Anonymity, authorisation, and legitimate attention – three lines of defence in privacy law

A review of a selection of Broadcasting Standards Authority privacy decisions

Katrine Evans

June 2014

Executive summary

This review considers how the Broadcasting Standards Authority's privacy decisions deal with the concepts of identification, informed consent, and public interest. It compares the Authority's approach with the way the Privacy Act manages the same issues, and concludes that they are broadly similar.

I suggest that it would be useful, though, for the Authority to adjust its approach in certain areas. In brief:

1. The Authority should explicitly recognise that online searches can enable viewers to identify people, even when the broadcast itself does not identify them.
2. The distinction between the privacy standard and the fairness and accuracy standards is not plain and further research is needed in this area.
3. The Authority needs to change how it deals with remedies for breaches of privacy. It should clearly frame its awards as compensation for harm suffered, receive sufficient information from complainants to be able to calculate compensation successfully, and substantially increase the level of damages that it awards to successful complainants.

The background for this review

In May 2014, the Broadcasting Standards Authority ("the Authority") asked me to review a selection of privacy decisions, and to write a report with my findings and recommendations. The terms of reference for my review are set out in Appendix One. I performed this review in my personal capacity, not my official capacity.[1]

There have been reviews of the Authority's decisions in the recent past, including by experts in common law privacy and in media law.[2] The focus of this review, though, is slightly different. I was asked to compare how the Authority's interpretations of some key privacy concepts line up with how the Privacy Act manages the same issues.

This may seem a strange exercise at first glance. Broadcasters and other news media are expressly exempt from the Privacy Act in relation to their news activities.[3] Instead, they are governed by industry-specific bodies such as the Authority. It is therefore tempting to assume that 'privacy' in the broadcasting context may be intended to mean something different from the way in which 'privacy' is managed by the Privacy Act. This would suggest that Privacy Act analysis is irrelevant.

However, the building blocks of privacy (what privacy *means*) are essentially the same regardless of the regulatory context in which they occur. The Broadcasting Act and the Privacy Act are already linked – section 4(1)(c) of the Broadcasting Act protects the "privacy of the individual", and the definition of "individual" is cross-referenced to the definition in the Privacy Act – privacy involves information about identifiable, living human beings.[4] There are other direct comparisons too. The Privacy Act provides exemptions from some of the information privacy principles on the basis that the individual has authorised the transaction. The Privacy Act also helps to define where the public interest lies when that public interest is or may be at odds with privacy protection. For instance, it directly recognises the value of law enforcement, administration of law, and personal and public safety.[5]

Also, there are benefits if different forms of privacy regulation can be aligned as much as possible:

- People can be more certain about what their rights are and organisations can be more certain about their obligations

---

[1] I am the Assistant Commissioner (Legal and Policy) at the Office of the Privacy Commissioner. However, the Authority asked me to undertake this project in my personal capacity not my professional capacity. My employer allowed me to do it on that basis and in my own time. All the views I express in this report and any errors it contains are therefore mine alone, and should not be attributed to the Privacy Commissioner or other members of his staff.

[2] See for instance Dr Nicole Moreham "Private Matters: a review of the privacy decisions of the Broadcasting Standards Authority" (2009): http://bsa.govt.nz/publications/research/91-2009/5761-private-matters-a-review-of-the-privacy-decisions-of-the-broadcasting-standards-authority. A general review last year also considered several of the privacy decisions that I have reviewed here: Simon Mount, Jim Mora and Raymond Miller "Review of the Broadcasting Standards Authority Decisions": http://bsa.govt.nz/publications/research/123-2013/6269-review-of-bsa-decisions-2013.

[3] The information privacy principles in the Privacy Act 1993 only apply to "agencies". There are limited exceptions from the term "agency", including news media when they are engaging in news activities: section 2 of the Privacy Act, under "agency", at (xiii).

[4] Section 2 of the Broadcasting Act: **individual** has the same meaning as in section 2(1) of the Privacy Act 1993.

[5] See for instance IPP 11(e) and (f).

- It avoids wheel reinvention – we can learn from one another's experience (particularly important in cutting edge situations such as those involving applications of technology)
- Wherever possible, the law should develop on a principled basis. Similar concepts should be treated similarly, and genuine differences (for example any that might be relevant because of media freedom principles) are then easier to define and apply
- It helps to prevent forum-shopping
- It provides a larger body of law to refer to when cases come before the regulatory authorities. Privacy is a relatively new area of law. While overseas cases can assist to some extent, there are significant jurisdictional differences (particularly, for instance, with United States privacy law). Home-grown precedents are more likely to be directly applicable.

The bodies that have made decisions about privacy law in New Zealand already tend to draw on each other's experience. For instance, the courts have explicitly considered the Authority's decisions when they have been developing the privacy tort jurisprudence.[6] This trend will only increase. The Authority's and Press Council's experience with Bill of Rights considerations in privacy cases will be able to assist the Privacy Commissioner with a growing number of cases that involve online publication by non-media agencies. And with around 800 complaints and 8000 enquiries every year, the Privacy Commissioner handles the greatest number and widest range of privacy complaints and policy queries – twenty years' worth of experience for other decision makers to draw upon as required.

I have structured this report around the three key cross-over concepts that the Authority particularly asked me to consider: identification, consent, and public interest. These are the key lines of defence for broadcasters. There is no breach of privacy if the individual is successfully anonymised, if he or she has clearly authorised the broadcast, or if the subject matter is one of legitimate public attention. I also briefly compare the Authority's approach to the requirement to show harm ("highly offensive to a reasonable person") with the Privacy Act approach to harm. I conclude by considering the remedial environment in some detail, as this is the area that I believe the Authority can most usefully develop to protect legitimate privacy interests in 2014.

[6] *Hosking v Runting* [2004] NZCA 34, at para 85.

Recommendations

For the most part, the analysis in this report supports the way in which the privacy principles, and the Authority's decisions, approach the question of privacy protection. There are substantial overlaps with the way in which the key concepts are dealt with elsewhere in privacy law, including in the Privacy Act.

However, I have a few recommendations:

1. The Authority should adapt the concept of identification to acknowledge that online searches may enable viewers to identify people, even when the broadcast itself does not identify them. Privacy rights should not be based on legacy media paradigms, where such an ability to find material was less available. To do so would unjustifiably restrict the situations in which protection is available. The Authority should acknowledge the realities of the modern media environment and people's increasing ability to source or check information for themselves.
2. The distinction between the privacy standard and the fairness and accuracy standards is not always particularly plain. A proper analysis goes beyond the terms of the current review, but the Authority could usefully do some further research work in this area.
3. The Authority needs to re-evaluate the basis on which it makes awards of damages to successful complainants. There are several aspects to this.
    a) Damages should be clearly articulated as *compensation* for harm suffered, or likely to be suffered, by the individual. The Authority's current terminology is confusing and its analysis of compensation is less clear than would be ideal. Both complainants and broadcasters need to be more certain of the basis on which compensation will be awarded.
    b) The Authority should specifically seek information from complainants about the level of harm that they believe the broadcast has caused. Current complaint forms do not ask for this information or indicate what orders the Authority can make.
    c) Where harm does not speak for itself, and credibility is important to a decision whether to award compensation, the Authority should consider receiving direct evidence from the complainant, for example via online videoconferencing.
    d) The Authority should make higher awards of damages in many of the cases where a breach of privacy is proved. The level of damages is currently insufficient to provide a meaningful remedy for injured complainants. The statutory maximum is simply the most that the Authority is entitled to award – but it is nominal in terms of compensation for privacy breaches in other areas of law. Somewhat radically, I therefore suggest that it not be reserved for the most serious cases but instead should be the starting point for a consideration of compensation, to be reduced as appropriate in individual cases.

