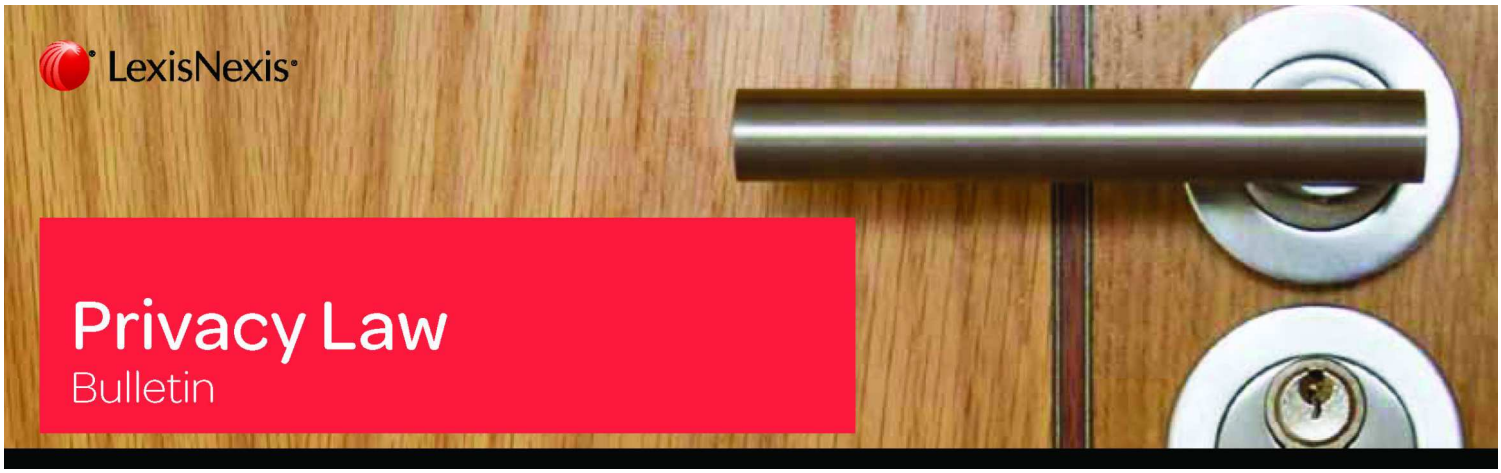

Privacy Law Bulletin

2019 . Vol 16 No 3&4

Contents

Information contained in this newsletter is current as at June/July 2019

LexisNexis® Butterworths

Caught on camera — the admissibility of audio and video recordings in family law matters — Part 2: the cases

Justine Woods *COOPER GRACE WARD*

- Courts will look at the factors in s 138 Evidence Act 1995 (Cth) when deciding whether or not secret recordings will form part of the evidence, but that list is not exhaustive.
- The cases reflect that attention will be paid to how the party obtained the evidence and an analysis of the probative value and importance of the evidence in the proceedings will be critical when the judge is deciding whether the desirability of admitting the evidence outweighs the undesirability of allowing in improperly obtained evidence.
- The court will also have regard to s 135 of the Evidence Act in its deliberation, which is the general discretion to exclude evidence.
- The scrutiny and weight of evidence once admitted is open to the judge once certain tests are passed.
- If the recordings pass the ss 138 and 135 tests, it is then open to the judges to scrutinise the evidence and give such weight to it, as they find appropriate, having regard to the issues in dispute and in parenting matters, the legislative pathway to determining what orders should be made about children.
- The cases reflect the full range of assessment of recorded evidence — for example, given profound weight in cases where unacceptable risk of harm to children was borne out (usually by a finding of sustained family violence) to evidence given little if any weight.
- The recordings can potentially backfire on the person making them — understanding the risks, including the criminal sanctions which may apply is important.
- Some of the risks lawyers should raise with their clients regarding tendering recordings as evidence include:
  - — the risk of police prosecution where the recording was unlawful
  - — the risk that the evidence will not be admitted
  - — the risk that the evidence will not be given any weight or determine the outcome as the client anticipates
  - — that the recording can be seen as a form of actionable domestic violence under each state and territory's Domestic and Family Violence Acts or in circumstances be regarded as stalking and
  - — the risk that the evidence will backfire on the party seeking to adduce it, whether or not the evidence also reflects poorly on the party secretly recorded
- The case of *Leos v Leos*[1] a decision by Le Poer Trench J illustrates the significant risk of criminal penalty when obtaining recordings. The father, in hiring a private investigator to audio and visually record the mother and children, breached the Crimes Act 1900 (NSW), and was sentenced to two 18-month bonds and fined $1000.
- Lawyers should also be extremely cautious when including evidence of parents directly questioning children — it is difficult to think of a circumstance when this will play well before a court, let alone represent sound or even "good enough" parenting.
- *Janssen & Janssen*[2] is a recent case on family violence where recordings were a vital aspect. The recordings made by the mother, which were prima facie unlawful under the NSW legislation, were admitted into evidence as they showed the father's propensity to commit family violence, both physical and sexual, towards the mother and children.
- Cases from around Australia highlight the differences between states' recording legislation, and the attitudes to admitting recordings of family violence in different circumstances.

What factors does the court look at when deciding whether or not secret recordings will form part of the evidence

The court will look at the factors in s 138 but that list is not exhaustive.

The cases reflect that attention will be paid to how the party obtained the evidence and an analysis of the probative value and importance of the evidence in the proceedings will be critical when the judge is deciding whether the desirability of admitting the evidence outweighs the undesirability of allowing in improperly obtained evidence.

The court will also have regard to s 135 of the Evidence Act in its deliberation which provides:

> **General discretion to exclude evidence**
> The court may refuse to admit evidence if its probative value is substantially outweighed by the danger that the evidence might:
> (a) be unfairly prejudicial to a party; or
> (b) be misleading or confusing; or
> (c) cause or result in undue waste of time.

The *Huffman v Gorman (No 2)*[3] litigation contains some guidance as to the manner in which the court will approach the task at [46]–[47]:

> It was submitted on behalf of the mother that … the father was able to manipulate and set up the environment in which the conversations were recorded, which resulted in the mother being portrayed unfavourably. It was also submitted that as the recordings were only parts of the conversation and did not record the events that led up to those conversations and they were thereby prejudicial to the mother.
> However, it is unclear on what basis the mother asserts that the admission of the recorded conversations would be **unfairly** prejudicial to her as required by the section, especially where she concedes that the transcripts accurately record the words spoken. The circumstances of their making, and the suggestions in some way the environment was manipulated can be the subject of cross-examination of the father and may ground submissions as to the weight to be attached to the recorded conversations. … the probative value of these conversations is significant and in circumstances where it is not been clearly identified how the admission of the evidence may be unfairly prejudicial to the mother, the evidence … should not be excluded …

On the question of the probative value of the evidence, Hannam J found that the recordings were:

> … highly probative of the issue of family violence which has been raised by both parties as they provide contemporaneous actual evidence of conversations in which threats of violence and abuse are directed by one party against the other.[4]

Her Honour also considered that that evidence was "very important as it goes to the heart of this matter",[5] and that the father's conduct was towards the "less serious end of the spectrum".[6]

Further, her Honour noted that it is "notoriously difficult to obtain evidence of family violence which takes place behind closed doors".[7]

These comments correspond to the factors in s 138.

The scrutiny and weight given to evidence once admitted

If the recordings pass the ss 138 and 135 tests, it is then open to the judges to scrutinise the evidence and give such weight to it, as they find appropriate, having regard to the issues in dispute and in parenting matters, the legislative pathway to determining what orders should be made about children.

The cases reflect the full range of assessment of recorded evidence — for example, given profound weight in cases where unacceptable risk of harm to children was borne out (usually by a finding of sustained family violence) to evidence given little if any weight.

Jasper v Corrigan (No 2)[8] is a case which emphasises the distinction between admissibility and weight, but as a preliminary judgment does not contain any finding about weight.

In this case, the court had to determine the admissibility of audio recordings the applicant argued would prove the existence of a de facto relationship between herself and the respondent. The parties had a 3-year-old daughter but the respondent contended a mere sexual relationship.

It was not in dispute that the recordings were obtained without the respondent's knowledge. He contended that they were illegally obtained, while the applicant argued that the recordings fell within an exception.

The relevant legislation was the Surveillance Devices Act 2007 (NSW). The applicant sought to rely on the exception in s 7(3)(b)(i), which allows recording without the consent of the other party if it is reasonably necessary to protect the interests of the principal party. The respondent maintained that the exception was not satisfied.

The court concluded that the applicant did have a lawful interest to protect. His Honour Altobelli J made reference to *Janssen*, because although the facts were entirely different, the difficulty in obtaining evidence of a de facto relationship was considered comparable to obtaining evidence of family violence. This aspect of Altobelli J's decision is set out below:

> [19] **Does she have a lawful interest to protect? The Court believes that she does**. The Court does not accept the highly rigid and narrow interpretation of lawful interest that was advanced by Counsel for the Respondent and which, for example, is quite inconsistent with the approach adopted in *Janssen & Janssen* and the cases referred to therein. Indeed, despite Counsel's attempt to distinguish Janssen & Janssen and the cases referred to therein, the issue in this case is not all that conceptually different to *Janssen or Huffman & Gorman* (No.2).
> [20] The violence that is referred to in those cases took place in private. The notoriety of establishing that which occurs in private, especially family violence, is something that the Full Court of the Family Court has taken judicial

> notice of. How is it conceptually different here? In private, the Applicant and Respondent appear to have had certain conversations. The Applicant contends that those conversations were about the nature of their relationship. That is the fundamental matter in respect of which the Court must decide under section 90RD. It is her word against his. There are only two witnesses in this case. It is an uneven contest with the Respondent represented by very experienced solicitor and counsel, and the Applicant representing herself.
> …
> [23] … [This] is not ruling on the weight that will be given to evidence. Evidence might be admissible but it might not receive much weight.
> [24] Indeed, the significance of these comments is particularly acute in a case like this where because of the way in which the case has been run, it is necessary to make rulings about evidence which is of an unspecific nature. …[9]

The applicant was ordered to provide to the respondent's solicitor in electronic form, audio recordings of no more than six conversations that she asserted were relevant to the issue of the nature of a relationship between the parties, plus an affidavit that set out the factual context of the making of the audio recordings, the date and time of such recordings and attach a transcript of the same recordings.

His Honour granted the applicant a certificate against self-incrimination under s 128 of the Evidence Act in relation to the evidence required by his orders.

In *Jasper v Corrigan (No 3)*,[10] the judge recused himself and transferred the case to the Family Court.

Corby v Corby (No 2)

Her Honour Sexton J was required in this case[11] to make parenting orders in respect of an 11-year-old boy where the mother alleged that the father was sexually, financially and psychologically controlling and coercive towards her over their 13-year relationship in a manner which had also affected and damaged their son. The father had spent limited periods with the child since separation in the 2 years prior to the trial, with no overnights.

The mother deposed that she had taped an occasion when she had refused the father's demand for sex made when their son was present. She said she had taped him yelling at her to come up the hall to give him sex "so I could have some proof of what I had been experiencing in the relationship".[12]

Three months later the mother made a further two brief audio recordings taping the yelling:

> … because I felt no one would ever believe that I was living in such a relationship. I felt that I needed to make the recordings for myself so that I would have some proof to remind myself of what my life was like.[13]

Sexton J discussed whether the recordings were reasonably necessary, a requirement under s 7(3)(b)(i) of the Surveillance Devices Act (NSW) and referred to the private nature of the circumstances of sexual and family violence. As discussed:

> [30] The evidence also discloses that the Father may have had a public face very different from his private face, a possibility accepted by Dr Q, who agreed that the Father may be charming and delightful in company, while intimidating and frightening in the home, as alleged by the Mother. The Mother here, as in *DW v R*, was not trying to extract an admission, as in the case of *Sepulveda v R*, but rather to establish her credibility if there was ever a dispute about what had actually happened.[14]

Although unnecessary as the recording was considered legal by the court, Sexton J discussed whether the court would have admitted the recordings under s 138 of the Evidence Act if the recording was illegal.

The mother's counsel argued that this case concerned risk, and if the recordings were admitted, they would corroborate the mother's version of the father's behaviours. The father agreed the content of the recordings could be significant in the case, however admitting the evidence would be unfairly prejudicial to him.

The court's reasons for admitting the evidence are outlined below:

> [36] In determining that I would have exercised my discretion in favour of the Mother on this issue, I have regard to these matters:
> a) These are parenting proceedings concerning an 11 year old child, and the court must therefore determine what parenting arrangements are in the child's best interests. The parenting capacity of each party is squarely in issue.
> b) The Mother alleges a pattern of coercive, controlling conduct towards her during the 13 years of the parties' relationship, allegations substantially denied by the Father, but which, if found to be true, are extremely serious, impact on parental capacity, and may lead the court to conclude that the child is presently at risk in the Father's care. The evidence is therefore relevant, and potentially important.
> c) In determining X's best interests, the court must give priority to his physical and psychological safety. The recordings are relevant to that issue.
> d) Dr Q, the court expert, emphasised the pivotal importance of the court's finding as to whether or not the Mother has told the truth about how the Father behaved during their relationship when deciding what parenting arrangements would be in X's best interests. Dr Q said that the Father made no admissions and showed no remorse, so if the Mother has been truthful, the problems are, indeed, serious, and would have a significant bearing on her recommendations. In her opinion, interpersonal violence and sexual coercion will not be modified by counselling.
> e) The improper conduct by the Mother in the obtaining of the evidence is not of the worst kind. There is no suggestion it was contrived in some way.
> f) It is unlikely the Mother would have been able to make the recordings with the permission of the Father.[15]

It is clear that the safety of the child in the proceedings, X, was considered more important than any potential prejudicial effect to the father. Therefore, the court admitted the recordings.

