THE UNIVERSITY OF NEW SOUTH WALES

galexia CONSULTING

Representative complaints - a new approach to making privacy laws work for consumers (September 2003)

Chris Connolly, Nawaz Isaji

This paper was presented at the Baker & McKenzie Cyberspace Law and Policy Centre's "Surveillance and Privacy 2003" conference (Sydney, 8-9 September 2003) by Chris Connolly[1].

This paper is available in the following formats from http://consult.galexia.com:

— HTML[2]

— PDF[3]

1. Abstract

This paper surveys national and international privacy laws to assess the ability of courts and privacy regulators to consider "representative complaints", and argues that privacy breaches are particularly suited to resolution through representative action. Several case studies of representative privacy complaints are included, as well as an overview of privacy class actions in the United States and Canada. The paper concludes that the benefits of representative complaints are yet to be fully realised in the privacy field.

[1] Chris Connolly is a Director of Galexia Consulting, a specialist consulting firm which focuses on electronic commerce, privacy, authentication and identity management. Chris is also a Visiting Fellow in the Law Faculty at the University of New South Wales, where he teaches Electronic Commerce Law and Practice (amongst other courses) in the Masters Program and is a Director of the Financial Services Consumer Policy Centre, a research centre affiliated with the UNSW.

[2] <http://consult.galexia.com/public/research/articles/research_articles-pa01.html>

[3] <http://consult.galexia.com/public/research/assets/gc_representative_complaints_200309.pdf

Contents

2. Introduction

In 1981, the *West Australian* newspaper published a photograph of a naked woman on the front page without the woman's consent. Not surprisingly this resulted in a privacy complaint to the Australian Press Council.

This may seem like a strange starting point for a discussion of representative privacy complaints, but the case is illustrative of one of the great pitfalls of privacy laws. The laws are only as good as the complaints, but the complaints process itself is not well suited to the protection of privacy.

To be fair to the *West Australian*, the woman was being carried down a ladder by a fire-fighter who had just rescued her from a burning building. The building was also in Sydney and the editor later explained that he doubted anyone in Perth would recognise her. The newspaper did not name her or provide any other identifying information.

Several people, including two members of parliament, complained that the photograph invaded the woman's privacy. This resulted in the Australian Press Council Adjudication Number 118 (November 1981)[4], in which the Council dismissed the complaint in one sentence:

> "The council considers that in the absence of any evidence that the woman, herself, felt her privacy had been breached, it is unable to uphold the complaint."

It is an extraordinary decision because it places the onus for complaining on a privacy victim, who would surely exacerbate the privacy breach by identifying herself and pursuing the matter through the formal complaints process.

On the other hand, if there had been some capacity for the Council to consider a representative complaint, an obvious breach of privacy would have been found (subject to due consideration of whether some other public interest justified the publication of the photograph).

It is our view that representative complaints are particularly suited to privacy issues, and that they have been under-utilised to date.

The advantages of representative complaints in the privacy field are:

- **Minimising further privacy intrusion**
  A third party can manage the formal complaints process in a way which limits any further invasion of the privacy of the person who has suffered the original breach.
- **Dealing with systemic issues**
  Many privacy breaches may appear minor to an individual, but actually represent serious systemic issues for the wider community. Complaints which may not be worthwhile pursuing for one consumer may be easier to justify for a class.
- **Effective deterrence**
  Solo privacy complaints do not represent an effective deterrent for privacy invasive practices. An individual complainant will probably settle at a lower threshold than a group. The company or agency responsible for the breach is unlikely to be named or receive any negative publicity. The higher profile of representative complaints and class actions provides a more effective deterrent.

[4] <http://www.austlii.edu.au/au/other/apc/>

— **Practical benefits**
There are numerous practical benefits to proceeding via a representative complaint, although these will differ from case to case. One of the benefits we have seen in practice include the ability to utilise information from complainants who would otherwise be unavailable for a formal individual complaint (such as transient, low income populations). Other obvious benefits are costs and the ability to access legal advice. An important benefit in Australia is the ability to see out the interminably long time privacy complaints take to be resolved – something an established advocacy organisation is in a better position to do than an individual consumer.

Having stated that there are significant advantages for representative complaints in the privacy field, it should be noted that representative complaints are not always an available option in privacy laws. Many jurisdictions do not appear to allow third parties to lodge complaints on behalf of privacy victims. Also, in those jurisdictions where privacy representative complaints can be lodged, there is little consistency on issues such as whether the consent of the victims is required.