Methodology and terminology

The Authority asked me to review 11 specified decisions. These are listed in Appendix Two. I have given each a brief descriptive title to make the report easier to read.

Since each of the decisions involved the Free-To-Air TV Code, I also asked to see a selection of cases under the Radio Code, to get a better overall view of the Authority's work. These are also listed in Appendix Two. A consideration of these decisions showed that there was no particular difference between the way in which the Authority handles complaints under the different Codes, so further comment has not been necessary.

For each decision, I read the decision and viewed or listened to the broadcast. I also reviewed information about privacy complaints on the BSA's website and talked to members of staff about the decision-making process and the information available to the Board.

Both the Authority and the Privacy Act use the term "privacy principle". The Privacy Act's principles are in section 6 of the Act, and are formally called "information privacy principles" [IPP]. So to avoid confusion, I have used the term "privacy principle" to refer to the principles in the Authority's advisory opinion explaining the broadcasting standard, and "IPP" for the Privacy Act's principles.

General comments about the decisions

The decisions that I reviewed were all correctly decided, in terms of substantive privacy law. I have identified a few areas where the analysis could be slightly clearer, for future decisions, but none would have affected the outcome in the original decisions.

The Authority is also consistent with how it approaches its decisions. Privacy complaints are notoriously contextual – small fact changes can entirely change the outcome.[7] However, it is important that the underlying principles are expressed consistently and clearly. Complainants and broadcasters alike need to know how the Authority is likely to approach a particular complaint, and the Authority itself needs to be confident about the basis on which it is making its decisions. The Authority has developed a significant body of decisions over the last two decades and it uses that experience well. The advisory opinion has remained reasonably unchanged for some time. Decisions often refer to earlier precedents and, from what I could see, they do so accurately. Of course the law does not stay still and the Authority needs to feel free to depart from earlier practice if it is no longer applicable. However, if the jurisprudence needs to develop (for example to take account of a new trend in broadcasting, or a change in technology), it should be able to do so on a principled and logical basis.

The only place where a more radical change is needed relates to the Authority's approach to compensation. I have commented on this in more detail in the final section of the report.

The decisions are also clearly written and reasonably easy to follow. The more recent decisions of the Authority are prefaced with a clear narrative summary of the facts and the Authority's conclusions on key issues (eg identification or consent); the standard involved and whether the

[7] The Authority explicitly makes this point in the advisory opinion: http://bsa.govt.nz/images/assets/Practice-Notes/Privacy-Practice-Note.pdf

complaint was upheld; and any orders that were made. The summary is displayed both as an introduction to the text of the decision itself and as a summary on the website. The narrative approach to the summary is clearer than the "headnote" style that the Authority used until fairly recently. It is also more flexible across different formats, particularly online.

I recommend that the Authority continue with this practice and keep the fields of information consistent. It is a concise and plain English way of informing people what happened and why. People can see at a glance whether the decision is relevant and interesting to them. It is also simple to compare the information against other decisions. This recent practice is a significant improvement on earlier decisions, which did not include such a concise and standardised means of describing the outcome of the complaint. The decisions that I reviewed had a wide variety of introductions or headnote styles, not all of which were particularly helpful to the reader.

Three main lines of defence – and a couple of supporting barriers

Broadcasters can avoid a breach of the privacy standard in three key ways:

1. **Anonymity**: They can ensure that the individual concerned is not identifiable; or
2. **Authorisation:** They can obtain the consent of the individual to the filming and broadcast; or
3. **Legitimate attention:** They can justify the broadcast of the material on the grounds of public interest.

There is also no liability in situations where the broadcast is not harmful, or where a person has no real expectation of privacy.

I will deal with each of these main lines of defence in turn, comparing them with the way the Privacy Act deals with the same matters.

Anonymity

From the decisions I have reviewed, it appears that the Authority's approach to identification is broadly on a par with the approach in the Privacy Act, though the structure of the analysis differs a little.

The Authority's test is correct and workable

The Authority's test for identification has been consistent since 2009. This test is not whether the person is actually named. It is whether the individual would be "identifiable to people beyond family and close friends who would reasonably be expected to know about the contents of the broadcast".[8] So a broadcaster will be unsuccessful in disguising a person's identity if:

(a) People beyond their family and close friends could recognise them from the broadcast; OR
(b) Family and close friends would be unlikely to know about the information that was disclosed in the broadcast.

[8] *Moore v TVWorks Ltd 2009-036*

In other words, there can still be a breach of the privacy standard even though a person is only identifiable to their family and close friends – as long as those family members or close friends were previously unaware of the damaging information that the broadcast discloses.

The Privacy Act ends up at a similar place though the analysis is a little different. Again, whether a person is named is irrelevant. The question is whether they are identifiable. If people are not identifiable at all, then the information is not "personal information" and the IPPs do not apply.[9] If information is about them and they are identifiable – regardless of *who* might be able to identify them, including family and close friends – then it is personal information and the agency has to consider how the IPPs operate.

This makes sense. People can be seriously harmed or distressed by disclosures of information to those who know them best, not just revelations to strangers: for instance, disclosures of medical information,[10] or disclosures of debts to colleagues.

However, the breadth of the definition of "personal information" does not mean that liability for disclosure of information about an identifiable individual (the equivalent of a broadcast) is automatic. Aside from any defences or lack of harm, which are discussed later, there is no "disclosure" in terms of IPP11 if the information is revealed to someone who already knew about it. This equates to the second part of the *Moore* test used by the Authority.[11]

It is increasingly difficult to anonymise people successfully

Several of the decisions under review indicate that broadcasters find it difficult to anonymise people successfully.

Pixellation is a common technique and is a good start but it is not always successful. Editing to show only parts of people's faces can also be used but again is fallible.[12] It is difficult to disguise distinctive facial features, hairstyles, voices, body shapes and clothes. For instance, the couple in the *Waikeria Prison* clip were clearly recognisable:

- only their faces were disguised, not other identifying features or distinctive clothing
- the location of the filming narrowed down the group of people that might have been featured

---

[9] http://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-64131-2006-nz-privcmr-7-man-complains-about-publication-of-his-photograph-in-a-booklet/. See also *Stevenson v Hastings District Council* [2006] NZHRRT 7 at 42, where an audio recording set up to capture dog barking also captured the complainant speaking. The voice was too faint to be identifiable though – the only person who could have recognised it as the complainant was the complainant himself. The existence of audio enhancement technology casts some doubt over the reasoning here, but in the context, there was no chance of the Council using that type of technology so the decision can safely stand.