The final outcome of this case was handed down by Sexton J in *Corby v Corby (No 2)*. Her Honour stated:

> [67] I accept the truth of the mother's allegations as to the father's sexually coercive behaviours… Her evidence was at all times consistent, while the Father's was not…
> [68] [I am satisfied] The Father's own admissions corroborate the mother's version of events, though I find he understates the frequency of his sexual demands and activity. The Father acknowledges being "annoyed" with the mother and angry, but "not all the time", when she would not give him what he wanted sexually. Having listened to the audio tapes, I find "annoyed" an understatement of his attitudes … The audio recordings reveal the manner in which the father at times speaks to the mother. The terms and tone are derogatory, threatening and abusive.
> [69] I find the Father was indifferent to the impact of his behaviours on the mother and on [the child].
> …
> [100] In [the single expert]'s opinion if [the child] had heard or witnessed behaviours revealed on the audio tapes [on the occasion which he did hear] more than once, [the child] will have conflicting feelings and also possible conflicting identifications…
> …
> [113] I am satisfied the Father engaged in family violence when he repeatedly taunted the mother in derogatory terms as she alleges, behaviour graphically illustrated on the audio recordings.

The judge ordered sole parental responsibility in favour of the mother and that the father should have day visits only until the child was 14 at which time the mother may consider increasing the time to include overnight at her election and with the child from age 16 to be free to spend time including overnight time with the father in accordance with his own wishes.

Risks

Family lawyers are not always asked for their advice before the client has embarked on a course of action such as secretly recording a conversation or event. Preferably at the commencement of the matter and certainly before including any evidence in the material, lawyers should discuss with their clients the risks of recording, which include:

- the risk of police prosecution where the recording was unlawful
- the risk that the evidence will not be admitted
- the risk that the evidence will not be given any weight or determine the outcome as the client anticipates
- that the recording can be seen as a form of actionable domestic violence under each state and territory's Domestic & Family Violence Acts or in circumstances be regarded as stalking and
- the risk that the evidence will backfire on the party seeking to adduce it, whether or not the evidence also reflects poorly on the party secretly recorded

The case of *Leos v Leos*[16] a decision by Le Poer Trench J illustrates the significant risk of criminal penalty if a client obtains the recordings in a manner not regarded as being at the "less serious end of the spectrum" quoting Hannam J in *Huffman v Gorman* — for example here, by engaging a 3rd party to secretly record the other parent.

It is also a salutary reminder that clients must be repeatedly advised that even if they have evidence of what seems to them to be grave, dis-entitling conduct on the part of the other parent, the outcome may not be as they expect. Despite the audio and video evidence appearing to be such powerful and incontrovertible evidence to the party seeking to rely on it, such recordings are simply evidence like any other category of evidence — to be considered by the judge as party of a mix of factors.

In this matter, the parents of three young children each alleged the other had committed family violence towards them and the children. The father made numerous complaints to the police and welfare authorities which were not actioned. After a neighbour of the mother told the father of alleged daily abuse of the children by the wife, the father hired a private investigator to audio and visually record the mother and children in the former matrimonial home between July and August 2014 and applied for parenting orders.

He was shortly arrested by the police and ultimately pleaded guilty to installing or using a listening device to record a private conversation and secondly to publishing a private conversation. He was sentenced to two 18-month bonds under the Crimes Act 1900 (NSW) and was fined $1000. He consented to an apprehended violence order (AVO).

The transcript of the surveillance tapes shows the mother screaming and swearing at the children "in language which was degrading and abusive to them" in the words of the judge, calling them vile names and striking and threatening the children, including threats to put needles in their nappies if they couldn't stop bed wetting at night or cutting their arms off.

The judge did not even have to look at the tapes because the mother conceded she had engaged in some of the alleged behaviour and had sought out community and therapeutic support.

In giving his reasons at [5]–[6] his Honour stated that:

> The mother [was] parenting very young children in what I am satisfied was an appallingly abusive manner. Being a child of the electronic age, [the father] resorted (I am satisfied out of the frustration or legitimate concern for his children) to the use of readily available hidden surveillance equipment.
> I am satisfied that the recorded material he obtained from that surveillance provided compelling evidence to support his case that the mother was at the time abusing his children in the manner of screaming at them, physically chastising them and using appalling profanities and threats which terrified those children.

Le Poer Trench J noted at [317]–[319]:

> I note here that it is my conclusion that had the father not taken the extreme and illegal path of installing surveillance equipment and recording the mother in the manner in which he did, I conclude it is unlikely that the mother would have conceded the level of abuse that she was perpetrating upon children which she ultimately conceded in the hearing before me. This statement is not made to justify an illegal action or to promote in others that such an action should be taken. It is made simply to recognise a frustration which the father faced at that time. I note that the father was appropriately dealt with by the law for having installed the surveillance equipment.
> The circumstance in which the father found himself is not an uncommon scenario as seen in litigation in this Court. How does one prove family violence which occurs behind the closed door of the matrimonial home? Invariably, accusations of family violence are met by total denials.
> The circumstance of the father using surveillance equipment to prove his case is novel for me, however, similar types of surveillance have been a feature in prior cases, although that usually involved the use of hidden video cameras or telephones. I do predict, however, as devices commonly in use in our society, such as mobile phones, develop even more capabilities than they currently have, the type of surveillance evidence which is sought to be relied upon will become a common feature in litigation in this Court.

The single expert, a clinical psychologist, assessed both parents as having marginal parenting skills.

The expert's opinion was that the children's needs would best be met by continuing to live primarily with the mother and spending significant time with the father, who although described as having a fun and affectionate relationship with the children was permissive and chaotic in his parenting style but also resorted to corporal punishment when strained.

With some reluctance it seems, his Honour ordered that the children stay with their mother and have alternate weekends, an additional overnight and holidays with the father. He concluded at [536]–[538] with:

> There was no cross-examination of the single expert which either shook her confidence in her recommendation nor was there enough compelling evidence to convince me the Court should not accept the expert evidence of the single expert.
> Having so concluded, I do want to record that I was shocked and confronted by the type of emotional abuse these young children were subjected to from their mother prior to her leaving the former matrimonial home. There is no evidence of that type of abusive parenting taking place since the move, however, it has to be said that the mother does not have a person such as 'the neighbour' to report same to the father.
> The single expert is as confident as she can be that things have changed for the children in the mother's home. I rely upon that expertise in framing the orders in this case.

In *Masri and Masri*[17] each parent sought to rely upon recordings they had made. After conducting voir dire hearings, the applications to admit were both dismissed.

The mother sought to adduce evidence she had recorded on her phone of the father allegedly hitting the child and threatening to do so again.

The father sought to adduce an audio recording of an incident where he was arrested and charged with assaulting the mother, however was later found not guilty.

The court found, first, that the mother's evidence was obtained illegally pursuant to s 7 of the Surveillance Devices Act (NSW), and no exception could be made out. The court then considered the operation of s 138 of the Evidence Act.

The court stated the following:

> [29] In my view while the evidence in question may have significant probative value as to the fact in issue this fact [in] issue is not of great importance in the proceedings, having regard to the competing parenting proposals. Although the mother contends that the evidence captured in the video recording is relevant to the father's "anger management issues" and parenting of the children, her concerns about these matters cannot be of great significance when she proposes that the parties equally share parental responsibility for the children and that the children spend substantial and significant time with their father. She also does not seek an order restraining physical discipline in her final parenting proposal. Further, the father does not dispute that he had [raised his hand] to the child, told her to "shut up" and said "do you want another one" (after [he says] the mother [not him] had smacked the child) prior to the commencement of the recording. In other words, the difference between the two versions of events is very limited.

The court concluded that the desirability of admitting the evidence did not outweigh the undesirability of admitting evidence that had been illegally obtained; "balancing the seriousness of the conduct in recording against the potential for harm to the children if the evidence is not admitted". There were other ways to get the evidence of the incidents other than illegal recordings — such as including an account of the events in their affidavits.

The father's evidence was also obtained in contravention of the Surveillance Devices Act (NSW). This evidence was not included either after a consideration of s 138 of the Evidence Act. The probative value of the evidence was not considered high and there were disputes as to its accuracy.

The case also illustrates the risks if your client's case theme and proposals are not consistent with the position sought to be advanced or supported by the recordings. Here the parents agreed that they should share joint parental responsibility, and each should have some time with the children and no injunction against physical discipline had been sought. The final orders made were for the children to live with the mother and spend time with the father.

Counter-productive risk

In the Victorian case of *Simmons v Simmons*[18] the parties had entered into consent orders in respect of their young daughter which provided for shared care. The mother alleged sexual abuse by the father and his time was then supervised.

There is no commentary in the judgment about the admission of the evidence of the mother of conversations she secretly taped of the father speaking to the child by telephone and of conversations between the father and the supervisor, which the mother alleged were denigrating of her.

Having listened to the recordings of the father and child, McGuire J was satisfied on the balance of probabilities that the father had encouraged the child to be uncooperative during court-ordered telephone time by telling her to talk in baby talk giving him "ammunition for complaint to the Department of Human Services" and that that was "selfish behaviour [which] fails to recognise the potential effect on a young child of being embroiled in such a way in parental dispute".[19]

The mother had taped the conversations which took place at the contact centre by placing a recording device on the child's clothes or in her bag or belongings. The supervisor (whose report was so favourable to the father that it was put to her the relationship with him had become personal) "readily conceded [in cross examination] she may have had conversations in the presence of [the child] which referenced the mother and which were inappropriate".

Comparing the father's conduct as described above to the mother's, McGuire J observed at [109]:

> … Similarly, however, the mother's actions in sending the child for supervised visits with recording equipment secreted on her is similarly appalling behaviour. The actions of both these parents are at best naïve and at worst a form of child abuse. In this sense they are equally culpable…

He ordered that the Consent Orders remain in force.

An extreme example of a litigant's case being detonated by the recordings introduced by them hoping to gain advantage is the decision in *Farrelly v Kaling*.[20]

In that case the father applied to have the parties' 4-year-old son live with him at his parents' home in Sydney. He alleged the mother had sexually abused the child, locked the child in rooms and was "mad".

The mother sought to remain with the child in Cairns.

The court and the single expert listened to more than 70 recordings produced by the father, mostly of him and the child talking. The father is heard to ask the child about how his mother plays with his penis, how she makes him eat margarine on chocolate or strawberries with vegemite so that he will "vomit, vomit", how she slaps him and tells him to hurt daddy.

The report writer gave evidence, summarised by Federal Magistrate Willis at [113]–[114] that the father's interaction on the tapes with the child is:

> … becoming quite toxic, the father has been making constant criticisms of the mother [which are] escalating. [The report writer] was unsure if the father was doing this consciously or unconsciously. However, what she heard on the tapes was that [the child] was starting to mirror his father's intense dislike for the mother. She considered that [the child] was being groomed. [The father] was cueing the child and when he asked the questions as heard on the tapes, that the child knows what he has to say.

For example, the father is heard to say:

> … so as well as being locked in the room screaming, what else happened? Did she play anything?" The child says "no, she got angry". The father then says "oh she gets angry all the time."

The judge found that the father gave a "first impression of being a pleasant and easy going person who has had a very difficult time because of the mother's conduct" but that this impression was a façade as he has been "domineering, controlling and intrusive towards the mother and "actively undermined the mother and attempted to create a false reality for the child" with "the father engaging in a campaign to undermine and demean [the] mother to the child" with the effect that "his behaviour will destroy the mother-child relationship.[21]

The judge did not find the father to be a witness of credit and that he had made up evidence as the trial progressed. She noted that the CD of the recordings tendered by the father was found to represent random selections made by him from his recordings on his tape-recorder. He said he had destroyed the original tapes.

> [224] I am satisfied as is explained in more detail elsewhere in these reasons that the father has staged the recordings made by him, even to the point of taping himself having a one way conversation with the mother from a phone box and alleging that he was having a dialogue with the mother. [225] In summary, I find that the father's evidence is generally untruthful and otherwise implausible. He is a most unimpressive witness whose testimony cannot be relied on. Wherever his evidence contradicts that of the mother, or any other witness, in the absence of any independent evidence I prefer the evidence of the mother.

The mother was given sole parental responsibility. The father's application for relocation was dismissed

and described as "entirely ill-considered and impractical". Nonetheless he was granted alternate weekends with the child from Friday to Monday and half school holidays.

Lawyers should be extremely cautious when including evidence of parents directly questioning children — it is difficult to think of a circumstance when this will play well before a court, let alone represent sound or even "good enough" parenting.

Family violence — Janssen & Janssen

In the case *Janssen & Janssen*,[22] the mother sought to tender voice recordings and transcripts of exchanges between herself and the father and between the father and children.

These recordings were prima facie illegal under s 7 of the Surveillance Devices Act (NSW) unless caught by one of the exceptions.

On the first day of a 4-day trial, McClelland J delivered his ex tempore reasons for admitting the voice recordings secretly made by the mother prior to and following separation and the transcriptions of same. He also issued a certificate pursuant to s 128 of the Evidence Act to the mother protecting her from self-incrimination in respect of her affidavit setting out the context in which the recordings were made, which had been sworn at the request of the father's barrister.