This paper should serve as a discussion starter on this issue and lead to the wider acceptance of representative complaints and some consistency about the conditions which are placed on such complaints.

3. The current legal position in Australia

3.1. Commonwealth

The *Privacy Act 1988 (Cth)* is Australia's authoritative source of legislation for dealing with privacy disputes. Personal information collected and handled by federal public sector organisations and by a significant part of the private sector is subject to the Act. In addition to establishing the Information Privacy Principles (for public sector agencies), the National Privacy Principles (for the private sector), and the capacity to register industry privacy codes of conduct, it sets out the role of the Federal Privacy Commissioner.

The Privacy Act specifically allows representative complaints to be made to the Commissioner. Furthermore, the section on representative complaints is more detailed than the legislation of those Australian states which have privacy laws, and the laws of other countries.

The Act provides details of:

— Conditions for complaint registration;

— How and when a Commissioner may refuse to pursue a complaint and what happens if the Commissioner makes such a determination; and

— How an individual complaint may become a representative one.

Under Section 38 of the Act, representative complaints must be lodged in accordance with the ordinary complaints registration procedure (s 36) plus several additional procedures set out in the section.

Section 38:

(1) A representative complaint may be lodged under section 36 or accepted under subsection 40 (1B) only if:

> (a) the class members have complaints against the same person; and
>
> (b) all the complaints are in respect of, or arise out of, the same, similar or related circumstances; and
>
> (c) all the complaints give rise to a substantial common issue of law or fact.
>
> (2) A representative complaint made under section 36 or accepted under subsection 40 (1B) must:
>
> (a) describe or otherwise identify the class members; and
>
> (b) specify the nature of the complaints made on behalf of the class members; and
>
> (c) specify the nature of the relief sought; and
>
> (d) specify the questions of law or fact that are common to the complaints of the class members.
>
> In describing or otherwise identifying the class members, it is not necessary to name them or specify how many there are.
>
> (3) A representative complaint may be lodged without the consent of class members.

Overall, the Commonwealth has one of the broadest approaches to accepting representative complaints, and two high profile privacy representative complaints have now been lodged (these are presented as detailed case studies at the end of this paper).

3.2. NSW

In NSW, the *Privacy and Personal Information Protection Act* 1998 provides a compliant handling system similar to the Commonwealth system. However, section 45, the key complaints provision, does not directly adduce any legislative support for the notion of representative complaints. There is no sub-section of the Act which unequivocally deals with representative complaints. However it may be inferred by s 45 (1) that another person may make the complaint. It states:

> s45 (1) A complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual.

It would seem from the wording of this clause that anyone may make the complaint, as long as it affects an individual.

Privacy NSW (the Agency which administers privacy complaints) has obviously considered this issue in some detail. On 22 July 2002 they issued a "Protocol for the handling of complaints by Privacy NSW (the Office of the Privacy Commissioner)"[5]. Section 2.2.2 deals with representative complaints:

> **2.2.2 Third party complaints**
>
> In January 2002 the Privacy Commissioner received legal advice to suggest that s.45 of the PPIP Act only contemplates that a complaint can be made by an individual whose privacy has

[5] <http://www.lawlink.nsw.gov.au/pc.nsf/pages/complaints#214>

> been violated or interfered with. That is, it is arguable that a 'third party' whose privacy has not been affected, such as a 'whistleblower', cannot make a complaint under s.45.
>
> Where a third party is acting *on behalf of* the person whose privacy has allegedly been violated or interfered with, Privacy NSW will treat that as a 'first party' complaint. (Examples here include a parent on behalf of their child, a lawyer on behalf of their client, or an MP on behalf of their constituent.)
>
> Unrelated third party complaints will not be accepted as complaints under s.45. However they may be treated as requests for advice.
>
> However if a complaint about conduct potentially affects an individual as a member of a class (for example a person whose records are inadequately secured by an agency), the fact that the personal information of other persons may be equally affected by that conduct does not preclude Privacy NSW from investigating the matter.
>
> This is not to suggest that the complainant must prove that they have suffered 'harm' in order for their privacy to have been 'violated or interfered with'. Whether or not a person's privacy has been 'violated or interfered with' is determined as against certain .
>
> In addition to his power to receive, investigate and conciliate complaints (s.36(2)(k)), the Privacy Commissioner also has power under s.36(2)(l) to "conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate". On that basis, the Privacy Commissioner will consider seriously any third party 'whistleblower'-type complaint, and may review the matter if it raises significant privacy concerns which may affect the public interest. On this basis the Privacy Commissioner may be able to issue a Special Report to Parliament about the matter under s.65.