[10] See for instance http://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-235915-2012-nz-privcmr-5-a-hospital-employee-disclosed-health-information-about-a-woman-to-a-mutual-friend/

[11] *A and A v G* [1999] CRT 8 (the Complaints Review Tribunal was the precursor to the Human Rights Review Tribunal).

[12] See for instance *Girl Gangs*, where the girls' bandannas were not sufficient to disguise their identities. Also, in the *Drowning Tragedy* case there were only brief shots of the relatives of the drowning victim at the beach, but they were still identifiable.

- the fact they were a couple, and that both of them were shown, made it far more likely that people would recognise them.

If only one element had been present in isolation, it might not have been possible to identify them but put together these factors made them identifiable.

The shop owner in *The Inspectors* was also recognisable. The shape of his face was clear despite the pixellation, his voice was audible, his shop was clearly identifiable, and his ethnicity was reasonably obvious. His customers and shoppers in that area of Dunedin would have had little difficulty in pinpointing who the broadcast was referring to.

Context can also easily give away someone's identity. Several of the broadcasts I reviewed showed people's homes. An interior layout, the colour and shape of the property and references to the neighbourhood are all features that can easily identify the subjects of the broadcast. *Search Warrant* was a good example.

The only reason that the tenant in *Renters* could not be identified was that the programme had been filmed three years before the broadcast. Though the letterbox number was blurred, the house was a distinctive colour and was shown in full; and the inside of the house showed the layout and the complainant's possessions in a way that would have been recognisable to anyone who had been in the house.

Of course, it is arguable that people might still have remembered who the tenant in the house was even three years later. However, the Authority did not have any direct evidence on the point – the complainant was not the tenant – so it was correct to decide the way it did. Where direct evidence is available, as it was in *Solvent Abuse*, then the Authority has not hesitated to say that a person can be identified from association with their property, even if the filming took place some time ago. Indeed, replaying the footage can aggravate the injury the person suffers, particularly where they have consistently raised objections to the broadcasts and have moved on with their life.[13]

Use of internet searches to identify the person?

The *Stem cell treatment* programme raised a potential new issue for the Authority. There was little visual information about Dr Z, the complainant, in the broadcast. The angle of the camera showed little more than his hand. His voice was not particularly distinctive. The information that was most capable of giving away his identity in the programme was the reference to his area of speciality – a highly unusual area of medical practice in New Zealand at the time.

Casual viewers of the programme would not be expected to know the medical practitioners in the area. Instead they would have to do an online search to find out Dr Z's identity. As it happens, the Authority found that Dr Z's family and close friends, who would certainly have identified him from his area of practice, would not have been aware of all the information contained in the programme, particularly the negative inferences.[14] The decision is therefore a straight application of the *Moore* test. The Authority did not need to decide that an online search was sufficient to make Dr Z identifiable for the purposes of the privacy principles.

---

[13] See the very recent decision of *TJ v TVNZ* 2013-092.
[14] *Stem cell treatment* at para 61.

However, at some stage, a case will undoubtedly arise in which no new facts are disclosed to family and close friends, but where the broadcast audience would be able to identify the individual from an online search. At that time, the Authority will have to determine the point head-on.

TVNZ argued that Dr Z was not named and care was taken with the footage to ensure he was not shown. It argued that only very interested parties would be likely to conduct a Google search leading to his potential identification through his website – so this could not meet the privacy standard test for identifiability.

In the days when a viewer would generally see a television programme only at the time it was initially broadcast, and on a fixed television screen, this position might have had greater weight. Before powerful search tools were available, 'practical obscurity' (inability to retrieve information) provided de facto privacy protection. Now, however, not only are those search tools available, but a mind-boggling amount of information is published online for all to find. There is a wealth of information within reach of even unsophisticated researchers.

Also, people are increasingly watching broadcasts on the internet – for instance, through broadcasters' websites, on demand. Those broadcasts can not only be recorded but are able to be paused and rewatched even when 'live'. Moreover, people are watching broadcasts on the same device through which they use other internet facilities such as search. Whether on a desktop computer or a mobile device, it is a matter of seconds to jump from a broadcast to a search tab to try to identify the person concerned. Even if watching a traditional TV screen, the chances are high that the remote control will be in one hand and the smartphone or tablet in the other.

TVNZ's argument about only interested parties searching for information cannot succeed, especially when it was also arguing public interest in the broadcast. It is not possible to predict how many people would be likely to try to locate an individual's identity, so that claim has little weight. The more remote the possibility is, the harder the individual might find it to prove they have been harmed – but that is a question of remedies, not of identification. Also, the stronger the ostensible public interest is in a programme, the more the public can be assumed to want to find out more and conduct their own search enquiries. Broadcasters cannot have it both ways. As long as information identifying a person is in fact readily retrievable by a search through publicly available information, this should be enough to meet the test. The legal threshold has to keep pace with the realities of the modern world, or rights to privacy will be unjustifiably left behind.

The problem is common to other areas of privacy law

In the Privacy Act environment, too, the ready availability of information means that it is becoming harder for agencies to say that a person is not identified. The Act has always catered for this to some extent. Several of the IPPs provide that agencies can use information that is anonymised, or where it will not be published in a way that is likely to identify the individual.[15] That is, the Act does not rely on the definition of "personal information" as its only backstop. It acknowledges the borderline cases where one can argue an individual may be identifiable when various items of information are combined, but where nonetheless the privacy risks are low. It focuses instead on providing safeguards against misuse of the data, and reducing the possibility of harm as much as possible.

[15] See for instance principle 11(h).

However, the law is increasingly having to acknowledge that 'anonymity' is largely a myth and in fact that it can provide a false sense of security.[16] Even a few data sets can identify people when merged. The classic research project that demonstrates how easy it is to re-identify individuals from combining disparate data sources dates back to the 1990s. A graduate student in computer science at MIT, Dr Latanya Sweeney, requested a copy of publicly released health data about state employees. The Massachusetts State Governor, William Weld, had promised the public that the information was completely anonymised. Dr Sweeney knew that Governor Weld lived in Cambridge, a city of 54,000 residents and seven ZIP codes. For twenty dollars she purchased the complete electoral rolls for Cambridge. These included the name, address, ZIP code, birth date and sex of every voter. Only six people in Cambridge shared Governor Weld's birthdate. Only three of those six were men, and of them, only he lived in his ZIP code. Dr Sweeney had the Governor's detailed health records delivered to his office, including diagnoses, prescriptions and details of hospital visits.[17]

If everyone is theoretically identifiable, this obviously poses some significant difficulties for broadcasters and other agencies that disclose information about people while trying to protect their identities. It also creates challenges for the shape of the law – if everything is possibly "personal information", agencies will be less certain about how the law applies to them, and individuals will be uncertain of their rights. In the data protection world, failures of anonymity are leading to increasing calls to introduce new rules to regulate re-identification, not simply to rely on apparent anonymity. People are likely to understand their rights and responsibilities more clearly, and the value in having information available is too great to be ignored.[18] But it is not necessary to accept that there has been a catastrophic failure of anonymity for amendments to be made to the broadcasting standard analysis. A small step change will suffice.