His Honour considered that s 7 of the Surveillance Devices Act (NSW) prohibiting the recording of private conversations without the consent of the parties did not apply because the recordings by the mother were reasonably necessary for the protection of her lawful interests and fell within the exception.

He found the comments of Sexton J in *Corby* and Hannam J in *Huffman & Gorman* to be apposite to the facts of the case — that is, the mother "had the right to protect her interest not to be intimidated or harassed, and not to be forced to respond to the Father's demand for sexual activity".[23]

His Honour further found he would have exercised his discretion under s 138 to admit the evidence on the desirability test even if he considered it to be unlawfully obtained.

In doing so, his Honour noted that he had taken into consideration the caution of senior counsel for the father that there is a "danger of the 'floodgates' opening with parties to a marital relationship that are experiencing difficulties, determining that it is appropriate to [rely] on surreptitiously obtained tape recordings" as per [12]. Furthermore, his Honour continued:

> [13] In that context, my decision is very much one that is based on the facts before me, including the allegation that the father has maintained a charming public face but has engaged in conduct within the family home that is alleged to have constituted family violence… I have also had regard to the potential difficulty of obtaining evidence of alleged family violence when it occurs behind closed doors without any witnesses being present other than the alleged perpetrator and victim.
> [14] I also note that as a result of the competing contentions of the parties, regarding the issue as to whether family violence has occurred, that credibility will necessarily be an issue in these proceedings. The recordings and transcript will be directly relevant to that issue.
> [15] [The father also sought the exclusion of the actual transcripts referring] to section 135 of the Evidence Act which enables the Court to exercise its discretion to exclude evidence if its probative value is substantially outweighed by the danger of the evidence being unfairly prejudicial to a party.
> [16] [As to] unfair prejudice, senior counsel referred to the emotional impact on the Court and the possibility of the actual recordings unreasonably evoking sympathies against the father as a result of the tone in which the communication occurred. In addition, it was said that there was potential prejudice in that the conversations may have been triggered or induced by the mother such that the father said things in a tone which would not otherwise have been the case if the recordings were not being made.
> …
> [23] … I determine that the best available evidence [was found to be] not only what was said, as recorded in the transcripts, but also how it was said.

The tapes and the transcripts were both admitted.

The judge dealt with the father's complaint that the mother may have switched the microphone on and off or staged the recordings by triggering or inducing the father to react in a certain way in the manner as her Honour in *Huffman & Gorman* such that whether there was manipulation of the environment will be the subject of cross examination and may ground submissions as to the weight to be attached to the recorded conversations.

The outcome of the substantive trial, *Janssen & Janssen (No 2)*,[24] is a good example of where recordings were central to the findings and orders of the court.

McClelland J stated:

> This is an application by [the mother] for sole parental responsibility for the parties' three children and that they spend no time [with the father] …
> The mother's application is based on allegations of physical, verbal and emotional abuse perpetrated by the father against her and the children during the course of the marriage. The father concedes that he engaged in conduct that constitutes emotional and verbal abuse but denies that he is physically violent towards the mother or the children.
> At the commencement of the final hearing, I admitted into evidence audio recordings made by the mother, prior to separation of interactions between the parties and on occasion the father and children. Transcripts of those audio recordings were also admitted into evidence.
> The audio evidence is, in its content and tone, compelling in establishing that the father has engaged in family violence as defined in s 4AB of the Family Law Act 1975 (Cth) …

> Transcripts of audio recordings made by the mother post-separation during the father telephone contact with the children were also admitted into evidence.[25]

The father was 40 and the mother was 38 and were both described as professionals. The children were 8, 6 and 5. At separation and on leaving the former matrimonial home, the mother gave a statement to police about what was said to have happened the day before and the police obtained an AVO which included her and the children. The father was charged with assault and stalking offences of which he was later convicted.

By the time of trial, the father had re-partnered and had another baby.

The mother's case was that any time with the father would expose the children to the risk of psychological and physical harm and that she would decompensate if time were imposed; presenting a further unacceptable risk to them.

His Honour appended extracts from the transcripts as exhibits to the judgment.

As one of many examples, the mother had refused the father sex. He says:

> You're a selfish c**t. Even your dead father knows that.
> …
> Oh yeah and thanks in advance for ruining Father's Day for me in 2013. Okay? Thank you, you're a wonderful c**t.
> …
> I work hard like a dog, I come home and like a big ball-less c**t, I clean up the house and do all the female stuff for you and you give me nothing.[26]

The youngest child is then heard to say "Can we go now? … Mummy, I like you. I love you."[27]

The father then says: "When I kill myself it will not just be one reason but many reasons."[28] The mother alleged this threat occurred in the child's presence.

The judge found at [5] that the:

> … transcripts provided evidence of ongoing inappropriate conduct on the part of the father, including embroiling the children in issues being considered in these proceedings, denigrating the mother, creating false expectations of the children seeing the father and blaming the mother for the children being unable to spend time with the father.

The judge was satisfied the father had engaged in conduct both prior to and subsequent to separation which presented a risk of physical and psychological risk to the children and that they and the mother had been exposed to family violence during the relationship. He also held that the mother's fear and anxiety about the children seeing the father were genuinely held and reasonable.

Orders were made for the children to spend supervised time with the father on two occasions per year to "maintain recognition", and, other than that, the father was not to communicate with the children by any means.

Shelbourne v Shelbourne

In this matter[29] the wife was an American citizen with two children when she married the husband and moved to Australia where they had two children together.

Both parties alleged that the other had been physically and verbally abusive to them. The police obtained an AVO against the mother and she was convicted of an assault upon the father which he had recorded on video. The mother had been admitted to the local mental health unit on several occasions.

By the time of the hearing about interim parenting and other issues before Rees J, all four children were living with the father and the mother was having supervised time.

The mother's application was for orders including that the children live with her and that the father be restrained from recording or filming the mother.

The father sought to tender a number of videos he contended bore out his allegations of violent and threatening behaviour on the part of the mother.

Her Honour admitted the videos which had been made by the father on his mobile phone in circumstances where the mother knew he was recording and asked him to stop but kept speaking.

Rees J referred to the decision in *DW v J* (2014) 239 A Crim R 192; [2014] NSWCCA 28; BC201401527, where lawful interest for the purposes of the exception under the Surveillance Devices Act (NSW) was discussed by the court at [31]:

> In *R v Le* [2004] NSWCCA 82; 60 NSWLR 108; 146 A Crim R 179, Adams J (with whom RS Hulme J agreed, Giles JA dissenting on this issue) held (at [83]) that the desire of a witness to protect her credibility generally; to support her credibility if she had to give evidence in a court proceeding about the matter; and to protect herself against exposure to being charged with making false allegations against other people about matters of considerable seriousness, did constitute a "lawful interest" for the purpose of that phrase as used in the predecessor to s 7(3)(b)(i) of the Act (s 5(3)(b)(i) of the Listening Devices Act 1984).

Nor did Rees J consider that the evidence should be excluded under s 135 observing at [39] and [41] that:

> … evidence is not unfairly prejudicial merely because it tends to damage the case of the mother and support the case of the father.
> …
> There will always be a degree of unfairness to one party where there is no opportunity to cross-examine the other in relation to the evidence, but these are interim proceedings relating to the welfare of children and the evidence is relevant to serious allegations that bear on the welfare of the children. I consider that the importance of the evidence, in assisting in the determination of the proper parenting arrangements for the children, outweighs any potential prejudice to the mother arising from the inability to cross-examine at this stage of the proceedings.

She also found that the mother's complaints about the conversations being staged or the tape recordings reconstructed, did not go to the question of admissibility but only to the weight to be attached to the evidence once admitted.

The judge described some of the recordings, which for example "shows the mother, in the presence of some of the children, screaming at the father in foul language. The video lasts over ten minutes. The children are extremely distressed and crying."[30]

Another recording showed the mother berating the father through the car window and making threats to kill the baby, to find the highest thing and jump off, and saying that she doesn't want to be alive and will kill the baby and herself. Other recordings show the mother, at [56]–[57]:

> … holding one of the children screaming [while] the father repeatedly begs [her] to stop … The children are screaming hysterically and calling for their father. They appear terrified. The mother's screaming continues for a long time… The father attempts to leave and the mother prevents him from [doing so]. She is aware that she is being recorded but appears to be unable to stop and appears oblivious to the children's distress.
>
> Whilst I accept that the recordings, made by the father, are self-serving, it is notable that he remains calm throughout and the mother's behaviour is completely unrestrained, although she is clearly aware that she is being recorded. It is also notable that the children turn to their father for comfort and do not want to be left with their mother. The father is heard calming the children and telling the children "She loves you".

At [70]–[72]:

> Based on the recordings of the mother's behaviour, I have grave doubts about the mother's capacity to provide for the children's emotional needs when she is agitated. I am unable to say whether she can do so when she is calm…. The mother's repeated threats to kill herself and [the baby] must be taken seriously.

Her Honour accepted that the recordings did not show the complete version of each incident or the context in which they arose, including the father's own conduct. The judge was conscious that given the interlocutory nature of the proceedings, the evidence was untested and she was not in a position to determine the children's wishes, the other father's views, the children's relationships with each parent or the mother's capacity to regulate her behaviour generally.

Nonetheless, interim orders were made, predicated on the concerns raised by the videos, for all four children to continue to live with the father and for the mother's time to be professionally supervised.

Some cases from each jurisdiction

New South Wales

In the New South Wales case of *Farnham & Deluca*[31] the mother attempted to tender a video recording on a USB which she alleged demonstrated what took place during changeover. The mother claimed the recording was important evidence concerning the safety of the children when in the father's care. The mother admitted that the father had not been informed that she was recording.

The father objected to the video being admitted into evidence and alleged that the recording would not assist the court even if admitted. Le Poer Trench J viewed the recording but could not discern anything which would assist his Honour in forming a conclusion about the alleged incident. All Le Poer Trench J could hear was screaming and what the mother said.

The USB was not therefore admitted into evidence, and the relevant New South Wales legislation was not considered. The mother was granted sole parental responsibility of the children and it was ordered that they live with her and spend time with the father.

In *Parsons & Chou*,[32] a decision of the Family Court in New South Wales, an audio recording emerged as a critical piece of evidence. The Independent Children's Lawyer cross-examined the father about the recording, which allegedly contained disclosures of sexual abuse when in the care of the mother. The recording was of the father asking "highly suggestive and leading" (as described by Hannam J) questions of the child, who was only 3 years old at the time.

Hannam J concluded that the father's evidence regarding the recording was problematic, and that "an inference" could arise that the recording was made after the child did not previously disclose anything similar on earlier occasions.

As there was no other evidence on this issue, the court could not be satisfied there was an unacceptable risk of harm to the children in the mother's household.

The court did not consider the admissibility of the evidence. The recording was not referred to in the father's affidavit, but with leave the Independent Children's Lawyer cross-examined the father about it, and the recording was played in court twice.

Australian Capital Territory

In *Broughton and Broughton*,[33] the tendering of recordings that could have been made improperly under s 5 of the Listening Devices Act 1992 (ACT) was considered.

The husband appealed against the trial judge's decision to refuse to allow him to present evidence of recordings that he had made of conversations that had taken place between him and the children, and him and the wife.

The husband asserted that there were recordings of the mother abusing him, as well as recordings of the children identifying the emotional impact on them of the change of arrangements from equal shared care.

The trial judge refused to admit the recordings for two reasons. The main reason was that it was too late to adduce the material, as it should have been provided as part of the husband's case in chief, so that the wife could be cross examined. The appellate court did consider that the recordings were prima facie admissible, and their contents potentially relevant to the proceedings. However, the appellate court found that it would have been grossly unfair to have allowed its admission at such a late stage, considering ss 135 and 138 of the Evidence Act, noting that it was quite possible that the recordings were improperly made, pursuant to s 5 of the *Listening Devices Act*. The appellate court did not make a decision on the matter of illegality in the circumstances and dismissed the appeal.

Queensland

In *Ladley & Farwell*[34] during the final hearing in the Federal Circuit Court in Queensland the mother stated she had "numerous" video recordings on USBs which would assist the court, some of which related to events 17 years prior. The USBs had not been provided to the father or the Independent Children's Lawyer. Turner J ruled that the mother was restricted to recordings made since the child had been in an almost equal shared care arrangement by consent in 2014.

Only one video was therefore produced, which was a conversation between the child and the mother regarding her time with the father. This recording was admitted into evidence.

Turner J concluded, however, that no weight could be given to the single video recording made by the mother, as her Honour considered that it was obvious the mother was questioning the child inappropriately about adult issues.

Turner J's final orders were that the child was to live primarily with the father and that the father would have sole parental responsibility. In the interim, the child would spend supervised time with the mother.

A domestic violence case in Queensland, *WJ v AT*,[35] featured the extensive use of recordings as evidence. This was an appeal against the decision of the Magistrates Court to make a domestic violence protection order against the father in favour of the mother and their three children.

Several recordings were tendered into evidence. These recordings were found to portray the father being verbally and physically abusive to the mother and the children and supported the finding that the father had committed domestic violence. Smith J of the Queensland District Court favoured the version of events that was found to be more in line with the recordings. The protection order stood.