NSW therefore appears to be willing to find a way to accept representative complaints, despite some technical difficulties with the Act. However, a complaint by an advocacy organisation on behalf of a broad class of unnamed consumers may struggle to meet the definition of a complaint (see the Tenancy Database case study for an example of this type of complaint).

3.3. Victoria

The *Information Privacy Act* was introduced in Victoria in 2000. The complaints section (s 25), also gives some regard to representative complaints. It states:

> (3) In the case of an act or practice that may be an interference with the privacy of 2 or more individuals, any one of those individuals may make a complaint under sub-section (1) on behalf of all of the individuals with their consent.

However, the complaint can only be made in a certain way here. The representative must be part of the group affected. That is, the representative must also face the same “interference” with his or her privacy as the others in the group in order to make the complaint. This is in contrast to the NSW Act and the Federal Act, where anyone may represent the group. Also in Victoria, the representative must gain the consent of his or her fellow litigants to make the complaint. This is in direct contrast with the federal law, which expressly states that representative complaints do not have to have the consent of their class members.

4. The current international legal position

This section provides a brief and partial survey of international approaches to privacy representative complaints and privacy class actions[6].

4.1. Canada

The Canadian *Privacy Act* 1985 does not provide a detailed description of representative complaints. Section 29(2) provides:

> **Complaints submitted on behalf of complainants**
>
> Nothing in this Act precludes the Privacy Commissioner from receiving and investigating complaints of a nature described in subsection (1) that are submitted by a person authorized by the complainant to act on behalf of the complainant, and a reference to a complainant in any other section includes a reference to a person so authorized.

The Canadian law does not provide details of representative complaints, although it does acknowledges that they can be made, and that there is nothing to stop them being made within the Privacy Act.

The first privacy class action in Canada was brought in February 2003.

The case, Taylor v. Saskatchewan[7], is a class action suit filed against several private and government organisations for the loss of the financial and health information of more than 850,000 Canadians due to the theft of a computer hard drive from an information technology services provider. The information included names, addresses, bank account details, social insurance numbers and cheque information. The suit includes claims for breach of fiduciary duty, breaches of contract and consumer confidence, and negligence in the custody of sensitive personal information. Class members seek damages for the "anguish and concern they have experienced since their information was placed at risk"[8].

4.2. Hong Kong

The Hong Kong *Personal Data (Privacy) Ordinance* 1995 sets out complaint procedures in Part 37. It states that:

> 1) An individual, or a relevant person on behalf of an individual, may make a complaint to the Commissioner about an act or practice
>
> a) specified in the complaint; and
>
> b) that:
>
> i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user specified in the complaint;

[6] The authors plan to update this paper with information from other jurisdictions. Input is welcome – consult@galexia.com

[7] *Taylor v. Saskatchewan*, Sask. Q.B., No. 243, filed 2/3/03; 2 PVLR 114, 02/10/03.

[8] WGM Internet Law Bulletin, March 17, 2003

> ii) relates to personal data of which the individual is or, in any case in which the data user is relying upon an exemption under Part VIII, may be, the data subject; and
>
> iii) may be a contravention of a requirement under this Ordinance (including section 28(4)).
>
> 2) Where 2 or more individuals may each make a complaint about the same act or practice, then any of those individuals, or any relevant person on behalf of any of those individuals, may make such a complaint on behalf of all those individuals, and the provisions of this Ordinance (including subsection (1)) shall be construed accordingly.

Note that the definition of 'relevant person' under the Ordinance does not shed any additional light on representative complaints, nor does the Commissioner's Complaint Handling Policy.[9] It seems clear that some form of limited representative complaint can be made under the Ordinance, and Part 37 (2) might imply that consent of additional affected parties is not required. However, there does not appear to be any scope for a third party representing the group.

4.3. New Zealand

The New Zealand *Privacy Act 1993*[10] contains a fairly broad definition of complaint. Section 67 (1) states:

> Any person may make a complaint to the Commissioner alleging that any action is or appears to be an interference with the privacy of an individual.

It seems clear that the 'person' referred to at the beginning of the clause, and the 'individual', do not necessarily have to be the same person. It is very much foreseeable that the 'person' could bring about the claim regarding any 'individual'.