The Authority can and should accept that internet search can make a person identifiable

It has long been the rule that someone is identifiable if the audience to whom the information is disclosed has access to other sources of information that can be added to the information in the broadcast to identify them. For example viewers may live in the same community, or have a common acquaintance or field of employment. Many of the decisions reflect this rule. Most New Zealanders would be unable to identify the men featured in *Solvent Abuse* and *Search Warrant*, and most would not recognise the fish and chip owner in *The Inspectors.* Unless we had encountered them, and recognised them, or could visit their premises, we would be unlikely to know who they were. However, those men are all identifiable because some viewers would have the additional knowledge necessary to pinpoint who they are.

Acknowledging that a person can be identified if viewers use an internet search is a logical extension of that rule. It is time for the Authority to acknowledge that expressly. When the Broadcasting Act and the Privacy Act were passed, the chances were relatively slim that someone would have access

[16] Paul Ohm has written a seminal article on this subject: "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA Law Review 1701.
[17] Latanya Sweeney "Uniqueness of Simple Demographics in the US Population" (2000) Laboratory for International Data Privacy, Working Paper LIDAP-WP4, used extensively in Ohm, above.
[18] See Ohm, above, though he is sceptical about whether we can have both valuable data and also protect privacy. However, others are not so pessimistic: see the discussion documents produced by the New Zealand Data Futures Forum at https://www.nzdatafutures.org.nz/.

to other sources of information to help them identify an individual in a broadcast. However, it is incontrovertible that such searches are now commonplace, and are a natural extension of the way in which people consume media information in 2014. The question is a simple factual one – can people *in fact* easily locate the individual's identity if they try to do so? Is the information readily retrievable from easily accessible public sources of information? If the answer is yes, then the individual is identifiable.

If anonymisation is becoming unreliable, then broadcasters need to ensure other safeguards are in place

In the broadcasting world as elsewhere, difficulties in anonymising people do not mean that trying to disguise identity is futile. On the contrary, it is still an obvious first line of defence to protect people in circumstances where publishing their identity is not warranted. If a person is not identifiable, there cannot be a breach of the privacy standard. There may be a breach of other aspects of the law (for instance a breach of confidence) – or, in the broadcasting context, a breach of other standards – but questions of privacy are not relevant.

Failure to try to anonymise is clearly going to be problematic. An example was the *Target Electricians* decision, where no attempt had been made to disguise the complainant's identity. The Authority was comfortable that adequate pixellation (as had been done with the other featured electricians) would have kept the broadcast within the bounds of the privacy standard.

It is therefore still worth trying to protect people's identity. Reducing the chances of identification reduces the risks both of harming the individual concerned, and of ending up as the subject of a complaint.

However, the reality is that broadcasters should be wary about relying on disguising identity alone to protect against a breach of the privacy standard. There are too many risks that the disguise will fail. It can also provide a false sense of security to the broadcaster. Instead, in any case where publication might cause significant harm, broadcasters need to make sure that they have also employed other lines of defence: either the individual has authorised the broadcast so cannot later complain about it; or there is legitimate public interest in the information disclosed in the broadcast. These are the next topics that this report will cover.

Authorisation

Consent is commonly used as a defence to a breach of privacy both in statutory regulation and in tort. Privacy is often said to relate to a person's ability to control information about them and to make autonomous decisions. Real, or "informed" consent is a positive exercise of control and autonomy, but it is not a checkbox exercise. For consent to be something on which an organisation can rely as a defence, it needs to be "informed" – that is, the individual must understand the nature of the transaction to which they are agreeing. Some useful analogies can be drawn from contract law – the parties must understand and agree on the material points of the contract for it to be valid.

The Privacy Act does not use the term "consent"; instead it refers to "authorisation". However, the concept is analogous. "Authorisation" clearly implies a reasonable level of knowledge about the

material terms of the transaction, and a willingness to engage in it. As the Commissioner's inquiry into insurers' collection of medical notes stated: [19]

> *Our inquiry has concluded that the main problem here is that it is not always clear that that clients know what they are authorising. While 'authorisation' is not as high a standard as medical concepts of 'informed consent', a client does need to have an adequate level of knowledge about what they are agreeing to before an authorisation will be valid.*

The Authority has always recognised consent as a defence under the privacy standard, and the relevant principle also recognises that consent needs to be informed:

> ***Privacy Principle 5: Informed consent defence to breach of privacy***
>
> *It is a defence to a privacy complaint that the individual whose privacy is allegedly infringed by the disclosure complained about gave his or her informed consent to the disclosure. A guardian of a child can consent on behalf of that child.*

The person does not need to appreciate all the consequences of giving an interview.[20] That would be too high a threshold for the broadcasting environment and would risk being an unreasonable limitation on freedom of expression. However, they do need to understand the key points of the transaction including that they are being filmed by a broadcaster, and what the filming will be used for.

Since it is a defence, it is up to the broadcaster to prove that the individual consented to the broadcast. Broadcasters have occasionally run into difficulty demonstrating consent where the original paperwork is no longer available, for instance because the production company no longer exists.

The decisions under review provided a good indication of how the Authority approaches the question of informed consent. Some particular factors to consider are as follows.

(a) Written consent is not the only form of consent that is acceptable

I agree with this approach. Some flexibility is required. It could be unrealistic to expect all recording of potentially privacy-invasive material to be accompanied with paperwork. Recorded oral agreement will also suffice. Sometimes, the circumstances may also clearly show that consent was provided. A person's demeanour in front of the camera, for instance expressing pleasure at the filming or deliberately attracting attention, may imply that they were willing to be filmed. Broadcasters should still be certain, though, that the individual understands what the filming is for (see the next heading).

Where practicable, though, written consent is most useful as it can more clearly show what it was that the individual believed they were agreeing to. This is particularly important for a

[19] "Collection of medical notes by insurers" (Privacy Commissioner, 2009) at para 15: http://privacy.org.nz/news-and-publications/commissioner-inquiries/collection-of-medical-notes-by-insurers-inquiry-by-the-privacy-commissioner/

[20] *CanWest TVWorks v du Fresne* (2008) High Court, Wellington CIV 2007-485-2060 at 18.

body such as the Authority which generally makes decisions based on the papers rather than on evidence gathered at hearings, where people can be more closely questioned.