Northern Territory

In *R v Metcalfe*, the accused faced nine counts of assault, one count of make a threat to kill with intent to cause fear and other charges (including a charge under s 103A(1)(d) of the Criminal Code Act 1995 (Cth), of causing detriment to a person with the intention of inducing them not to act in a way that might influence the outcome of proceedings under the Domestic and Family Violence Act) relating to alleged conduct towards a former spouse.

Ruling solely on evidentiary issues, the court found that the recordings were not illegally or improperly obtained in contravention of Surveillance Devices Act 2007 (NT).

This was because the secret recordings were of conversations or incidents to which the complainant was a party at all material times and the publication of the conversations was allowed because the communication was necessary in the public interest and also for protecting the complainant's lawful interests.

Therefore, the exceptions were made out, the recordings were admitted into evidence and described as having high probative value.

In *Preston v Baker*,[36] recordings made by the father formed a crucial aspect of the father's evidence in proving the abuse he alleged the mother committed. The recordings captured verbal abuse, often taking place in front of the children. They also recorded the mother threatening and actually carrying out physical assaults against the father in front of the children. For example, the mother was heard to hit and kick the father and slam the door on him when he was buckling the children into the car.

Turner FM considered that this behaviour by the mother towards the father, which was supported by the audio recordings along with other evidence, would spill over into the mother's day to day care of and interaction with the children.

Turner FM found that the children were being exposed to psychological harm and family violence by the mother and that there was a significant risk this exposure would continue.

The admissibility of the audio recordings was not discussed.

Orders were made that the children leave the care of the mother and come to live with the father; with the mother to have supervised time until further order.

Victoria

Pettit and Fairs[37] is a case from Victoria which contained a "staggering" number of recordings and transcripts of recordings made by the father and stepmother, predominantly during conversations between

the father or stepmother and the children. The stepmother also recorded calls made by the children to Kids Helpline, in addition to recording conversations held between the Department of Health and Human Services and the children and stepmother. The recordings were made without the knowledge or consent of the children. The recordings were considered by the Independent Children's Lawyer as a "gross abuse" of the children's human rights.

Bender J found that the call to the Children's Helpline contravened the Surveillance Devices Act 1999 (Vic), and there was no proof as to its authenticity or the transcript's authenticity. The evidence was also not allowed under s 138 of the Evidence Act.

For the remainder of the recordings, Bender J did not explicitly find that the recordings were illegal, but they were not given much (if any) weight. The recordings undermined the privacy of the children and were not particularly probative in value.

The final decision was for the mother to have sole parental responsibility for the children, and for them to reside with her. The father and stepmother were not to have contact with the children other than the exchanging of cards, letters or gifts.

In *Glendale v Rubin*,[38] an audio recording was admitted into evidence without any examination as to its admissibility or reference to Victorian legislation. The audio recording, which was played in open court, was an important aspect of the evidence considered by Jones J. The recording was of an incident where the father entered the matrimonial home and attempted to talk to the children. This incident was of particular importance to the court when deciding whether family violence had occurred.

The audio recording, which was made and tendered by the father, showed behaviour by the father that was concerning to the court. Some of this behaviour, such as repeatedly denigrating the mother by referring to her "erratic, irrational behaviour and delusional behaviour", and asking her whether she was on medication, the court considered to be family violence. The father had produced the audio recording because he believed it would support his version of events, however Jones J concluded that it did not support his case. Instead, the audio recording disclosed behaviour by the father such as making inappropriate remarks to the children and refusing the mother's requests he leave.

The audio recording in this case helped support a finding of family violence against the father. The mother was awarded sole parental responsibility for the children, and the children were to live with her. The father was permitted only to communicate with the children by way of cards, gifts and letters on birthdays, Easter and Christmas.

Tasmania

In the older Tasmanian case of *Parker and Williams, In Marriage of*,[39] the wife taped a telephone conversation between the husband and their children, which she sought to adduce as evidence support of her application for interim custody of the children.

The wife had recorded the conversations between the husband and their children, who did not know that they were being recorded (although in two of the conversations they knew the wife was listening in). Butler J concluded that the recording of these conversations was in contravention of s 5 of the Listening Devices Act 1991 (Tas), and the recordings could not be relied upon.

South Australia

The decision of the Magistrates Court to admit into evidence an audio recording relating to domestic violence was appealed to the South Australian Supreme Court in *Groom v Police*.[40] The audio recording was surreptitiously made by the complainant in respect of an alleged contravention of an intervention order.

The mother and father were in a shared care arrangement and as part of that regime they would meet at designated locations for handovers. According to the intervention order between the two parties, the father was only permitted to have contact with the mother at the handovers about issues regarding the child. The mother made an audio recording of a discussion at a handover of the child where the father talked about appealing the intervention order. The mother gave evidence that:

> … most of the incidents between her and the [father] involved communications or meetings unwitnessed by anyone else, such that her subsequent complaints to police became a case of her word against his. She said that the police advised her to record future communications should the [father] commit any further breaches of the intervention order.[41]

This audio recording was used as the primary piece of evidence regarding the contravention of the intervention order. The Magistrate at first instance decided that the audio recording, and its transcript, should be admitted into evidence. The audio recording was found admissible notwithstanding s 4 of the Listening and Surveillance Devices Act 1972 (SA); an exception having been made out. His Honour found there was a lawful and legitimate interest in the mother recording the conversation without the appellant's knowledge, and recording the conversation was in the public interest.

It should be noted this case referred to South Australian legislation which has now been replaced.

Western Australia

In *Briggs & Kerr*,[42] a decision of the Family Court of Western Australia, the mother included in her affidavit a

transcript of a recording she made of a conversation between her and her son. She alleged that this transcript constituted a disclosure of sexual abuse by the father against the son. The mother sought that the father have only supervised time with the child.

The single expert in the case commented on the transcript, and the weight that should be given to it, stating "on reading the transcript … it is clear the mother asked leading questions, implies answers and coerces the child".[43]

The mother also provided a transcript of another recording made on a later date. The recording was also transcribed by a professional transcription service, and it was slightly different from the transcription given by the mother. The mother was criticised for these transcripts, by both the expert and Thackray CJ, as the recording showed a mother who was "far more interested in obtaining a recorded 'disclosure' than she was in attending to the needs of her child".[44]

The child was ordered to continue living with the mother but the father was granted unsupervised and overnight time.

Conclusion

The cases make it clear that recordings of private conversations in family law proceedings, if admitted on the tests outlined and avoiding the risks detailed where possible, can have a powerful effect on the outcome of matters; especially those involving parenting and family violence issues.

Justine Woods
Partner
Cooper Grace Ward
justine.woods@cgw.com.au
www.cgw.com.au

Footnotes

1. *Leos v Leos* [2017] FamCA 1038; BC201751239.
2. *Janssen & Janssen* (2016) 55 Fam LR 439; [2016] FamCA 345; BC201650370.
3. *Huffman v Gorman (No 2)* [2014] FamCA 1077; BC201451921.
4. Above, at [38].
5. Above n 3, at [39].
6. Above n 3, at [41].
7. Above n 3, at [43].
8. *Jasper v Corrigan (No 2)* [2017] FCCA 1467; BC201705419.
9. Above n 8, at [19]–[20], [23]–[24].
10. *Jasper v Corrigan (No 3)* [2017] FCCA 2272; BC201708928.
11. *Corby v Corby (No 2)* [2015] FCCA 3213; BC201511950.
12. Above, at [56].
13. Above 11, at [56].
14. *Corby v Corby* [2015] FCCA 1099; BC201503718.
15. Above.
16. *Leos v Leos* [2017] FamCA 1038; BC201751239.
17. *Masri and Masri* [2017] FamCA 539; BC201750601.
18. *Simmons v Simmons* [2013] FCCA 304; BC201309865.
19. Above, at [109].
20. *Farrelly v Kaling* [2012] FMCAfam 210; BC201204340.
21. Above, at Headnotes.
22. *Janssen & Janssen* (2016) 55 Fam LR 439; [2016] FamCA 345; BC201650370.
23. Above, at [6].
24. *Janssen & Janssen (No 2)* [2016] FamCA 796; BC201650851.
25. Above, at [1]–[5].
26. Above n 24, at [14].
27. Above n 24, at [15].
28. Above n 24, at [17].
29. *Shelbourne v Shelbourne* [2017] FamCA 761; BC201750822.
30. Above, at [51].
31. *Farnham and Deluca* [2018] FamCA 548; BC201850668.
32. *Parsons & Chou* [2016] FamCA 3; BC201650002.
33. *Broughton and Broughton* [2018] FamCAFC 96; BC201850415.
34. *Ladley & Farwell* [2017] FCCA 270; BC201701109.
35. *WJ v AT* [2016] QDC 211; BC201640295
36. *Preston v Baker* [2012] FMCAfam 308; BC201221030.
37. *Pettit and Fair* [2016] FCCA 2693; BC201609185.
38. *Glendale v Rubin* [2018] FCCA 1716; BC201805994.
39. *Parker & Williams, In the Marriage of* (1993) 117 FLR 1; (1993) FLC 92-394.
40. *Groom v Police* (2015) 252 A Crim R 332; [2015] SASC 101; BC201506391.
41. Above, at [17].
42. *Briggs & Kerr* [2015] FCWA 54.
43. Above, at [146].
44. Above n 43, at [185].

Pointing the finger at privacy law: Fair Work Commission's new take on when a direction is lawful and reasonable

***Andrea Beatty**, **Tim Lange** and **Chelsea Payne** PIPER ALDERMAN*

Can an employer dismiss you for not providing them your fingerprint biometric data?

The recent Fair Work Commission (FWC) decision of *Jeremy Lee v Superior Wood Pty Ltd*[1] (*Superior Wood*) provides interesting insights on the extent to which an employer can request your biometric data.

This case gives insight on whether the collection of a fingerprint scan of an employee as part of a new attendance recording system is a practice that is exempted from the reach of the Privacy Act 1988 (Cth) (Privacy Act) under it's "employee records" exemption.

If it is an exempt practice, the Privacy Act would not be a barrier to employees being directed to comply with the new attendance system. However, if it is not exempt, a fingerprint will be the type of sensitive biometric information which has a high level of protection, and cannot be collected without the permission of the person concerned (unless an exemption applies). That protection prevents an employer from enforcing a management direction to comply with the collection of sensitive information.

Fingerprint-based attendance systems are relatively uncommon and generally unnecessary when alternatives based on radio-frequency (RFID)-chip or smartphone geo-fencing are available. However, "sensitive information" goes well beyond mere biometric information. The principle established in the *Superior Wood* case will apply equally to other employee sensitive information commonly required by an employer for ordinary and legitimate management purposes, and (until now) thought to be entirely outside the Privacy Act's regulation of information collection.

Background

Jeremy Lee was employed as a general hand at one of Superior Wood's sawmills in Queensland for approximately three and one-fourth years, before he was dismissed on 12 February 2019 for failing to comply with Superior Wood's Site Attendance Policy. The Site Attendance Policy required employees to use newly introduced fingerprint scanners to sign on and off the work site.

Mr Lee refused to provide his fingerprint for the purposes of signing on and off the worksite. His concerns were about the control of his biometric data and the inability of Superior Wood to guarantee no third party would be provided access or use of the data once stored electronically.

After a number of discussions with Superior Wood and the scanner's supplier, Mitrefinch, Mr Lee was provided with a verbal warning for refusing to use the scanner. Two written warnings were subsequently issued in the following weeks advising Mr Lee that failure to follow the Policy would result in termination of employment.

Following further discussions, a show cause letter was issued on 6 February 2018 and Mr Lee's employment was officially terminated on 12 February 2018, for his failure to follow the management directions contained in the Policy.

Mr Lee challenged the termination in an unfair dismissal claim in the FWC, which had to consider whether the failure to follow the direction to comply with the Policy was a valid reason for termination. The FWC in its initial decision determined that Superior Wood was not exempt from complying with Australian Privacy Principle (APP) 3.3 under the employee records exemption in s 7B(3) of the Privacy Act, but that the direction was nonetheless reasonable and his failure to comply with it formed a valid reason for termination.

Questions to be considered

The questions to be considered by the FWC initially were:

- Did Mr Lee's refusal to use the fingerprint scanners amount to failing to comply with a reasonable and lawful direction?
- Was there a valid reason for Mr Lee's dismissal?
- Was the dismissal harsh, unjust or unreasonable, and therefore unfair under the Fair Work Act 2009 (Cth) (Fair Work Act)?

Fair Work Commission initial decision

In the initial decision of the FWC, the Commissioner found that the Site Attendance Policy was not unjust or unreasonable because:[2]

- it improved safety in the event of an emergency by avoiding having to locate a physical copy of attendance
- the scanners improved the integrity and efficiency of the payroll
- Superior Wood had the right to require employees to comply with the Policy, and refusal to comply after adequate caution would not render any dismissal invalid.