Section 71 (1)(e) of the Act gives the Privacy Commissioner some discretion as to whether or not to accept a representative complaint:

> (1) The Commissioner may in his or her discretion decide to take no action or, as the case may require, no further action, on any complaint if, in the Commissioner's opinion…
> (e) The complainant does not have a sufficient personal interest in the subject-matter of the complaint.

In New Zealand, the Commissioner can only conciliate complaints. In order to obtain a determination, the complainant must approach the Human Rights Review Tribunal (HRRT). Section 82 of the Privacy Act includes a specific provision for class actions at this stage:

> (4) The [Director of Human Rights Proceedings] may, under subsection (2) of this section, bring proceedings on behalf of a class of individuals, and may seek on behalf of individuals who belong to the class any of the remedies described in section 85 of this Act, where the [Director of Human Rights Proceedings] considers that a person to whom this section applies is carrying on a practice which affects that class and which is an interference with the privacy of an individual.

[9] <http://www.pco.org.hk/english/enquiries/complaint_handling.html>

[10] <http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html>

Note that Section 82 deals with proceedings brought by the Director of Human Rights Proceedings. Individuals can potentially pursue a matter on their own behalf using Section 83. However, it is "uncertain" whether an aggrieved individual can bring a representative or class action under Section 83:

> In *New Zealand Freedom from Discrimination Group v New Zealand Grand Lodge of Freemasons* (1984) EOC 92-008, the Equal Opportunities Tribunal left unresolved the issue whether a group of aggrieved persons could pursue a class action where the Human Rights Commission or Race Relations Conciliator declined to proceed on their behalf[11]. [Note: the Equal Opportunities Tribunal is the predecessor institution of the current Human Rights Review Tribunal, which has jurisdiction now over privacy cases]

4.4. United States of America

There have been numerous privacy class actions in the United States, under a variety of state and federal laws[12]. One of the first privacy class actions was a case called ***Forrest v. New York Telephone***, Sup. Ct., Albany Co., Index No. 1690-95.

In that case, a class of some 30,000 phone customers claimed that New York Telephone failed to deliver promised All Call Restrict` services and published without permission "non-published numbers" through Call ID terminals. The Forrest class charged NYT with breach of contract, violation of privacy rights, unjust enrichment, gross negligence and wilful misconduct. The Court certified the action finding that the breach of contract and privacy claims involved a course of conduct common to the class[13].

Some of the better-known US privacy class actions include:

4.4.1. Double Click

In re DoubleClick[14] was a class action seeking millions in damages filed by Web users for the advertising company's use of personal information (e.g., name, address, e-mail address and Web pages visited) gathered through Internet cookies placed with the authorization of affiliated web sites. The federal claims were dismissed on the merits in March 2001. Most state claims were dismissed for lack of jurisdiction or were the subject of a fairly weak settlement between the parties in 2002.

4.4.2. Trans Union

In re Trans Union Corp[15] was a class action seeking $100 each for an estimated class of 130,000 individuals for a breach of the privacy provisions of the Fair Credit Reporting Act. Trans Union Corp. was selling lists of names and addresses to commercial marketers. The company also sold so-called "target marketing" products that contain lists of individuals who meet certain criteria. Marketers purchased these lists and then contacted the individuals to sell them various goods and services.

---

[11] Roth, Paul, Privacy Law and Practice, LexisNexis 2003, page c/535.

[12] A list of Privacy Class Actions is maintained at: <http://www.bna.com/current/cla/topp.htm>

[13] Some additional US privacy class actions include: ***Wilson v. American Cablevision of Kansas City, Inc.***, 133 F.R.D. 573 (W.D. Mo. 1990); ***Parker v. Time Warner Entertainment Co., L.P.***, 1999 U.S. Dist. LEXIS 18883 (E.D.N.Y. 1999); and ***In re Intuit*** Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001)

[14] ***In re DoubleClick*** Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001)

[15] ***In re Trans Union Corp***. Privacy Litigation, 200 U.S. Dist. LEXIS 17209 (Sept. 2002)

The Federal Trade Commission determined that Trans Union's target marketing was not an authorised use of "consumer reports" under the Fair Credit Reporting Act of 1970. Trans Union has been permanently enjoined from further sale of target marketing lists. This decision was affirmed on appeal in ***Trans Union Corp. v. F.T.C.***[16]