Information asymmetry can be a problem for broadcasters when they are asserting implied consent. The broadcaster is in control of the transaction – the film crew knows exactly what it is doing and why. But it is not necessarily apparent to the individual being filmed at all. In *Search Warrant*, for instance, MA did not object to the film crew's presence and TVNZ said that he had willingly engaged with the camera crew. However, the Authority was correct when it did not accept that he had consented. As the Authority said, people on *Police Ten 7* are often not aware of their rights, and are unlikely to have had much experience in dealing with the media. The Authority thought it likely that MA did not know he could ask the cameras to leave:

> *"… the fact the camera crew accompanied the police onto MA's property would have given it the appearance of having legitimate authority to be there and may have influenced the complainant's apparent acquiescence to its presence."*

For those reality TV programmes that involve film crews accompanying authority figures (Police, Customs etc), this is an important dynamic to consider. There may be no real consent to the filming, let alone to the broadcast. The person may well not want to be seen as uncooperative with the authorities and may also believe they have little or no choice. However, obviously it will be easier in some circumstances to imply consent. Public figures, for instance, are likely to be familiar with dealing with the media, and can be more readily presumed to understand the nature of the transaction.

(b) **The person must know the purpose for which the recording will be used**

Again, a person does not have to appreciate all the consequences of being recorded. However, the High Court said in the *du Fresne* decision that:[21]

> *In my view, "informed consent" in a Broadcasting Code more obviously relates to an awareness of being interviewed, of knowing the true context of the interview, and of being aware of the purposes to which the interview is to be put. In other words, what use is planned for it. Thus Ms X would need to have known that she was being interviewed, that it was going to involve disclosing her name, medical status and history, and that it was going to be shown on national television as part of the news.*

The Authority found the shop owner in *The Inspectors* may have believed that the film crew was from the council rather than that the film would be used for a television show. Even the film crew could not believe that he had allowed them to accompany them into the back of the shop. The Authority commented that if he had been aware of the true purpose of the filming, the chances are high that he would not have consented.[22]

---

[21] *Du Fresne* at para 18.
[22] *The Inspectors*, para 25-28.

(c) **Only the consent of the individual concerned will count**

This rule has been established for some time[23] and is clearly correct. If consent is an exercise of autonomy and control over one's information, it would not make sense to say that someone else could make that decision for you. The only exception will be where a person does not have capacity to consent for themselves, and their guardian (or other legally recognised representative) makes that decision for them. Privacy principle 5 recognises this when it states that guardians can consent on behalf of children.

Two of the decisions raised this point. In *The Renters* the Authority said a landlord cannot consent to a broadcaster's entry into a house when the tenant is not home.[24] The information broadcast was clearly about the tenant, not about the landlord. Of course the landlord could not consent if the tenant was at home either. The rule is still equally apt, and in any case tenants have legal rights of possession, and of seclusion in their homes.

In *Target Electricians*, the broadcaster had communicated with the employer company with a summary of the trial findings, and asked whether it wanted the employees' faces to be blurred. It did not receive a reply. More importantly, though, it did not talk to the complainant electrician. The Authority commented that an employer cannot consent to publication of information on an employee's behalf.[25]

(d) **Lack of response does not mean there is consent**

Again, this must be correct. If a broadcaster is going to defend what would otherwise be a breach of a privacy principle on the basis of consent, a positive act is required.

The Authority has taken the view that silence from the individual cannot be taken as assent. For instance, in *Search Warrant,* the programme producer sent MA a consent form, seeking his permission to use the footage on *Police Ten 7*, and inviting him to make contact if he had any concerns about being identified. He did nothing – he did not return the form or talk to the producer at all. The language in the consent form was clear: return it *if you decide to give consent*. It was reasonable of MA to assume that if he did nothing, then there was no consent. It was essentially an opt-in. [26]

However, it should not assist the broadcaster to change the wording of the form to an opt-out (if you do not contact us to decline permission, we will use the film). The whole context must still be considered to see whether the person did in fact impliedly provide informed consent for the filming and broadcast. I would suggest that an opt-out of this type should never be acceptable. There are many reasons why a person might not return a consent form to a broadcaster, including that they never received it or did not understand it. The principle of "privacy by default" should apply – if the person does nothing, they will not be taken to

[23] *O'Connell v TV Works Ltd* 2007-067, at para 55.
[24] *The Renters*, para 20.
[25] *Target Electricians*, para 32.
[26] *Search Warrant*, para 44-46.

have consented. The broadcaster cannot use principle 5 to justify the broadcast. Instead it must consider other lines of defence.

In data protection law, the situation is rather more nuanced. Questions often arise about whether only an "opt-in" (a positive choice to engage) can amount to legal authorisation or whether an "opt-out" (an assumption of consent unless the individual says otherwise) is sufficient. Opt-in is clearly a stronger recognition of privacy rights, and again in principle the default setting should be that a person's privacy is protected if they do nothing.[27] However, opt-out is also recognised as valid in certain contexts, particularly where the chances of harmful impact on individuals is low. Sometimes it may also be impracticable to require express consent in the form of an opt-in.

However, taking a more nuanced approach is relatively acceptable as compared with broadcasting law, because data protection law contains important backstop safeguards for the individual. It is not possible to contract out of all the IPPs in the Privacy Act. For example, an agency is still restricted to collecting only the information that is necessary (principle 1) and the purpose of collection must be legitimate – it is not given free rein to do as it likes. A person cannot sign away their rights to request access to information. Centrally important is the fact that the individual must still be told that the information is being collected, and what it will be used for. They must also be told clearly that they can opt out if they wish but also what the consequences of opting out might be (principle 3).

There is still debate about what is appropriate in any given situation, but it is clear that complete transparency about the transaction is key in any case. For instance, European privacy laws recently introduced requirements for a website to state when cookies are being placed on a user's computer. Data protection authorities interpret the requirement differently. For some, it is enough to have a clear declaration on a website that cookies will be installed if the individual continues with use of the website (the user has a choice, but the default is to use cookies). Other authorities require websites to ask users to actively agree to the installation of the cookie – the website user cannot proceed unless they exercise that choice (the default is not to add a cookie). Whichever approach is taken, though, failure to communicate effectively with the consumer results in a breach of the rule.

Consent is not always possible, but is still useful as an option

In many circumstances, it will not be possible or desirable to seek consent from the individual featured in the broadcast. It may not be practicable to contact them, or the information about them may be disclosed on the spur of the moment.[28] If a broadcast shows a person in a negative light but the public interest nonetheless requires the information to be provided, then consent is also immaterial (as well as unlikely to be forthcoming).

---

[27] This is the second of the seven foundational principle in the concept of privacy by design: http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[28] Live broadcasts are particularly susceptible to this: see for instance *Dunedin resident*; *Ex family member*; and *Assault charges.*

However, for some types of programmes, particularly reality TV shows, consent is still an important component of the environment. In fact, it may be unfair to fail to seek consent where it is practicable to do so.

Legitimate attention

Legitimate public interest, in one guise or another, is a defence in all forms of privacy law. For example it is well established as a positive defence in the privacy tort arena,[29] as it is in the closely related action for breach of confidence.