The Commissioner also found that although biometric data is "sensitive information" for the purposes of the Privacy Act, it was reasonably necessary to collect the information for one or more of Superior Wood's functions or activities under APP 3.3.[3]

Superior Wood was not exempt from complying with APP 3.3 by reason of the employee records exemption in s 7B(3) of the Privacy Act. The Commissioner found that the need to consolidate payroll across a group of organisations and the number of employees to be covered by the new method of signing, meant that allowing Mr Lee to use an alternative method to sign would be inefficient, inequitable and a burden.[4]

Superior Wood was not entitled to collect Mr Lee's sensitive information without his consent,[5] something that Mr Lee did not provide either expressly or impliedly. Although the FWC raised the issue of a potential breach of the Privacy Act in obtaining consent, it left the determination of this issue to the Australian Information Commission and the Privacy Commissioner.[6] The FWC also criticised Superior Wood for failing to have a privacy policy in place and failing to provide employees with a collections notice at the time of the event.[7]

Amongst other findings, the Commissioner found that although Mr Lee was entitled to withhold consent, in doing so he failed to meet a reasonable request of his employer and consequently Superior Wood had a valid reason for dismissal.[8] Interestingly, the Commissioner noted that Mr Lee's position in relation to the use of his biometric data contradicted his position regarding other biometric data and his DNA, in connection with his agreement to participate in drug and alcohol testing.[9]

Grounds of Appeal — FWC Full Bench

Mr Lee raised nine grounds of appeal in relation to the initial FWC decision.[10] For the purposes of this article, we will discuss those grounds which are relevant to the Privacy Act.

- The finding that failure to comply with the Policy was a valid reason for dismissal, given potential breaches of the Privacy Act and despite the finding that Mr Lee was entitled to refuse to provide his biometric data.
- The finding that there was no breach of the Privacy Act with respect to the collection of information from Mr Lee, because his data was never collected.[11]

Full Bench Decision

In the appeal, the FWC Full Bench:

- confirmed that Mr Lee had not (under his contract) given general consent to comply with new management directions in a later-introduced policy (after his employment had commenced)
- confirmed the view that the employee records exemption applies only to records after they have been created, and could not exempt a practice in collection of information from the Privacy Act's reach
- confirmed that as the employee records exemption had no application, the biometric data in a fingerprint was sensitive information for which an employee's consent to collection must be obtained
- said that consent could not be coerced by a management direction to comply with a collection practice under threat of disciplinary action, and
- considered that no exemption from the requirement to obtain consent applied

Contractual requirement to comply with the Policy

The FWC Full Bench found that a strict reading of Mr Lee's employment contract could be read to suggest that Mr Lee was only bound by any policies, procedures and work rules in place *at the time of entry* into the contract.[12] As the policy in question came into existence following Mr Lee's employment and there was no variation to the contract, the FWC Full Bench was not satisfied that compliance with the Policy was a term of Mr Lee's employment.[13] Consequently, Mr Lee's obligation to comply with the Policy was dependent on whether the direction to comply was reasonable and lawful.[14]

Australian Privacy Principle 3

APP 3 outlines when a regulated entity may collect solicited personal information. The FWC's interpretation of APP 3 was that it applies both to solicitation and collection of personal information and therefore operates at a time before the information is collected.[15] Consequently, any collection of personal information that occurs without first having obtained consent to that

collection would be in breach of APP 3.[16] Although it was found that Superior Wood did not breach APP 3 in actually collecting Mr Lee's information, the direction to collect the information was directly inconsistent with APP 3.[17] Mr Lee was entitled to refuse to provide his biometric data to Superior Wood.[18]

Employee records exemption

Section 7B(3) of the Privacy Act contains an exemption from an APP-regulated employer's requirement to comply with the APPs in regards to an employee record held by the organisation and relating to the individual directly related to a current or former employment relationship.

The FWC did not agree that the fingerprint scanners fell under the employee records exemption, as it was inconsistent with the plain words of the statute, which are in the present tense and refer to a record in the possession or control of the organisation.[19] The FWC stated that a record is not held if it has not yet been created or is not yet in the possession or control of the organisation.[20] Consequently, the exemption will not apply to a thing that doesn't exist or to the creation of future records.[21]

As the employee records exemption does not apply in these circumstances, the APPs applied to Superior Wood in connection with the solicitation and collection of sensitive information, up until the point of having possession of the information. Once collected, the employee records exemption will apply and the Privacy Act will no longer regulate the information's use or disclosure.[22]

This is an interesting interpretation of the Privacy Act, as it essentially means that employers are required to adhere to the APPs in the collection of personal information but are then able to use this information in an unregulated manner once they have possession of the information under the employee records exemption.

Was the direction lawful?

The FWC found that the direction given to Mr Lee and other employees was not lawful. Any consent Mr Lee may have provided once he was informed that he may be disciplined or dismissed for failing to provide consent would likely not be considered genuine consent.[23]

Although it was not necessary to determine whether the direction was reasonable, the FWC stated that the direction was not reasonable, finding:

> A necessary counterpart to a right to consent to a thing is a right to refuse it. A direction to a person to give consent does not vest in that person a meaningful right at all.[24]

Decision — FWC Full Bench

The FWC Full Bench decided to uphold the appeal and quash the decision,[25] which in turn required a rehearing of the decision. In determining whether there was a valid reason for the dismissal, the FWC Full Bench was then required to weigh up the factors listed in s 387 of the Fair Work Act.

In the rehearing, the FWC Full Bench found the fact that there was no valid reason for the dismissal was a significant factor in the circumstances of the case.[26] Although Superior Wood followed the rules of procedural fairness, the weight given to this was not sufficient to outweigh the significance of an absence of valid reason.[27] Accordingly, the dismissal was unjust because Mr Lee was not guilty of the alleged conduct.[28] As the direction Mr Lee was provided was unlawful, he was entitled to refuse to follow it.[29]

Implications

It has been a long-held view of courts and employment tribunals that there are genuine operational reasons which can justify an employer requiring employees to provide personal information, even quite sensitive information. In a situation of that kind, an employee can be directed to provide the information and be subject to disciplinary action if they do not comply.

Situations of that kind will include:

- where an ongoing illness or injury potentially affects the employees' capacity to safely work or to carry out the inherent requirements of their employment
- where an incident of workplace harassment includes allegations of unlawful discriminatory conduct involving opinions about an employee's sexual orientation, political affiliations or religious beliefs, and the employer is conducting a workplace investigation

There is no general exemption (in APP 3.4) reflecting these operational employment reasons from the requirement that collection of sensitive information of this kind must be consented to by the employee — the exceptions that do allow collection of sensitive information without consent are more limited.

There are also cases which demonstrate that without adequate medical evidence of incapacity to carry out the inherent requirements of their employment, an employer will not have positively established it had grounds to terminate for capacity reasons (*CSL Ltd (t/as CSL Behring) v Papaioannou*[30]), and that employers are required to take action to protect employees from risks, including psychological risks of bullying and harassment.

Although this is an employment law case, the decision also provides helpful guidance to all APP-regulated entities on the interpretation of the APPs and the

obligations that regulated entities are required to adhere to. This case is also an important reminder to ensure your business has a sufficient privacy policy in place, and that your business is aware of its obligations under the Privacy Act, including the APPs.

In particular, in a group of companies, be aware that the employee records exemption applies only to the actual employer of an employee. If records are created or held by another group company, the employee records exemption will not apply.

Summary

The Fair Work Commission has upended the accepted understanding of the remarked-upon "employee records" exemption in the Privacy Act and in the process, potentially severely impacted the capacity of employers to manage issues of medical capacity and unlawful discrimination in the workplace.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au

Tim Lange
Partner
Piper Alderman
tlange@piperalderman.com.au
www.piperalderman.com.au

Chelsea Payne
Lawyer
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946.
2. Above, at [13].
3. Above n 1, at [14].
4. Above.
5. Above.
6. Above.
7. Above.
8. Above n 1, at [15].
9. Above n 1, at [16].
10. Above n 1, at [18].
11. Above.
12. Above n 1, at [23].
13. Above n 1, at [24].
14. Above n 1, at [25].
15. Above n 1, at [47].
16. Above.
17. Above n 1, at [48].
18. Above.
19. Above n 1, at [53].
20. Above n 1, at [56].
21. Above.
22. Above n 1, at [57].
23. Above n 1, at [58].
24. Above.
25. Above n 1, at [90].
26. Above n 1, at [102].
27. Above.
28. Above.
29. Above.
30. *CSL Ltd (t/as CSL Behring) v Papaioannou* (2018) 273 IR 168; [2018] FWCFB 1005; BC201807436.

Privacy Law
Bulletin

Thinking harder about data "ownership" and regulation of data driven business

Peter Leonard *DATA SYNERGIES and UNSW BUSINESS SCHOOL, SYDNEY*

Key takeaways

- Misuse and abuses of data about citizens and consumers clearly must be subject to sanctions which operate as effective disincentives to misconduct by data controllers. But there is not always a close correlation between size of data holdings and potential to cause harm to data subjects. We need to think carefully about how to best address concerns about "big data" and market power of global data platforms, and make sure that regulator responses are reasonable and proportionate.
- There are now frequent calls for regulation of data driven businesses. Regulators are examining their toolboxes and calling for new powers and penalties. Already available tools include enforcement of data protection, consumer protection and competition (antitrust) laws, the new "consumer data right", and facilitation of enforcement by individuals of rights of access to, or portability of, transactional data (whether or not personal information about them) as held by data custodians.
- Protection of consumers, of individual's rights of privacy, and of fair competition between entities that operate in a shared data ecosystem over a data platform controlled by one of the parties, are tightly intertwined. Rebalancing of rights and responsibilities of participants in this ecosystem — affected individuals, other consumers, platform operators and entities that willingly or not contribute relevant data through use of the platform — can have profound implications. Proposals for changes in regulatory settings require careful analysis.
- Concerns as to so-called "data rich" businesses sometimes fail to distinguish between the quantity and range of data sets that a business holds, and the capabilities (or lack thereof) of a business to transform those data sets into actionable insights or other sustainable business advantage. Protection of consumers, of individual's rights of privacy, and of fair competition between entities that operate in a shared data ecosystem over a data platform controlled by one of the parties, are tightly intertwined. We need to be careful that regulation of data uses and data sharing does not have the counter — intuitive outcome of nurturing a few "dataopolies".

Introduction

Much of today's discussion as to reasons to regulate big data is misguided. Misuse and abuses of data about citizens and consumers clearly must be subject to sanctions which operate as effective disincentives to misconduct by data controllers. But there is not always a close correlation between size of data holdings and potential to cause harm to data subjects. Common errors in correlation include: over-estimation of value of raw data, as distinct from value in ability and capability to link diverse data sets and thereby derive actionable insights; generalisation of conclusions about data capabilities of global consumer data platforms to include other large data driven businesses and shared data eco-systems; and over-concentration upon current tools of competition policy, rather than exploring the possibilities for using a variety of incentives and regulator tools to effect context specific rebalancing of data rights.

Raw data has little inherent value. Big qualities of data are often less valuable than small quantities of the right diversity of transformed and correlated data sets. Data value is derived not by what data is, but by the ability of an entity:

- to create value using that data as an input
- to then endurably capture that value (not by ownership, but by practical control — that is, by denying others the ability to do those things), and
- to do these things in a way which does not excite regulatory intervention that may strip that value

Exclusivity of an entity's practical control of data can be qualified through regulatory action in a variety of ways. Possible value depleting regulatory interventions include:

- enforcement of data protection, consumer protection and competition (antitrust) laws
- addressing information asymmetries through new requirements as to transparency

- creating new "consumer rights" over data, and
- facilitating enforcement by individuals of rights of access to, or portability of, transactional data (whether or not personal information about them) as held by data custodians

Sometimes data derives value not through direct application of that data, but through enabling testing and development of code for application on other data. So-called artificial intelligence (AI) didn't beat grand masters in chess and Go by being intelligent, but through learning by 24x7x365 playing of games, generating "training data" to inform machine learning (ML). In AI and ML applications, data may thereby enable code that enables analysis of other data, making that other data more valuable. And often a large volume of data of uneven quality can yield algorithms of substantial value, which may then make poor data or narrow data sets more valuable. In short, data (through the intermediary of code) can be transformative in value of other data.

Creating value in data

Valuation of so-called "data rich" businesses is sometimes confused by failure to distinguish between the quantity and range of data sets that a business holds, and the capabilities (or lack thereof) of a business to transform those data sets into actionable insights or other sustainable business advantage. Transformational methods and code and algorithms are often fungible across business sectors, with the result that data rich businesses concentrated within particular industry sectors may not achieve economies of scope of data analysis that are available to cross-sector service providers. Scarcity of human capital, and in particular experienced data scientists, means that much data that is captured today is not transformed and never achieves its potential value. Human capital remains the key investment in cleansing, transforming and linking data, in discovering useful correlations, and in creating and applying algorithms to data sets to derive actionable insights. Technology enables, but humans (still) create. And humans are ambitious, fickle and moveable. Quality people culture will continue to be a key differentiator of good data driven businesses.

To put it another way: the analogy commonly drawn between "control of data" and "ownership of oil" undervalues the value-adding contribution of the processes required to "refine" data and create algorithms and code to power actionable insights for businesses. Good insights as outputs require great labour to create quality data inputs and to derive robust algorithms that are used as the engines of transformation. Which is one reason why many of the more ambitious predictions as to roll-out of applications of artificial intelligence have proven incorrect.

Valuable business insights are often deployed in disrupted product or service sectors that are characterised by increasingly short product lifecycles, where returns on investment are highly uncertain. Markets for outputs of data are volatile and unpredictable. Refined (real) oil can be stockpiled: much data is time sensitive and rapidly loses value. Actionable insights often have narrow application, a short shelf-life and require continuing innovation and reapplication. Oil is fungible across many industrial, transport and heating applications, and the movement from fossil fuels to alternative energy is still agonisingly slow. Oil markets may appear to be volatile, but the markets for outputs of data analysis are often substantially more unpredictable.