4.4.3. TriWest Healthcare

This class action has been brought against TriWest Healthcare Alliance for failing to protect individuals' personal information adequately. In December 2002, hard drives and laptops containing personal information were stolen from TriWest. The personal information of 500,000 military personnel was contained in the stolen equipment[17]. It was "suspected" that the thieves were targeting the personal information, as they left behind computer equipment that was more valuable. The lawsuit alleges violations of the Privacy Act, breach of contract, and negligence.[18]

5. Conclusion

While there are some gaps and inconsistencies in privacy laws in relation to representative complaints, the main issue seems to be that (outside the United States) representative complaints have been under-utilised by consumers. Many individual complainants have taken formal "solo" complaints to Privacy Commssioners, yet this has resulted in very little in the form of publicity, determinations, the naming of defendants or any form of effective deterrence. Many other potential complainants will not have taken any formal action because of concerns about exacerbating the original privacy breach, or because of a lack of confidence in formulating a complaint, or because of practical issues such as a lack of time, resources and access to legal advice.

It is useful to note that there is some opposition to the growth in privacy class actions in the United States. The leading article on the debate to date is "Limiting Private Rights of Action In Privacy Legislation" by Ronald Plesser and Stuart Inglis.[19]

> "Enforcement of privacy law is a significant issue in the debate about privacy legislation. Generally, enforcement alternatives include a private right of action, Federal Trade Commission (or other federal agency) enforcement, and state attorney general enforcement of a federally-enacted standard. Although there may be narrow circumstances in which a private cause of action is appropriate, the potential negatives that result from frivolous class action lawsuits in the privacy context should be limited. Private causes of action in privacy laws have been used to attempt to recover significant monetary awards in situations where there is no injury to consumers. Private causes of action in privacy statutes offer incentives for class action lawyers, and result in the spending of significant amounts of money to defend lawsuits raising technical claims."

This article was rebutted (somewhat) by Seth Richard Lesser's companion piece – "Internet Privacy Litigation And The Current Normative Rules of Internet Privacy Protection" (March 2003)[20].

---

[16] ***Trans Union Corp. v. F.T.C.***, *345 U.S. App. D.C. 301, 245 F.3d 809 (D.C. Cir. 2001).*

[17] <http://www.triwest.com/announcement/>

[18] <http://www.privacy.org/archives/001086.html>

[19] <http://www.cdt.org/privacy/ccp/privaterightofaction1.shtml>

[20] <http://www.cdt.org/privacy/ccp/privaterightofaction2.shtml>

> "What is made clear by the litigation of the cases… is the importance of a private right of action to protect whatever privacy interests exist. Although no company likes to receive inquiries from government investigators, the reality is that it is often the threat of private litigation that prompts corporations to take notice. Most certainly, the class actions did so here.
>
> Insofar as, going forward, the privacy matters that arise will be in the nature of breach of privacy policy claims, it seems doubtful that government enforcement actions will follow. More egregious instances of consumer fraud will consume already-stretched entities like the FTC or state attorneys general offices. The FTC will continue to pursue the worst privacy offenders but the most likely offenders will be companies that, under guise of privacy policy obfuscation, have acted wrongfully. Such less than clear-cut cases are not likely to obtain much in the way of enforcement resources. The lesson is that the threat and, sometimes, the reality of private enforcement mechanisms are necessary to deter wrongdoing. Where the regime is a private contractual one, those mechanisms are particularly appropriate and necessary."

While the US debate is of interest, there will be additional benefits for pursuing privacy representative complaints in other jurisdictions, especially those (like Australia) where little or no effect is achieved by individual complaints.

The following case studies point to a more positive future for privacy law, where committed individuals or experienced advocacy organisations will have the patience and determination to ensure that privacy breaches are dealt with in a high profile, systematic way, without risking further harm to those individuals who have already suffered privacy breaches.

6. Case study – Tenancy databases complaint

This is a representative complainant by the Tenants' Union of Queensland against TICA Default Tenancy Control Pty Ltd of (TICA). In fact there are four separate complaints (because the affected class differs slightly for each alleged privacy breach).

Complaint 1 concerns access and Complaint 2 concerns notification and accuracy. These two complaints are discussed below in some detail. Complaint 3 relates to listing timeframes and Complaint 4 relates to consent issues. These last two matters are not discussed in detail in this paper.

This was the first high profile representative complaint made under Australian privacy law. The complaint was lodged in February 2003, and although the matter is still undecided at the time of writing. It is progressing well through the Commissioner's conciliation process.

Each complaint was accompanied by a set of anonymous case studies collected from tenancy casework agencies (these are not included here).