As a data protection statute, the Privacy Act approaches the concept of public interest in a more specific way than at common law. There is no general "public interest" defence. Certainty is important for business arrangements in the data protection arena, so data protection statutes tend to specify what aspects of public interest might be relevant. The IPPs provide express exceptions allowing collection, disclosure, and non-provision of personal information in situations where the public interest is generally accepted to override privacy considerations. So, for instance, if an agency reasonably believes that someone's safety is at risk, it can disclose information to the appropriate authority.[30] Other exceptions in the Act cover prevention, detection and investigation of crime, and protection of the public revenue, trade secrets, administration of justice and legal privilege.

The Authority has always formally recognised legitimate public interest as a defence to a claim that the privacy standard has been breached. This recognition is particularly important to make sure that freedom of expression is limited only to the extent justified by law. Protection of privacy is itself a fundamental human right.[31] It can justifiably limit speech, but it is also subject to reasonable limitations prescribed by law. The concept of "public interest" goes a long way towards defining what those limitations are.

Principle 8 states that:

> *Disclosing the matter in the 'public interest', defined as of legitimate concern or interest to the public, is a defence to a privacy complaint.*

Discerning what is in the public interest is not always straightforward. However, the case of *Balfour* adopts a generally accepted list of matters that are usually said to be in the public interest:

- Criminal matters
- Issues of public health and safety
- Matters of politics, government or public administration
- Matters relating to the conduct of organisations which impact on the public
- Exposing misleading claims made by individuals or organisations
- Exposing seriously anti-social and harmful conduct.

---

[29] *Hosking v Runting*, at para 129ff.
[30] *Director of Human Rights Proceedings v Henderson* [2011] NZHRRT 10
[31] Privacy is not directly listed in the New Zealand Bill of Rights Act 1990. However, it is a right that existed in New Zealand law before the Bill of Rights was passed, and so is arguably protected by section 28.

So far, so uncontroversial. However, many of the decisions reviewed involve reality television programmes, where the lines between public interest and entertainment are blurred and claims of public interest tend to struggle.

The Authority correctly recognises that reality shows can have elements that are valuable to society. For instance, several of the decisions involve programmes that informed viewers about the rules that operate in a variety of situations, such as housing (*The Renters*), entering prison grounds (*Waikeria Prison*), and food safety (*The Inspectors*). In *Waikeria Prison*, for instance, the Authority classified the programme as being primarily entertainment, but recognised that there were some areas of legitimate public concern as well.[32]

The fact that the content of reality shows is so weighted towards entertainment, however, means that it is always going to be harder for broadcasters to rely on the public interest defence to rescue situations where they breach privacy. The more substantial the breach of privacy, the greater the degree of legitimate public interest needed to justify the breach.[33] And when there is a strong (even dominant) dose of entertainment in there, the chances of any serious privacy breach being excused tend to fade. Entertainment is a good excuse in itself, and is protected expression. But a privacy breach that causes harm to an individual is likely to be even more deserving of legal recognition.

Another problem for some of the decisions under review is that the public interest must relate to the disclosure of the particular information that is alleged to be a breach of privacy. For instance the fact that the broadcast deals with criminal matters – a classic public interest situation – does not mean that the actual disclosures can be justified.[34] In *Waikeria Prison* the Authority commented that if the complainant had admitted to an offence, or there was evidence of a specific and relatively serious crime so as to justify the disclosure of information about him, the broadcast would probably have been acceptable. But there was no evidence of a particular crime or illegal activity – the most that can be said was that the officer searching the car suspected there might have been drugs in the car at some stage (not necessarily connected to the complainant). He was not charged or arrested – he was simply sent on his way with a warning to stay away from the prison. The incident was at too low a level to justify identifying him.

This analysis is correct, particularly in an environment where the Bill of Rights is a key consideration. The Broadcasting Act explicitly recognises the importance of protecting privacy rights. While freedom of expression – including expression for the purposes of entertainment – can limit privacy, it should do so only to the extent that is proportionate to the interests being served.

Another line of defence – the individual has not suffered significant harm

A breach of privacy is generally not actionable unless it has caused or is likely to cause some form of harm. This is a natural result of privacy's beginnings in tort law. It would be possible in principle to create strict liability for privacy breaches, but to refuse a remedy unless the individual has suffered harm. However, as a matter of policy, this might open the doors too wide to liability, particularly in

[32] *Waikeria Prison*, para 8.
[33] *Waikeria Prison* para 31.
[34] *Waikeria Prison*, para 30.

situations where there are other relevant interests such as freedom of expression. It would also be much harder to meet requirements of proportionality (for instance in analysis under NZBORA) in circumstances where there was no harm to the individual.

The Privacy Act takes a firmly harm-based approach to liability for breaches of most IPPs. There is an "interference with privacy" only when some form of harm has occurred or is likely to occur from a breach of an IPP.[35] The only exception is where an agency fails to properly provide access to or correction of personal information on request – these are rights that are so fundamental to the operation of data protection law that they are actionable without proof of harm.[36] In all other cases, such as collection or disclosure of personal information, the breach must be harmful to the individual.

Harm can include financial loss, or loss of an opportunity (for example loss of a chance to get a job,[37] or an inability to put a case properly to a decision maker[38]). However, it most commonly includes significant emotional harm. Mere annoyance or discomfort is not enough – the emotional harm must be at a level above the 'ordinary'.

The Authority's privacy standard is also based on a requirement for harm, though differently worded. The privacy principles use the tort formulation (taken initially from United States privacy tort jurisprudence and adopted by the New Zealand courts): the intrusion, or the disclosure of facts about the individual must be "highly offensive and objectionable to a reasonable person of ordinary sensibilities". This is an objective test (a 'reasonable person' standard) rather than the more subjective calculation under the Privacy Act (can the individual demonstrate that they have in fact suffered harm – or are likely to suffer harm – as a direct result of the breach). In the majority of circumstances, though, the results are likely to be similar.

The Authority's analysis of whether the information disclosed is "highly offensive to a reasonable person" seems sound enough.[39] However, in an earlier review of Authority privacy decisions, Dr Nicole Moreham commented that the terminology can be confusing – the analysis of what is a private fact, where reasonable expectations of privacy lie, and whether a matter is "highly offensive" tend to be unhelpfully conflated.[40] I agree with Dr Moreham's criticism, and suggest that it is something that the Courts as well as the Authority will have to resolve at some stage. It may be possible to do this relatively simply – by discarding "highly offensive" and instead creating a more direct requirement for the breach of privacy to either have caused harm, or be likely to cause harm. The way in which the Privacy Act deals with questions of harm would be a useful consideration.

---

[35] Section 66(1).
[36] Section 66(2): see also *Winter v Jans* (2004) High Court, Hamilton, CIV-2003-419-854.
[37] *EFG v Commissioner of Police* [2006] NZHRRT 48.
[38] *Shahroodi v Director of Civil Aviation* [2011] NZHRR 6 (as an access case, the harm was only relevant to the remedy sought, but the discussion is useful in any case).
[39] For instance in *Renters*, the programme disclosed that the tenant had failed to pay her water rates, and that she had been given notice to leave; that she had caused damage to her house; and the agent made comments about her standard of housekeeping. All this information was capable of causing significant embarrassment to the tenant. In *Waikeria Prison*, there was a strong insinuation that DS had engaged in illegal activity. In *Target Electricians*, the complainant's standard of work was criticised (not strongly, but his professional reputation could still have suffered). And the fish and chip shop owner in *The Inspectors* was criticised for the state of hygiene in his shop, in a broadcast that may not have reflected the current state of affairs at the shop.
[40] "Private Matters" at page 14ff.