Further, you can own oil, but (generally) you can't own data. The closest simulation of "real" legal ownership of data that is available to a data controller is to ensure that "the service provider's data" (which the provider does not "own" as "property") remains defensibly protectable as legally trade secret and confidential information. But increasingly, data sets must be shared to some degree to yield value. Data sharing within multi-party data ecosystems is required to deliver almost all online services, particularly internet of things (IoT) applications, and also many offline supplied products and services. Many IoT services, and online platforms such as Amazon and Alibaba, require a complex supply-side data sharing eco-system of five or more data holding entities to enable delivery of a service to an end-user and billing for that service. A business to consumer IoT service may include a retail service provider, a data analytics service provider, a cloud data platform, a telecommunications network services provider, a billing services provider, a mobile app provider and an IoT device provider, all sharing data in a world today without settled industry standards as to data minimisation and data security. In other words, at least some sharing of data is required to deliver many services, while at the same time the service provider seeks to protect data value through imposition of safeguards and controls to ensure that "the service provider's data" (which it does not "own" as "property") remains defensibly trade secret and confidential. This is a difficult balancing act.

How should uses and applications of data be regulated?

To consider whether particular uses and applications of data needs to be regulated, we need to develop a more nuanced understanding of data and good data governance.

Data can be infinitely reproduced and shared at effectively zero replication and sharing cost. Data does not derive its value through scarcity. Value in data is usually created through investment in "discoverability" in collecting and transforming raw data to enhance capability to link data to other data and then explore the linked data sets for correlations and insights. Often in data analytics projects about 70–80% of the cost is cleansing and transforming raw data to make it discoverable — the high-end work of then analysing the transformed data is the smaller part of a program budget.

Discoverability may be created within a privacy protected data analytics environment. In many cases, substantial data value can be created and commercialised without particular individuals being or becoming identifiable. Through deployment of appropriate controls and safeguards, analysis of personal data need not be privacy invasive. Of course, it is easier to link disparate data sets by using personal identifiers than it is to deploy a properly isolated and safeguarded data analytics environment that uses only pseudonymised data linkage transactor keys. It is also easier to release outputs and insights without taking reliable steps to ensure that the outputs cannot be used to re-identify affected individuals. Good privacy management is exacting. The frameworks, tools and methodologies for good data governance are immature and therefore not well understood. And good data handling does not create good outputs. Senior management of businesses and government agencies often do not know how to evaluate data scientists and their outputs. The term "data science" carries, as the term management science once did, the enticing ring of exactitude. However, algorithms may be painstakingly derived and applied, but based on poor data, or simply misapplied in particular contexts. Often poor data practices are implemented through inadvertence, or as a result of cutting corners, rather than bad intent.

Most importantly, we need to recognise that most data about what humans think or do is generated through transactions involving those humans in circumstances where humans no longer understand or control the data exhaust associated with those transactions. Most data is inherently transactional, but gathered from or about transactions in circumstances where many individuals that are transactors do not fully understand the transactional data — and sometimes, that there has been a transaction at all. In any event, relevant transactions are between transaction parties and accordingly, there is a bundle of rights and responsibilities attaching to the respective transactors that can be reallocated or repackaged by regulatory intervention. Where citizens and consumers are unwilling or unknowing transactors, there is particular vulnerability to data uses that may be adverse to their interests. A simple example: I don't choose to be observed by my very smart rental car, but I am. When I drive it out of the parking slot, I don't reach for the vehicle manual to school up on the car's data analytics capabilities. Often, I have no real opportunity to think about whether or not they should give consent. Even when I am informed about particular data collections, life is too short for me to read and evaluate the terms: I do not knowingly and reflectively give consent to particular uses.

Protecting the rights of participants in multi-party data ecosystems

Should recalcitrant consumers (such as me) who don't read all terms proffered to us be punished for our failure to engage with the torrent of privacy disclosures by organisations with whom we deal?

I don't need more notice or more click-through consents.

I don't expect, or need, regulators to force more responsibility on me.

But even if I don't care about privacy, I might wish to join ranks with many millennials and demand to know who is doing what, with what data about me. Many millennials do not care about privacy or transparency by right, but sense that value is being derived from data about them, that free services are great but no-cost may be less than fair value, and that they aren't given enough information to force a meaningful negotiation over fair allocation of data value.

Many businesses are frightened to initiate a discussion as to what is fair to consumers, because they can't control that discussion, or they simply don't want to give away value. Some early mover data platform businesses captured the data high ground and since then have engaged in tactical retreats, giving away certain data value if and when required to mitigate particular crisis in digital trust of consumers. Many other data driven organisations, such as some insurers and banks, are more willing to sacrifice short term data value in order to preserve longer term certainty and therefore sustainability for data value-adding investments. However, they fear that initiating a discussion with customers as to fair data exchange can lead to unpredictable and uncontrollable outcomes. And explanations of many data applications and data value chains are devilishly tricky. Explanations often sound self-serving, or just plain spooky. Try explaining to sceptical citizens and consumer advocates how real time programmatic advertising does not require any disclosure of the identify of ad recipients, or explaining how audience segmentation

value is allocated at points in the advertising and media supply chain. And most data applications have unique, but similarly complex, multi-party supply and fulfilment value chains.

Leaving aside the desire for demand-side transparency to reduce information asymmetry and to enable negotiation as to data value exchange, why should a consumer need to engage with a data collector as to whether a particular collection of data is a fair exchange for benefits that the data collector provides to the data subject, proportionate and reasonable? More transparency may help a consumer advocate or regulator to make relevant assessments, but regulators should not be forcing transparency on the pretext that citizens should then determine whether to change their behaviour. Regulators don't require consumers to take responsibility for determining whether a consumer product is fit for purpose and safe when used for the product's stated purpose, and unsuitable or unsafe when used for other purposes. Why should data driven services be any different? In any event, usually I don't even know when an algorithm is being used in a way that may affect how an entity deals with me, particularly where the algorithm is fuelled by data which is not personally identifying (and therefore largely unregulated by most existing data privacy laws). I don't want transparency and then responsibility for me to exercise a decision based upon evaluation of that transparency. Instead, I want accountability of the data controller, to ensure that the data controller responsibly and reliably does what is fair and reasonable. And this may lead to a need to restrict data flows within a multi-entity data ecosystem, or require opening up of data ecosystems to new data intermediaries. Of course, "fairness" is a notoriously normative concept, which is why competition law seeks exactitude of economic theory in evaluating effects on consumer welfare. Beneficence for most consumer means less than "fair" treatment of a few, at least as those few perceive treatment by others of them. It all turns on the particular context.

Heading here?

Critics of data driven businesses often rightly say that too many data businesses are not self-reflective about balancing their own and societal interests — many businesses don't stop to ask — just because I can use data in a particular way, should I? There is a risk that regulators will fall to a similar temptation when considering regulation of business uses of data. Big data holdings of global data corporations look like clear candidates for competition regulation. Data driven businesses can't assert legal protection against deprivation of "their property" in data, because the bundle of rights and responsibilities of a data controller are not property in data. Rebalancing is unusually enabled because most data is not legally "owned", as "ownership" is conventionally analysed in most jurisdictions. Legally recognised "property" may be tangible (chairs, dogs and pencils) or intangible (software, creative writing, trade marks and patents). Data is none of these things — I don't own personal data about what I think or do, and often I don't even know when it is collected or used. Often a large component of intangible value is trade secret, or as we usually call it in Australia, confidential information. Trade secrets are not "property" in most national legal systems and in most (if not all) national variants of generally accepted accounting principles. Rights of protection of trade secrets more readily yield to regulatory interventions.

Of course, the market capitalisation of both "unicorns" and "data giants" demonstrates that public share markets and venture capitalists see value outside traditional classes of property. A single trade secret "asset" can be worth millions, or billions, of dollars. Google emerged out of nowhere to dominate the search engine world by use of Google's trade secret algorithms. Google's success today depends upon protecting the trade secret assets collectively described as the Google brand. Many trade secrets derive their value through closely guarded central control — the recipe for Coke, the Google search ranking algorithms, and so on. These trade secret 'assets' may not appear in the balance sheet as assets, but derive value through being closely held, and through being so managed scarcity is created.

Conclusion

Regulators have a broad range of available regulatory tools that may be used to affect activities of data driven businesses. Available tools include enforcement of data protection, consumer protection and competition (antitrust) laws, the new "consumer data right", and facilitation of enforcement by individuals of rights of access to, or portability of, transactional data (whether or not personal information about them) as held by data custodians. These tools should be selectively and surgically used to address particular contexts of data use by businesses that warrant regulatory intervention. But protection of consumers, of individual's rights of privacy, and of fair competition between entities that operate in a shared data ecosystem over a data platform controlled by one of the parties, are tightly intertwined. Rebalancing of rights and responsibilities of participants in this ecosystem — affected individuals, other consumers, platform operators and entities that willingly or not contribute relevant data through use of the platform — can have profound implications. There is clearly a role,

and a need, for good regulation. But context is critical in dynamic markets. Outcomes of regulatory interventions may be unpredictable and unintended. It is hard to be a good regulator.

Peter Leonard
Principal, Data Synergies
Professor of Practice, IT Systems and Management and Business Law, UNSW Business School, Sydney

It is better to be safe than sorry — the importance of regular privacy health checks

Monique Azzopardi *and* ***Mathew Baldwin*** *CLAYTON UTZ*

As public awareness and concern about privacy grows, conducting privacy health checks and implementing appropriate privacy management practices are increasingly important in helping an entity to meet its obligations at law and to build and sustain public trust. This is particularly important in a climate where data breaches involving personal information are increasingly being reported in the media and pose a significant privacy risk.

In Australia, privacy breaches have come to the forefront, in part, due to the operation of the Commonwealth's Notifiable Data Breach (NDB) scheme. A recent report from the Office of the Australian Information Commissioner[1] (OAIC) highlights the frequency of data breaches across certain sectors in Australia. The OAIC reported that 1,132 notifications of data breaches were made to it between 1 April 2018 and 31 March 2019.[2] This is likely to be just the tip of the iceberg, as many entities in Australia are not subject to the NDB scheme.

All entities handling personal information should take responsible steps to prevent data breaches, both to comply with their obligations under relevant privacy laws and as a matter of ensuring they maintain public trust and confidence in their operations.

Privacy health checks are one measure that enable entities to manage personal information responsibly and to determine any privacy gaps. This allows them to take the necessary steps to prevent and mitigate privacy and data breaches, including those notifiable under the Privacy Act 1988 (Cth) (Privacy Act), other relevant legislation, private agreements, and any applicable foreign laws, such as the EU General Data Protection Regulation (GDPR).

Privacy health checks have two additional benefits:

- First, they foster awareness and understanding of privacy issues within an entity's business or organisation which assists with privacy compliance generally.
- Second, they demonstrate to the public that an entity takes privacy seriously.

Types of privacy health checks

There are two main forms of privacy health checks: privacy audits and privacy impact assessments (PIAs).

A privacy audit is an audit of the way data is collected, held and processed within an organisation to assess the extent to which an entity is complying with its legal obligations (including under privacy laws). A privacy audit should be comprehensive enough to capture all the data flows within an organisation and any disclosure or transfer of personal information to third parties, such as suppliers. Typically, a privacy audit will involve core units within an organisation reporting on the personal information that they collect, process or deal with. These core units may include human resources, marketing, IT and/or customer service departments. The audit should be targeted towards the operations of the organisation or the specific unit and will typically be framed around the relevant privacy principles or requirements that apply.

A privacy audit should be undertaken on a periodic basis and as necessary to respond to privacy risks as they may arise and evolve over time. The frequency of privacy audits will depend on several factors, including an organisation's size and whether there have been any changes in personal information flows within the organisation since the previous privacy audit.

A PIA is more proactive. A PIA is typically undertaken as part of designing and developing a new activity, function, system, project or programme (Project) to assess the potential impact of the Project on the privacy of individuals and compliance with privacy laws. For example, if an entity holding customer records was moving from paper-based file management to an electronic file management system (or from one electronic system to another), it would be prudent to undertake a PIA. PIAs are especially relevant if an entity is utilising third party information and communication technology products and services to provide a new system. Follow-up PIAs are often undertaken when there has been a significant change in a Project that has the potential to impact on the original recommendations.

A PIA during the conceptual stages of a Project helps to build privacy into the Project at the outset (privacy by design), rather than trying to retrofit a Project for privacy compliance after the Project has significantly progressed or been completed.[3] However, a PIA should not be done so early that there is insufficient information to properly assess applicable privacy impacts and risks.

PIAs will only be required where a Project has a potential privacy impact, for example, if it will collect, use or disclose personal information. The OAIC's Guide to undertaking privacy impact assessments states that: "The greater the project's complexity and privacy scope, the more likely it is that a comprehensive PIA will be required, to determine and manage its privacy impacts."[4] In addition to addressing privacy impacts and risks, a PIA will usually set out recommendations for managing and mitigating such privacy impacts and risks.

The recommendations of a PIA should aim to identify any further action that can reasonably be taken to address privacy risks, such as building further security into the development of the Project or agreements, or preparing a privacy management or data breach plan. In some cases, the privacy risks that a PIA uncovers may be so significant that a Project may need to be redesigned or its implementation altered.