6.1. Overview of the access complaint

The access complaint (Complaint 1) describes a class of members, in this case, tenants or former tenants, who incur charges from TICA in order for them to access information about their listing on the database.

Contact by a tenant or former tenant, is usually to ascertain whether a person is listed on the TICA database and the details of that listing; and/or to attempt to resolve a dispute about an existing listing.

The size of fee to obtain this information depends on the method of contact. People who contact the organisation by phone are charged $5.45 per minute ($327 per hour), via a 190 number. People who contact the organisation by mail must pay a fee of $11.00 in order to obtain an extract from the TICA database. This latter service may take up to 10 working days.

The complainants submit that the TICA charge for accessing personal information is in breach of TICA's obligations under the Privacy Act. The charge for access is so excessive as to be prohibitive. Further, the individuals who need to contact TICA are often low income earners for whom this cost is a very substantial amount of money. A listing on the TICA database may have substantial adverse impacts for individuals, yet it is extraordinarily difficult and expensive for a person to seek to resolve problems with inaccurate listings.

The cost to access the TICA database is simply not justified. Many tenants find themselves paying large amounts of money, through the 190 phone number in particular, to obtain information about their listing on TICA. The 190 number or the mail service are the only ways in which TICA will deal with tenants or former tenants. Tenants have no choice therefore, other than to incur these costs.

The complainants noted that:

— NPP 6 gives an individual a right of access to all the personal information that an organisation holds about them. Although there are exceptions, we submit that none of these would apply to typical access requests to a tenancy database.

— NPP 6.4 says that the charges for giving access to information should not be "excessive". Also, an organisation cannot charge an individual for lodging a request for access.

They also noted that the Commissioner's NPP Guidelines state:

> "This provision aims to prevent organisations from charging excessive amounts to discourage individuals from making requests for access. Generally speaking, an organisation could consider not charging for letting an individual view a screen or for sending information to an individual by email.
>
> When considering how much to charge an organisation may like to consider not charging an individual more than it costs the organisation to give access (for example, an organisation could base charges on the marginal cost of giving that particular access); or waiving or remitting the cost of providing access (for example, where the organisation is aware that an individual receives a benefit or pension)."

In summary, the NPPs provide that organisations cannot charge an individual for lodging a request for access, and cannot charge an excessive amount for providing the information requested.

6.2. Relief sought for the access complaint

The complainants submitted that the Privacy Commissioner, using his powers under s40 and s52 of the Act, make an order:

— prohibiting any charges by TICA when tenants or former tenants contact the company by telephone during business hours; and,

— requiring TICA to provide information to a tenant or former tenant about their listing electronically or by mail – for no cost; or by other means – only after approval by the Privacy Commissioner and on a marginal cost-recovery basis; and,

— requiring TICA to publicise on its website and in other appropriate materials, the fact that access to information by a tenant can be provided free of charge electronically or on a cost-recovery basis for other means.

6.3. Overview of the accuracy complaint

The accuracy complaint (Complaint 2) describes a class of members, in this case, tenants or former tenants, whose listing on the TICA database is either inaccurate, incomplete or not up to date. The complainants argue that TICA's listing policies result in information on the TICA database regularly being inaccurate, incomplete or out of date. As a result consumers are being listed unfairly. Many people are subsequently unable to access the private rental market due to their listing on TICA.

The complaint notes four related problems:

1. There is no process for verification of the accuracy of a listing by an independent third party. The decision to list is instead made entirely be a member of TICA. As a result, some tenants are listed vexatiously, inaccurately, for trivial matters or under non-specific headings such as 'refer to agent'.
2. Even where a listing is accurate, it may not be a breach of tenancy legislation. An example may be a listing for arrears of rent. All states allow a grace period before a lessor may issue formal notices requiring payment of rent outstanding. A TICA listing has the effect of undermining the intent of tenancy legislation.
3. TICA is in breach of National Privacy Principle 1 because it does not advise tenants that a listing has been made. Many only find out that they have been listed in a round about way, when they are denied access to renting through a real estate agent. Eventually they discover that the reason for being denied access is a TICA listing. The complainants argue that that given the serious adverse effect for individuals arising from a listing on the TICA database, the "reasonable steps" required under NPP 1.5 require TICA to contact individuals and inform them of the listing.
4. The complainants argue that the dispute resolution process provided by TICA is woefully inadequate. TICA places the onus on the tenant to investigate the reasons for the listing with the real estate agent. Real estate agents do not always co-operate. There is little a tenant can do if the real estate agent and the tenant disagree about the circumstances surrounding the listing. Some tenants also find themselves in the 'catch 22' situation of being unable to either prove or disprove a listing. This can occur when the real estate agent involved is no longer in business. This results in inaccurate, incomplete or out of date information remaining on the TICA database for years, or sometimes indefinitely.