However, I do not suggest that the Authority should go it alone to revise the wording of the privacy principles at this time. The Authority's approach is closely aligned to the way in which the New Zealand courts have expressed the test as well as to overseas authority, and there is considerable benefit to maintaining that linkage. After all, broadcasters can be the subject of privacy tort proceedings as well as complaints about broadcasting standards. It could unreasonably fetter broadcasting activities if the standard they had to meet in the different forums was too different and broadcasters too uncertain about what they were legally entitled to do. Aligning liability in tort and broadcasting standards also provides greater certainty for individuals about the nature of their rights, particularly given the relevance of the NZBORA. Since broadcasters are generally not subject to the Privacy Act, it matters less if the overall test for liability does not exactly mirror the way the Privacy Act conceptualises harm. If the Courts reframe the test, however, the Authority should consider doing the same.

The cross-over between privacy, accuracy and fairness – further work is needed

The Broadcasting Act treats privacy differently from other standards. There is a recognition that a breach of privacy has a direct and harmful effect on individuals. A privacy complaint can be made directly to the Authority rather than having to complain first to the broadcaster. Also, privacy is the only area in which the Authority can make an award of damages to an affected individual.

However, privacy is not as distinct a concept as the Broadcasting Act would suggest that it is. In particular, there are substantial overlaps with fairness, and with accuracy (when the information that is inaccurate relates to an individual). Failures of fairness or accuracy are considered as breaches of privacy under the IPPs in the Privacy Act, when they involve information about individuals.[41] Incorrect information may be damaging in some situations where correct information would not cause harm. Covert filming is inherently unfair but can also clearly be an intrusion into solitude. Yet in the broadcasting environment, the distinctions are not plain. Decisions where breaches of both the fairness and privacy standards are pleaded are often repetitive because essentially the same calculations can apply under each. The most important factor sometimes seems to be how the complainant has chosen to categorise their grievance. This is not a criticism of the Authority – it is simply a reflection of the difficulties that the current statutory scheme creates.

There may be an argument for saying that if a complaint about a broadcast is in fact about collection or disclosure of personal information – that is, information about an identifiable living person – the privacy principles are triggered whether the complainant describes it in terms of the privacy standard or not. But there are some practical as well as legal ramifications of taking this step. Resolving these questions falls outside the terms of my current review. However, I recommend that the Authority should consider doing some further research in the field. It may be possible to improve the advice it provides to the public about the different standards, or adjust the approach that it takes to dealing with complaints where there are overlaps.

[41] For instance, IPP 4 requires agencies to use methods of collecting personal information that are lawful, and not unfair or unreasonably intrusive in the circumstances. IPP 8 requires agencies to take reasonable steps to make sure that information is accurate, complete, relevant, up to date and not misleading before they use that information.

Remedies

A breach of privacy is unique under the Broadcasting Act in that the Authority can order the broadcaster to pay compensation to the person affected.[42] The availability of an order to pay compensation is common to the other major areas of privacy protection in New Zealand (the privacy tort and the Privacy Act).

Nine out of the eleven TV decisions that I considered found a breach of the privacy standard, and the Authority made an order for payment of money to the complainant in 5 of those cases. Other orders are also available, most commonly payment of costs to the Crown (a punitive order) for egregious breaches of the privacy principles.

The basis for an award of damages is to compensate the individual

It was unclear from my review of the decisions how the Authority makes decisions about awarding damages. In some cases, the fact of breach appears to be a reason for making an award,[43] where in others (*Target Electricians, The Inspectors* and *Stem cell treatment*) it is unclear why no award was made. The decisions often include references to the effect that the broadcast has had on the individual, but these can be scattered throughout the decision rather than brought together at the point where the Authority is considering whether to award compensation and if so how much. I recommend instead having a specific, clearly labelled section in any decision where compensation is a possibility, to make it easier to follow the Authority's reasoning.

Section 13(1)(d) of the Broadcasting Act expressly states that the order is "compensation". It is therefore puzzling to find that the Authority refers to the awards as "costs to the complainant for breach of privacy". I recommend that the Authority should switch its terminology. This is not mere semantics – compensation and costs do not usually mean the same thing. The analysis differs, and the evidence is assessed differently too. Using the language of the statute will help the Authority to focus on the points that are relevant to considerations of compensation.

The Authority is in an unusually difficult position when it comes to assessing awards of compensation. Most decision making bodies will have the benefit of direct evidence about the effect that a breach of privacy has had on an individual. For example, the Human Rights Review Tribunal receives formal evidence from individuals complaining about breaches of the privacy principles, so it can assess their credibility and make well-reasoned calculations about the level of harm that the respondent has caused. But the Authority almost always makes its decisions on the papers. It does not require sworn statements. The complaint form on the website does not ask people to explain what effect the programme has had on them, or ask them to specify what kind of order they are seeking.[44] This might be one reason why the shop owner in *The Inspectors* did not claim compensation – his lack of submissions on the point appears to have been one reason why no award was made, but he may have been unaware what it was that he could ask for. I suggest that a section on the form asking people for this information is an essential addition, to help the Authority assess whether the broadcaster has caused harm to the complainant and, if so, what the level of that harm is.

---

[42] Section 13(1)(d).
[43] For instance in *Waikeria Prison*, there is no indication whether the complainant asked for an award of compensation.
[44] http://bsa.govt.nz/images/assets/Complaints/BSA-Printable-Privacy-Complaint-Form-May-2012.pdf

It is obviously beneficial to keep matters as informal and unstressful for parties as possible, and not to incur unnecessary expense either for the parties or for the Authority. However, I suggest the Authority should also consider receiving direct evidence on harm from people (either through a hearing or through sworn statements). For instance, Skype or other videoconferencing technologies make it increasingly feasible and inexpensive to talk directly to people. Where credibility is an issue, as the broadcaster argued it was in *Solvent Abuse*, this would allow the Authority to assess the credibility of the complainant for themselves. It would not need to go as far as allowing cross-examination or other formal procedures to test evidence. But it would give a stronger basis for the Authority to make decisions about awards. Even if the Authority is only prepared to consider additional gathering and testing of evidence on a temporary basis, this would be valuable. It could help the Authority to establish new analytical principles about compensation, particularly if it accepts my suggestion about raising the levels of compensation it is prepared to award.

There are a couple of other points to note here. First, harm for which a person is compensated needs to be the direct result of the broadcaster's breach of privacy. This is a standard reflection of principles of causation in tort law. Often causation is not hard to establish in this environment – were it not for the broadcast, information about the complainant would not have been known to their employer, their friends, or the world at large. However, privacy can often be one factor in a much more complex situation (for instance an existing employment dispute, family breakdown or neighbourhood conflict), and it is important to consider what part the broadcaster actually played in exacerbating matters for the complainant. In some cases, the answer may be "not much".

Secondly, compensation is different from a punitive award. The behaviour of the broadcaster or the severity of the breach of the privacy principles is simply not relevant except to the extent that it has in fact caused, aggravated or mitigated the harm that the person has suffered.[45] If the broadcaster has behaved in a way that warrants punishment, this should be recognised by use of the other orders, such as costs to the Crown. It should not be allowed to confuse the analysis about compensation.

The amount of damages awarded is out of touch with privacy awards elsewhere

It is also unclear how the Authority decides how much to award. It considers what was awarded in earlier decisions, and appears to consider how serious the breach was in relation to earlier awards. This approach is fine (a) as long as the earlier awards were justified and (b) as long as the context of decisions about damages has not changed in the intervening time. I suggest that the earlier awards have been out of touch with movements in privacy law for many years now, and that decisions about compensation need to keep pace with the times if they are to have any meaning.

The maximum amount that the Authority can award is $5000. Obviously, only Parliament can change that. However, the Authority can legitimately consider how it exercises its discretion to make awards within that maximum limit. The question to me is simply what award will actually compensate the complainant for the harm that they have suffered, as far as the maximum limit permits the Authority to act.

[45] See for instance *Yeo v McDowell* [2006] NZHRRT 11 at 48.

The $5000 limit is extraordinarily modest by the standards of privacy compensation today (even though privacy awards are nowhere near the levels of some other areas of compensation such as defamation). This should have some effect on the level of the awards that the Authority is prepared to award. In other areas of privacy law $5000 would be seen as a nominal amount to compensate the victim for harm suffered from a breach of this important right. For instance, the Human Rights Review Tribunal has made several awards of between $10,000 and $20,000 for breaches of principle 6 (the right to access personal information about oneself on request).[46] The only recent case involving disclosure of personal information resulted in a $15,000 award.[47] The highest award so far made in the Privacy Act arena was $40,000, again in a disclosure case but more than a decade ago. One can presume it would be a very great deal higher if that case had come before the Tribunal today.[48]

In the past the Authority has been willing to go to the maximum only in the most serious cases. As far as I can tell, it is around seven years since the Authority has awarded the full amount.[49] Moreover, the awards in the cases I considered are extremely low: $500 (*Baby goods)*, $750 *(Waikeria Prison)*, $1000 *(Solvent abuse)*, $1500 *(Search warrant)*, and $500 *(Matchmaking)*. While these awards may be logical in the context of what the Authority has awarded for similar breaches in the past, they are frankly far too low to be a meaningful remedy for the breach of the right. Parliament has singled out privacy as a right that deserves particular attention in the broadcasting context, and has provided that the Authority can order a unique remedy. But Parliament's intention will be undermined if the remedy awarded is not more realistic.

The Authority obviously needs to exercise its statutory discretion in a reasonable and lawful manner. However, awards made for breach of privacy in other areas are clearly a relevant consideration. And while awards for breach will always give rise to arguments about chilling of speech, with a limit of $5000 (unchanged since 1989), this should not be an overwhelming consideration. The media organisations in question also have to deal with other potential liability in fields such as defamation or breach of confidence. Even the privacy tort has resulted in far more significant awards than are available here, without creating a crisis for chilling of speech.

I therefore recommend that the Authority should completely rethink its approach to compensation. If harm does not speak for itself, then it should be based on evidence from the complainant, so that it is properly justified, and further testing is warranted in any case where credibility is an issue. However, I suggest that the starting point for consideration should be the $5000 maximum. It should be reduced only if there is justification for doing so – most obviously if the harm is not particularly serious, but also if the broadcaster has mitigated the effect on the complainant, or if the complainant has contributed markedly to the situation.

---

[46] *Lochead-Macmillan v AMI Insurance* [2012] NZHRRT 5; *Director of Human Rights Proceedings v INS Restorations Ltd* [2012] NZHRRT 18; *Director of Human Rights Proceedings v Hamilton* [2012] NZHRRT 24.
[47] *Geary v Accident Compensation Corporation* [2013] NZHRRT 34
[48] *Hamilton v The Deanery* [2003] NZHRRT 28. The maximum the Tribunal can award is $200,000.
[49] *LM v TVNZ*, 2007-138.

Conclusions

The Authority has one of the most developed bodies of privacy law in New Zealand. It deals with privacy queries routinely and is expert in the field. Its jurisprudence is also deservedly influential in other areas of privacy law and practice. In fact, its decisions should be referred to more often than they are.

However, like all good things, improvements are possible. I hope that this review provides the Authority with some useful food for thought about ways in which it might further develop its expertise in this high profile and vitally important area of law.

Katrine Evans
June 2014

Appendix One: Terms of Reference

The terms of reference for this review were for my report to cover:

- How the approach that the Authority takes to its privacy decisions compares with the approach taken by the Privacy Act, looking particularly at the topics of identification, informed consent, informed participation, public place and public interest.
- Legal robustness of the decisions
- Quality of legal reasoning
- Style and structure – readability and clarity of decisions
- Degree to which the decisions provide guidance and useful clarity on the Authority's approach
- Consistency of approach (where possible, given small sample size)
- Overall analysis with suggestions.

Appendix Two: List of decisions considered

To make the report easier to follow, I have given a descriptive name to each of the decisions that the Authority particularly wanted me to review (not that all have ended up being referred to in the report):

- "**Girl gangs**": *Hastings District Council v TVWorks Ltd*, 2009-088
- "**Drowning tragedy**"**:** *Rae, Schaare and Turley v TVNZ Ltd*, 2010-007
- "**Search warrant**": *MA v TVNZ Ltd*, 2010-084
- "**Solvent abuse**": *MQ v TVNZ Ltd*, 2011-033
- "**Waikeria Prison**": *DS v TVNZ Ltd*, 2011-144
- "**Baby items**": *Hodson v TVWorks Ltd*, 2012-012
- " **The Inspectors**": *FS v TVNZ Ltd*, 2012-036
- "**Target electricians**": *CP v TVWorks Ltd*, 2012-069
- "**Stem cell treatment**": *Dr Z v TVNZ Ltd*, 2012-074
- "**The Renters**": *Vertigans v TVNZ Ltd*, 2013-045
- "**Police dog attack**": *Moore v TVNZ Ltd*, 2013-093

Since all these decisions involved the Free-to-Air TV Code, I also suggested that I consider some decisions under the Radio Code. These were:

- "**Matchmaking**": *NJ v Apna Networks Ltd*, 2010-066
- "**Assault charges**": *Stables v RadioWorks Ltd*, 2012-105
- "**Ex family member**": *AB and CD v Access Community Radio Inc*, 2013-005
- "**Dunedin resident**": *Hill v Radio One*, 2013-074