PIAs can also be mandated by certain legislation. For example, under the Privacy Act entities can be directed to undertake PIAs by the Australian Information Commissioner where the Commissioner considers that an activity or function might have a significant impact on the privacy of individuals.[5] There are also obligations under the Australian Government Agencies Privacy Code to conduct a PIA for all "high privacy risk" projects. As discussed further below, under the GDPR a similar Data Protection Impact Assessment (DPIA) must be undertaken where the processing of personal data is "likely to result in a high risk" to the rights and freedoms of individuals.[6]

Privacy health checks (both privacy audits and PIAs) are also an example of data protection by design and default, which assists entities to comply with their obligations for establishing privacy management processes within their operations. For example, Australian Privacy Principle (APP) 1 under the Privacy Act requires that entities take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities to ensure that the entity complies with the APPs and that enable them to deal with enquiries or complaints about privacy compliance.

Similar obligations exist internationally. The GDPR requires that data controllers implement appropriate technical and organisational measures to ensure that the requirements of the GDPR are met,[7] including adopting internal policies and measures which meet the principles of data protection by design and default.[8]

Data Protection Impact Assessments under the GDPR

Due to the broad extra-territorial reach of the GDPR, many Australian organisations that are controllers and processors of personal data may be subject to the GDPR. This will be the case if they:

- have an establishment in the EU and process personal data in the context of the activities of the establishment (Art 3(1))
- offer goods or services to individuals in the EU (Art 3(2)(a)), or
- monitor the behaviour of individuals in the EU (Art 3(2)(b))

Even for those entities that are not subject to the GDPR, increasingly, the standards for data protection under the GDPR are becoming recognised as international best practice.

The GDPR includes a requirement to conduct a DPIA prior to processing personal data where the processing "is likely to result in a high risk to the rights and freedoms of natural persons" (Art 35(1)). A DPIA is similar to the Australian concept of a PIA.

The former European advisory body on data protection and privacy, the Article 29 Data Protection Working Party, provided some guidance on when a processing operation may be "likely to result in a high risk".[9] Its Guidelines on DPIAs highlighted the following nine criteria for evaluating the likelihood that the relevant processing of personal data will result in a high risk to the rights and freedoms of natural persons:[10]

1) evaluation or scoring of data subjects, including profiling and predicting (for example, in the context of a financial company screening its customers against a credit reference database)
2) automated decision-making which may have legal impacts on data subjects
3) systematic monitoring, including data collected through monitoring of publicly assessable areas
4) highly personal or sensitive data (such as health information)
5) data processed on a large scale
6) matching or combining datasets (for example, combining or matching datasets originating from two or more data processing operations performed for different purposes or by different data controllers in a way that exceeds the data subject's reasonable expectations)
7) data concerning vulnerable data subjects, such as children, the elderly or those persons who face a power imbalance with the data controller
8) the utilisation of innovative or new technologies, which can allow for more novel forms of data processing (for example, combining the use of finger print and face recognition to establish security controls within a particular environment or system), and/or

9) where the processing in itself may prevent subjects from exercising a right or using a service or a contract (for example, a bank screening its customers against a credit reference database to determine whether or not to offer a loan to the data subject)

The more criteria that are met, the more likely it is to present a high risk to the rights and freedoms of data subjects.[11]

Additionally, Art 35(3) of the GDPR specifies that a DPIA:

> … shall in particular be required in the case of:
> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
> (c) a systematic monitoring of a publicly accessible area on a large scale.

Article 35(7) of the GDPR outlines what content a DPIA is required to contain as a minimum. This includes a description of the measures envisaged to address the privacy risks identified and to demonstrate compliance with the GDPR. In addition, for DPIAs the GDPR directs data controllers to seek the views of data subjects on the intended processing of personal data (Art 35(9)), and to conduct reviews if there is a change in the risk associated with a particular processing operation (Art 35(11)).

Conducting privacy health checks

The way that an entity conducts privacy health checks will depend on a range of factors, such as the type of health check being undertaken, which laws apply, the scope of the health check and the potential privacy risks and impacts. There is not a one-size-fits-all approach. However, there are general principles that should be followed to ensure the relevant privacy health check provides the desired outcome:

- Privacy audits and PIAs should be carefully mapped out and scoped from the outset. Planning is key to a successful audit or assessment.
- Both privacy audits and PIAs will need to be sufficiently broad and comprehensive that they adequately map all relevant information flows and do not miss privacy touchpoints (though they can be limited to specific aspects of a Project or operations if this is desired).
- Privacy health checks should address all applicable legal privacy obligations that apply to the entity concerned, as well as applying a "public expectations" filter to ensure that the analysis meets the expectations of the public (which may be higher than the legal requirements).
- Privacy risks or impacts should not be downgraded or omitted in an attempt to get a Project over the line or to meet Project deadlines. Where risks exist, it is important that they be disclosed with a full explanation of how mitigations will be applied or risks addressed.
- Privacy health checks should involve relevant stakeholders, both internal and external (such as customers), and should capture all relevant areas within their scope.
- Appropriate resources should be utilised in carrying out privacy health checks. Privacy health checks are not just for the remit of privacy specialists or lawyers. Other professionals, such as IT professionals, data scientists and data analysts should also be involved, where applicable. They are often better placed to assess the susceptibility and penetrability of systems to cyber-security incidents, assess the benefits or potential mitigations, and can work with privacy specialists and lawyers to help map data flows and to identify and test whether certain datasets disclose, or have the potential to disclose, any personal information.
- The findings of a privacy audit or PIA should be actioned in a timely manner based on the relative likelihood and the potential impact of risks. If undertaking a PIA, the PIA's recommendations should be incorporated in the Project's development and design.
- Usually it will be appropriate for the stakeholders involved in the Project to have the opportunity to comment on any draft recommendations from a PIA prior to them being finalised. This allows for modifications to reflect what is practical and proportionate to address risk.
- A PIA report should be treated as a "living document"[12] to be updated to reflect any changes to a Project that creates new privacy impacts or changes any assumptions or facts underlying the report.[13]

Conclusion

We live in a data-driven age where data breaches are occurring on an increasingly frequent basis. The impact of a data breach extends far beyond the consequences of breaching relevant privacy laws and can result in significant reputational and financial damage to an organisation. The argument for undertaking effective privacy health checks to mitigate the risk of such damage is therefore especially strong. Privacy health checks enable

entities to keep their finger on the pulse and are important tools for flagging early privacy gaps and non-compliances that, if not addressed, can lead to more significant privacy breaches.

Monique Azzopardi
Senior Associate
Clayton Utz
mazzopardi@claytonutz.com
www.claytonutz.com

Mathew Baldwin
Special Counsel
Clayton Utz
mathewbaldwin@claytonutz.com
www.claytonutz.com

Footnotes

1. Office of the Australian Information Commissioner *Notifiable Data Breaches Scheme 12 Month Insights Report* www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/ndb-scheme-12%E2%80%91month-insights-report.pdf.
2. Above n 1, at 8.
3. Office of the Victorian Information Commissioner *Privacy Impact Assessment — Accompanying Guide* https://ovic.vic.gov.au/resource/privacy-impact-assessment-accompanying-guide/ at 5.
4. Office of the Australian Information Commissioner *Guide to Undertaking Privacy Impact Assessments* (May 2014) www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf at 3.
5. Privacy Act, s 33D.
6. GDPR, Art 35(1).
7. Above n 6, Art 25.
8. Above n 6, Recital 78.
9. Article 29 Data Protection Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (As last revised and adopted on 4 October 2017) (Guidelines) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 at 8–12.
10. Above n 9, at 9–11.
11. Above n 9, at 11.
12. Above n 3, at 5.
13. Certain public sector entities have published helpful guides to undertaking PIAs, including the OAIC (www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf) and the Office of the Victorian Information Commissioner (https://ovic.vic.gov.au/resource/privacy-impact-assessment-accompanying-guide/). While they are geared at specific legislation (the Privacy Act and the Privacy and Data Protection Act 2014 (Vic) respectively), they are broadly applicable to other entities seeking to undertake similar PIAs.

Castles and casualties: recent case law about procedure, trespass and the private sphere

Dr Bruce Baer Arnold *UNIVERSITY OF CANBERRA*

Two recent judgments in the Northern Territory and New South Wales highlight the importance of procedure in body searches and collection of evidence in residences. Those judgments reaffirm privacy dicta such as an Australian's McMansion is their castle and illustrate police action may be vitiated by disregard of formal protocols.

Introduction

How does privacy — the protection of the private sphere from inappropriate interference — play out in Australian law? Given media coverage over the past decade members of the public and other non-specialists are likely to understand privacy as a matter of sensitive personal data, addressed through information privacy statutes such as the Privacy Act 1988 (Cth), the Census and Statistics Act 1905 (Cth) and the Health Records (Privacy and Access) Act 1997 (ACT). In contrast practitioners recognise that privacy encompasses physical and spatial integrity, for example protection from arbitrary and disproportionate searches of an individual's dwelling place or person. They also recognise that procedure is important, with non-compliance by officials or other entities potentially invalidating searches and resulting in damages awards.

Two recent judgments in the Northern Territory and New South Wales — *O'Neill*[1] and *Attalla*[2] — illustrate the salience of historic law regarding the protection of the private sphere and the scope for courts to restrict official action that is disproportionate. They also highlight concerns about misreading by law enforcement personnel of formal procedures regarding searches. This article considers those judgments.

Salient points for practitioners and policymakers regarding searches of criminal suspects and collection of evidence at domestic premises are:

- Tort and criminal law coexist with information privacy statutes to protect the personal sphere and bound executive over-reach.
- Law enforcement agencies continue to experience difficulty in communicating and ensuring compliance with protocols that embody privacy.
- In the absence of a justiciable national Bill of Rights, Australian courts draw on a large body of common law that recognises the personal sphere.

Forced disclosure

"Pat downs", emptying of pockets and disrobing are standard but contentious features of law enforcement across Australia: evident in every jurisdiction and authorised under a range of statutes. That law expressly authorises both strip searches and cavity searches of inmates of correctional institutions and of criminal suspects or migration detainees. Police practice has on occasion been condemned as an egregious abuse of power.[3] Its authorisation may encompass video recording of the search as a mechanism for minimisation of abuse, highlighted in *Riera*.[4] Searching is not prohibited under the international human rights agreements to which Australia is a signatory and is not impermissible in either the three Australian human rights jurisdictions or in the European Union under the benchmark European Convention on Human Rights.[5]

In *Attalla* the NSW District Court has noted egregious disregard by NSW Police personnel of requirements under the Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), awarding the plaintiff $112,387 for an unjustified and incorrectly conducted strip search alongside unlawful detention. The Act specifically referred to regard for privacy in the conduct of searches.

Steven Attalla was arrested in a public place during March 2015 for hindering police in the execution of their duty. At that time he was 53 years old, with no relevant criminal record. Senior Constable Courtney Cruickshank told Attalla that she reasonably suspected him of being in possession of prohibited drugs. His "hindrance" took the form of rejecting her proposition that he be searched. Attalla was then wrist locked, handcuffed, taken in the rear cage of a police wagon to Kings Cross Police Station and strip searched. That involved him removing his pants and underpants, lifting his genitalia to allow inspection and squatting while naked. Proceedings after a Court Attendance Notice for hindering police were ultimately dismissed. Attalla sued the state for wrongful arrest, and assault and battery by the police officers.

The state conceded that both the strip search and his continued detention after that search were unlawful. The Act provides for warrantless stop, search and detention of persons whom NSW police officers suspect on reasonable grounds of having control/possession of anything stolen, prohibited plants or prohibited drugs.[6] Section 32 of the Act specifically refers to privacy, mandating protocols regarding searches by a police officer or other person. The search must be conducted "in a way that provides reasonable privacy for the person searched", "as quickly as is reasonably practicable" and as least invasive as practicable in the circumstances.[7] Further, conduct of the search must not encompass the person's genital area unless the police officer or person suspects on reasonable grounds that it is necessary to do so for the purposes of the search.[8]

Attalla referred to insulting language.[9] More saliently, he characterised the search as an invasion of privacy, with hurt, humiliation, disgust and embarrassment.[10] "It was outrageous. It was something that I thought I'd never ever be in a position to be treated in such a humiliating fashion".[11] The state, in contrast to Officer Cruickshank, conceded the search was unlawful, "humiliating" and "difficult".[12]

Is there a systemic problem? The court noted:

> Officer Cruickshank admitted a lack of familiarity with the requirements of s 31. The pre-requisites in s 32(2), (3), (4), (5), (6), and (7) were not established on the evidence. Yet the State, to the conclusion of submissions, maintained that the strip search was only a technical breach. Neither of the two male police officers who conducted the strip search gave evidence of a suspicion on reasonable grounds that it was necessary to search the genital area of Mr Attalla for the purposes of the search, as s 32(6) requires.[13]

In considering damages the court indicates that by the time of the strip search Officer Cruickshank no longer suspected that Attalla possessed prohibited drugs. Damages were aggravated by the absence of any evidence explaining the purpose and need for the strip search. Although it might be possible that a strip search could reveal drugs that might not have been identifiable by an ordinary search, that was not explained and there was no evidence as to whether alternatives to the invasive procedure were considered.[14]

The court thus commented:

> The State's concession in relation to the strip search illustrates that the police officers have used a most invasive power without the slightest justification. None of the several requirements in ss 31 and 32 of LEPRA were the subject of evidence or submissions. The grievous nature of the offensive conduct might be mitigated in circumstances of urgency or turmoil, but here the admitted worst offence, the strip search, was done in the relative peace of the police station, where there was no resistance from Mr Attalla. Even this did not produce any consideration of the requirements of the law governing strip searches by any officer, apparently because Officer Cruikshank had some time ago determined to proceed with the strip search. I am not persuaded that she retained a bona fide belief in the need for the strip search to locate the once suspected drugs.[15]

The court noted *New South Wales v Ibbett*[16] and *Adams v Kennedy*[17] regarding the award of exemplary damages, with *Ibbett* characterising that award as:

> a method by which, at the instance of the citizen, the State is called to account by the common law for the misconduct of those acting under or with the authority of the Executive Government.[18]

The state's schedule of damages referred to the humiliation of Mr Attalla from its unlawful conduct, but, in the court's view, grossly understated the appropriate level of damages.[19]

What can we make of the judgment? It is not a crime to be busy texting while sitting on a fence in one of the busier streets of Darlinghurst at 3.30 am but police might well have suspicions. Those suspicions need to be reasonable. More importantly, law enforcement agencies need to ensure that their personnel are acquainted with and abide by law regarding detention and searches. The unlawful detention in *Attalla* is regrettably not isolated[20] and arguably has attracted inadequate remedies, with damages rarely more than $30,000.[21] For readers of this *Bulletin* the salient conclusion is that disregard of the personal sphere, extending beyond strip searches to cavity searches and coerced provision of DNA *is* permissible in Australian law if agents of the state act lawfully. In *Attalla* they did not and it's disquieting that the casualty in this instance was required to hold the state to account.

