues where no redress is available to show there would be sufficient efficiency or benefit from a new regulatory regime.

**Question 72: Should the media be subject to any greater, or lesser, legal restrictions concerning surveillance and other intrusions than other members of the public?**

The media should be subject to the same restrictions concerning surveillance and other intrusions as other members of the public.

**Question 73: Does the current framework of content regulation by the BSA and the Press Council provide adequate protection against intrusions by the media? Alternatively, does it go too far in limiting media freedom?**

The current framework of content regulation provides some protection against intrusions by the media. As the report suggests, the blurring of boundary lines between different forms of media and the emergence of new media and quasi-media forms raises real concerns about the consistency of approach between the existing regulatory entities and the divide between regulated and unregulated media expression.

Consideration should be given to moving towards a regulatory regime that covers all forms of media and applies consistent standards to the regulation of all forms of media.

**Question 74: To what extent should the media be exempted from laws dealing with surveillance and other intrusions (either current laws, or options for reform discussed in this issues paper)?**

Exemptions from laws concerning surveillance and other intrusions should not be available specifically to the media. An exemption based on lawful purpose (not specific to the media) may be appropriate.

**Question 75: What form should any exemptions for the media take? Should they be restricted to newsgathering, and if so, how should newsgathering be distinguished from entertainment?**

Please see answer to question 74.

**Question 76: Are the issues relating to surveillance and other forms of intrusion in employment significantly different from issues in other areas? If so, how?**

Issues relating to surveillance and intrusion in workplaces are not significantly different from the issues that arise in other areas. However, elements of complexity do arise as a result of workplaces being partly-private/partly-public spaces.

**Question 77: Does the current legal framework achieve an appropriate balance between the interests of employers and employees with regard to surveillance and other forms of intrusion? If not, in what areas is reform needed to achieve an appropriate balance?**

In general the current legal framework provides an appropriate balance between the interests of employers and employees. Subject to comments made at question 79, the working party considers that this balance is best developed in the employment sphere through developments in the interpretation of the mutual obligations of good faith, fidelity, trust and confidence between employers and employees.

**Question 78: Should there be a specific statute governing workplace surveillance? If so, what areas should it cover?**

No.

**Question 79: Should there be a code governing workplace surveillance or workplace privacy generally? If so, what areas should it cover, and what mechanism should be used to introduce it?**

A code of best practice in respect of workplace surveillance could provide useful guidance in developing the interpretation of the mutual obligations between employer and employees (as it relates to privacy, surveillance and intrusion issues). Such a code could provide guidance around the reasonable expectations of both employers and employees in relation to:

- a) Overt or incidental surveillance;
- b) Covert surveillance;

- c) Monitoring of internet/email; and
- d) Consultation with employees

**Question 80: Should private investigators be subject to any greater legal restrictions than other members of the public in order to protect privacy?**

It is inconsistent that licensed private investigators are subject to greater legal restrictions than those that apply to an unlicensed person carrying out the same or a similar activity.

**Question 81: Do any of the current laws relating to privacy, or any proposals for possible law reform, discussed elsewhere in this issues paper have particular implications for private investigators?**

The working party does not consider that there are particular implications for private investigators that do not arise in relation to the general public.

**Question 82: Should additional privacy-related crimes be added to the list of “specified offences” in the Private Investigators and Security Guards Act 1974? Are there any other ways in which the licensing process could be used to protect privacy?**

To the extent that any new surveillance legislation creating or modifying privacy related crimes is introduced, those offences should be added to the list of specified offences in the PISGA.

**Question 83: Should section 52 of the Private Investigators and Security Guards Act 1974 be retained? If so, should it be modified in any way?**

No.

**Question 84: Should surveillance and other privacy-intrusive activities by private investigators be regulated by any of the following: a code of ethics made under the Private Investigators and Security Guards Act 1974; a Code of Practice made under the Privacy Act 1993; or a code of ethics developed and enforced by the industry itself?**

Section 71 of the PISGA provides that a code of ethics may be prescribed by Order in Council if required. However, given the way in which technology (and expectations of privacy) change and develop over time, a Code of Practice under the Privacy Act 1993 may allow for more flexibility to deal with future developments promptly.

Should you have any queries regarding this submission, please contact the working party's secretary, Diana Brown, by phone (04) 463 2967, or by email [diana.brown@lawsociety.org.nz](mailto:diana.brown@lawsociety.org.nz).

Yours sincerely



PP

John Edwards  
Convener, Privacy Working Party