The complainants noted that NPP 3 requires organisations to ensure that the 'personal information it collects, uses or discloses is accurate, complete and up to date'.

To meet a reasonable standard of accuracy, given the serious adverse effect of database listings on people's capacity to obtain accommodation, an adverse database listing must be subject to independent verification. The optimum way for this to occur is by way of a breach of a Tribunal or court order.

In addition, the Commissioner's NPP Guidelines state that if an organisation 'collects personal information from someone else, there may be a greater need for the organisation to take appropriate action to confirm that it is accurate, complete and up-to-date.' 'Refer to Agent' listings, 'Tenant History Only' or similar wordings are incomplete. This class of listings results in personal information being held contrary to the obligations of the Privacy Act.

6.4. Relief sought for the accuracy complaint

The complainants asked the Privacy Commissioner, using his powers under s40 and s52 of the Act, to make orders requiring TICA to:

- only list a person if the person has breached an order of a state tenancy tribunal, or similar body; and,
- require that its members keep records of these orders in order to support the listing and will provide these to TICA within seven days in the case of a dispute; and
- immediately remove listings which are incomplete, such as 'refer to agent' or 'tenant history only'; and
- remove listings where an agent is no longer in business or no longer a member of TICA and therefore the listing cannot be substantiated; and
- publish the amended listing criteria on its website and in all materials provided to tenants (such as documentation provided under the Privacy Act).

7. Case study – ISP complaint

7.1. Overview of the complaint

In July 2003 a representative complaint was made to the Federal Privacy Commissioner of Australia regarding "*Unlawful Collection, Disclosure and Use of Calling Line Identification information by Carriers and Internet Access/Service Providers."*[21]

The complaint remains undecided and is an interesting example of an alleged breach which might affect many thousands of consumers. It is also a good example of a representative complaint where a number of advocacy organisations are informally "involved", but three specific representatives have been chosen to lodge the formal complaint.

The complaint is that a breach of privacy arises when a person's telephone number can be seen and collected by their Internet Service Provider (ISP), when they dial in to connect to the Internet, despite the fact that they have elected to have their number blocked. This occurs because some telephone call carriers unblock the number in order to send it on to the ISP.

The complainants are Irene Graham (Executive Director of Electronic Frontiers Australia), Roger Clarke (an officer of the Australian Privacy Foundation and a board member of the EFA) and David Fitch.

It is stated in the complaint that the members of the class represented by the above persons are almost limitless in number. Any individuals who are customers of ISPs and/or of telephone call carriers who are affected or potentially affected by the practices complained of, are represented. This is because anyone may potentially wish to use their account to dial an ISP using calling number blocking, or may wish to change their account to silent or line blocking and to then use it to dial an ISP.

[21] The ISP case study was prepared with the assistance of Nawaz Isaji, a Galexia Consulting researcher.

The respondents in this case are twofold - the major telephone companies in Australia (namely Telstra, Optus and Comindico) for making the 'blocked' numbers visible, and also an unspecified number of ISPs who are collecting the numbers.

The complainants argue that the potential impact on the privacy and well-being of individuals arising from ISPs having access to silent and other blocked calling number information, without the individual's consent, is significant because:

- ISPs have large databases of personal information at present, which may be used to data cross-reference and data match;
- ISP staff or a temporary contractor may obtain this information and be able to match it to a real world identity;
- Some ISP owners/staff fail to recognise that blocked calls numbers, if disclosed, could result in bodily harm or death;
- Collected numbers may carry a risk of unauthorised access by crackers and hackers;
- An ISP staff member/contractor may utilise telephone information to ascertain physical whereabouts. This exposes individuals to potential blackmail, bodily harm or pressure intended to repress the individual's behaviour or speech; and
- Examples of classes of individuals who may be put at a further risk, if there whereabouts be known includes: victims of domestic violence and stalking, VIP's, celebrities, politicians, notorieties, protected witnesses, judges and other court officials, undercover law enforcement officers etc.

The complainants also note that many callers from silent and other blocked numbers are unlikely to be aware of this breach of privacy. Callers and telephone subscribers have no adequate means of knowing which carriers are involved in the transmission of their calls and hence may be disclosing blocked calling numbers.

Complaints were made by telephone and writing to the respondents prior to the formal complaint being made. In April 2003, the complainants were advised by both Telstra and Optus that the matter would be investigated and a response would be provided. However, no response has been received.

Written complaints were sent to Telstra, Optus and Comindico and ISP respondents named above on 29 and 30 June 2003. The respondents were advised that in the absence of a satisfactory response within 14 days, representative complaints would be sent to the OFPC and the Australian Communications Authority. Telstra and Optus advised, in letters dated 2 and 3 July, that they will investigate the matter and provide a response, as they did in April. Comindico, OptusNet and Netspace have provided responses, denying the complaint.

7.2. Application of the Privacy Act

7.2.1. Alleged breaches by the carriers

- **NPP 2.1**
  The complainants argue that the carriers are in breach of NPP 2.1 because the disclosure of blocked numbers to an ISP is a secondary use that is not related to the primary purpose of providing a telephone service. The carrier does not need to disclose the calling party number to the ISP in order to undertake its function of delivering the call to the called number. Furthermore, the disclosure of a blocked calling number is clearly contrary to the express wishes of the subscriber to that line.

— **NPP 1.3 and 1.5**
NPP 1.3 and 1.5 both dictate that the carriers take reasonable steps to make telephone service customers and other callers reasonably aware that they are disclosing silent numbers to ISPs. Telstra claims to have published a public notice in The Australian on Friday 22 March 2002 which told of the situation. However the complainants argue such an advertisement does not comprise 'reasonable steps' to make individuals aware of Telstra's intention to commence invading their privacy without their consent. The Optus newsletter in February 2003 stated "Note: Your number will be automatically sent when a call is placed to an Emergency Service Number. This is regardless of your CND status". It fails to state that such an unblocking also occurs when the call is transferred to an ISP.

— **NPP 8**
NPP 8 provides "Whenever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation". The complainants argue that it is both lawful and practical for carriers to deliver calls to dial up Internet access numbers without disclosing identifying information to the ISP. The complainants note that such information is sent even if the person is not even the ISP's customer. If an individual connected to their ISP from their friend's telephone line, which was blocked, the ISP would also have their number, despite their not being a customer of the ISP.

7.2.2. Alleged breaches by the ISPs

— **NPP 1.1 and 1.2 and NPP 2.1**
The collection of all such information is not necessary for an ISP's primary business of providing Internet access, nor is it used for the purpose of billing the ISP's customers.

— **NPP 1.4**
This principle relates to consent. The complainants argue it is possible, practical and reasonable for ISPs to ask for consent from their users, for them to receive their numbers, instead of covertly from the call carrier despite the caller's express instructions to the contrary.

— **NPP 1.3 and 1.5**
This principle relates to the lack of notice given, which the complainants argue compounds the primary breach.

— **NPP 8**
The complainants argue that the ISP respondents collecting blocked calling numbers are in breach of NPP 8, for the same reason as the carriers. The ISP is able to identify their customer by the username entered to gain access to the ISP's Internet services. They do not need the calling number information that in many cases is capable of identifying a person who is not the ISP's customer.

7.3. Relief sought

The complainants in this matter are seeking a Section 52 determination. They seek relief which comprises of:

— a declaration that carriers and carriage service providers who have disclosed blocked calling numbers to dial-up ISPs and ISPs who have collected same, have engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct;

- a declaration that carriers must issue a written apology to all holders of silent numbers and other blocked numbers whose numbers have been disclosed;
- a declaration that such individuals are entitled to compensation for loss or damage suffered as a result of the carrier's actions;
- a declaration that carriers must provide a new silent number, without fee, to any holder of a silent number affected by this breach on request;
- a declaration that ISPs who have received blocked calling number information must take reasonable steps to comply with NPP 4 (Data Security), in particular to destroy or permanently de identify blocked calling number information that has been unlawfully collected and/or is not permitted to be used or disclosed under NPP 2; and
- a declaration that ISPs who have received blocked calling number information, if they are not able to destroy or permanently de identify same, must prevent access to databases and records containing such information by staff other than specifically authorised staff who need access to other information in the database or records to undertake a necessary function; and establish an enquiry audit trail on such databases and records so that staff accesses can be recorded and the audit trail can be used in the investigation of any future alleged disclosure or misuse of that personal information.