Whose castle?

It is axiomatic that an Australian's McMansion is their castle — a manifestation of their private sphere that is not to be invaded other than in exceptional circumstances. That axiom, an iteration of the long-standing dictum that an Englishman's home is his castle,[22] recognises the scope for individuals to preserve their dignity through mundane action such as closing a door or drawing blinds and curtains. That action is a foundation of common law regarding trespass, in other words a law-abiding person's scope for exclusion of unwanted observation or other interaction in a dwelling place. It coexists with criminal law regarding residences[23] and inappropriate scrutiny in other places such as change rooms where there is an expectation of non-interference.[24] It is reflected in the large body of Australian case law that draws on landmark judgments such as *Entick* regarding accountability through a requirement for carefully-delimited warrants for searches of

residential or other spaces.[25] (Concerns regarding overly-broad warrants are evident in the June 2019 Australian Federal Police search of the Australian Broadcasting Corp's head office.)

Questions about police misunderstanding of authority, about procedure and the admissibility of evidence are at the heart of the judgment in *O'Neill v Roy*.[26] The Northern Territory Supreme Court heard an appeal from the Local Court's finding Ms Roy not guilty of breaching s 120(1) of the Domestic and Family Violence Act (NT), centred on her cohabitation with her partner in public housing while allegedly intoxicated. There were multiple previous interactions between Roy and the Police.[27] The Local Court's finding was based on the inadmissibility of NT Police evidence through a visit to the residence.

In the first instance the Local Court held that, absent complaints, the police lacked power under the Police Administration Act (NT) or the Domestic and Family Violence Act to attend at the private residence to check on persons of interest to ensure that they are complying with a domestic violence order. They had no reasonable belief that Roy was intoxicated and thus should be visited and breath-tested.[28] Further, there was no basis for a request for the breath test at the residence as the police had exceeded their powers on the day in question while "conducting pro-active DVO compliance checks" as part of *Operation Haven*.[29] It is unclear whether *Haven* extended to private housing in more upmarket locations in Darwin.

The Local Court did not specifically deal with arguments about an implied licence to knock on Roy's door, with her counsel arguing that where the legislature had carefully defined the rights of the police to enter private property, it was not for the courts to alter the balance between individual privacy and the power of officials.[30] It was common ground at the voir dire that if the breath test was excluded that was the end of the case, the Local Court accordingly found Roy not guilty.[31] The Territory appealed.

The Supreme Court commented that Reg 6 of the Domestic and Family Violence Regulations (NT) does not empower a police officer to enter a defendant's private property or home for the purpose of administering a breath test. Regulation 4:

> … relates only to a condition prohibiting consuming alcohol; it has nothing to say about a condition prohibiting being in the company of the protected person when intoxicated. However that may be, the requirement to comply with a direction arises only if the direction is reasonable. It was submitted by the appellant that lack of "reasonableness" in this context may relate to excessively invasive and frequent requests, or requests that a defendant cannot reasonably comply with. That may well be so but I see nothing reasonable about knocking on the door of a person's home and directing a person to come to the door in order to conduct a breath test, particularly if the circumstances are such that s 126(2A) of the PAA do not apply and the police officer is a trespasser. To recognize that such a direction is reasonable would be to in effect enlarge the statutory powers given to police officers by s 126(2A).[32]

The court recognised that a police officer making enquiries from neighbours who may be potential witnesses to an offence can enter private land and knock on doors and ask questions.[33] However, going to Ms Roy's door for the purpose of investigating whether or not she was complying with the Domestic Violence Order was outside of the purposes of implied entry to the premises or any part thereof.[34] The court affirmed the statement by Brennan J in *Halliday* that:

> This case is about privacy in the home, the garden and the yard. It is about the lawfulness of police entering on private premises without asking for permission. It is a contest between public authority and the security of private dwellings.[35]
>
> There is, of course, a tension between the common law privileges that secure the privacy of individuals in their own homes, gardens and yards and the efficient exercise of statutory powers in aid of law enforcement. The contest is not to be resolved by too ready an implication of a licence in police officers to enter on private property. The legislature has carefully defined the rights of the police to enter; it is not for the courts to alter the balance between individual privacy and the power of public officials. It is not incumbent on a person in possession to protect his privacy by a notice of revocation of a licence that he has not given; it is for those who infringe his privacy to justify their presence on his property. There may well be a case for enlarging police powers of entry and search, but that is a matter for the legislature.[36]

After considering a range of authority[37] it endorsed[38] the Canadian Supreme Court's statement in *Evans* that if:

> … under the "implied licence to knock", the occupier of a home may be taken to authorize certain persons to approach his or her home for certain purposes. However, this does not imply that all persons are welcome to approach the home regardless of the purpose of their visit. For example, it would be ludicrous to argue that the invitation to knock invites a burglar to approach the door in order to "case" the home. The waiver of privacy interest that is entailed by the invitation to knock cannot be taken that far. …
>
> [if] intention is not a relevant factor, the police would be then be authorized to rely on the "implied licence to knock" for the purpose of randomly checking private homes for evidence of criminal activity. The police could enter a neighbourhood with a high incidence of crime and conduct "surprise checks" of the private homes of unsuspecting citizens, surreptitiously relying on the implied licence to approach the door and knock. Clearly, this Orwellian vision of police authority is beyond the pale of any "implied invitation".[39]

The NTSC judgment concludes:

> … consistently with the decisions of the High Court of Australia, the Court of Appeal of New Zealand and the

> Supreme Court of Canada, absent a clear and express statutory power to do so, neither the police nor anyone else has an implied invitation to enter private property, or the threshold of a person's home, for the mere purpose of investigating whether a breach of the law has occurred or for the purpose of gathering evidence of criminal activity by the occupier, in circumstances where there is no basis for believing or even suspecting that an offence has been or is in the process of being committed, absent an express invitation by the occupier to do so. To hold otherwise would be an Orwellian intrusion into the fundamental rights of privacy that the common law has been at great pains to protect and would amount to a new exception to the common law. It is not for judges to create such an exception. That is the province of the elected legislators who are responsible to the people for their decisions. I therefore find that the police had no power to go to Ms Roy's home and take a sniff of her breath and then require Ms Roy to provide a sample of her breath, that they were trespassers when they entered her alcove and knocked on the door. Consequently the evidence was unlawfully obtained.[40]

The court in *O'Neill* states that "this appeal from the Local Court raises important questions about the admissibility of evidence relating to an alleged breach of a domestic violence order".[41] Given the Territory's approach to "social order" we might expect amendment of the two statutes to address the procedural problem that invalidated the police action. The court has however provided an important restatement regarding the jurisprudence on invitation and access to residences for the purposes of law enforcement.

Dr Bruce Baer Arnold
Assistant Professor
Faculty of Law
University of Canberra
www.canberra.edu.au

Footnotes

1. *O'Neill v Roy* [2019] NTSC 23; BC201902885.
2. *Attalla v New South Wales* [2018] NSWDC 190; BC201840353.
3. See for example E Russell "Revisiting the Tasty raid: lesbian and gay respectability and police legitimacy" (2015) 41(1) *Australian Feminist Law Journal* 121; and M Groves "Not So Tasty" (1995) 20(3) *Alternative Law Journal* 123.
4. *R v Riera* [2016] SADC 108; BC201607545 at [58].
5. See for example *Wainwright v United Kingdom* (2007) 44 EHRR 40.
6. Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), s 21.
7. Above, s 32(4) and (5).
8. Above n 6, s 32(6).
9. Above n 2, at [84].
10. Above n 2, at [81] and [101].
11. Above n 2, at [101].
12. Above n 2, at [90] and [107].
13. Above n 2, at [99].
14. Above n 2, at [95].
15. Above n 2, at [118].
16. *New South Wales v Ibbett* (2006) 229 CLR 638; 231 ALR 485; [2006] HCA 57; BC200610288.
17. *Adams v Kennedy* (2000) 49 NSWLR 78; [2000] NSWCA 152; BC200003503.
18. Above n 16, at [38].
19. Above n 2, at [94].
20. Recent examples of unlawful restraint include *New South Wales v Quirk* [2012] NSWCA 216; BC201205501; *Majindi v Northern Territory of Australia* (2012) 31 NTLR 150; 260 FLR 459; [2012] NTSC 25; BC201202071; *Randall v New South Wales* [2013] NSWDC 277; BC201340315; *Hamilton v New South Wales (No 13)* [2016] NSWSC 1311; BC201607961; *Raad v New South Wales* [2017] NSWDC 63; BC201740155; *Costello v New South Wales* [2017] NSWDC 152; BC201740357; *Hemelaar v Walsh* [2017] QDC 151; BC201740316; *Lule v New South Wales* [2018] NSWCA 125; BC201804938; *Gibb-Smith v New South Wales* [2018] NSWDC 204; BC201840396 and *Johnson v South Australia* [2019] SADC 35; BC201902442.
21. See more broadly J Ransley, J Anderson and T Prenzler "Civil litigation against police in Australia: Exploring its extent, nature and implications for accountability" (2007) 40(2) *Australian & New Zealand Journal of Criminology* 143 and T Hopkins "When police complaint mechanisms fail: The use of civil litigation" (2011) 36(2) *Alternative Law Journal* 99.
22. *Semayne's case* [1572] EngR 333 and *Bostock v Saunders* (1773) 2 Wm Bl 912; 96 ER 539, endorsed in *Monis v R; Droudis v R* (2013) 249 CLR 92; 295 ALR 259; [2013] HCA 4; BC201300755 per Crennan, Kieffel and Bell JJ at [321].
23. See for example Police Offences Act 1935 (Tas) s 14A.
24. *R v Cemitis, Andrew [No 2]* [2010] NSWDC 89; *Brown v Palmer* (2008) 192 A Crim R 18; [2008] VSC 335; BC200807762; *Todd v Police No SCCRM-02-1796* (2003) 226 LSJS 31; [2003] SASC 62; BC200300746; *R v Hore* [2010] SASFC 60; BC201008903 and *Carger v Police* [2004] SASC 388 BC200407873.
25. *Entick v Carrington* (1765) 19 State Tr 1030; (1795) 95 ER 807. See also T Endicott "Was Entick v Carrington a Landmark?" in *Entick v Carrington: 250 Years of the Rule of Law*, A Tomkins and P Scott (eds) London: Hart, 2015, p 109.
26. Above n 1.
27. Above n 1, at [5].
28. Above n 1, at [9] and [15].
29. Above n 1, at [4], [7] and [16].
30. Above n 1, at [9].
31. Above n 1, at [11].
32. Above n 1, at [20].
33. Above n 1, at [21].
34. Above n 1, at [38].

35. *Halliday v Nevill* (1984) 155 CLR 1; 57 ALR 331; BC8400463 per Brennan J at [2].
36. Above, per Brennan J at [20]; above n 1, at [26].
37. *Barker v R* (1983) 153 CLR 338; 47 ALR 1; BC8300076; *Halliday v Nevill* (1984) 155 CLR 1; 57 ALR 331; *Munnings v Barrett* [1987] Tas R 80; (1987) 5 MVR 403; *Fisher v Ellerton* [2001] WASCA 315; BC200106302; *Tasmania v Crane* (2004) 148 A Crim R 346; [2004] TASSC 80; BC200404906; *Plenty v Dillon* (1991) 171 CLR 635; 98 ALR 353; [1991] HCA 5; BC9102635 *Morris v Beardmore* [1981] AC 446; *Kuru v New South Wales* (2008) 236 CLR 1; 246 ALR 260; [2008] HCA 26; BC200804305; *Howden v Ministry of Transport* [1987] 2 NZLR 747; *O'Connor v Police* [2010] NZAR 50; *Police v McDonald* [2010] NZAR 59; and *Evans and Evans v R* (1996) 104 CCC (3rd) 23.
38. Above n 1, at [43].
39. *Evans and Evans v The Queen* (1996) 104 CCC (3rd) 23, L'Heureux-Dubé J at [7]–[13].
40. Above n 1, at [44].
41. Above n 1, at [1].

For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047
Cite this issue as (2019) 16(3&4) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067 This newsletter is intended to keep readers abreast of current developments in the field of privacy law. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers.