

## *The Privacy Act 1993 and university disciplinary proceedings: A hypothetical case study?*

Gordon Stewart\*

---

*Since the passage of the Privacy Act 1993, a number of concerns has been raised regarding its application to university practices. That concern was illustrated, for example, by the cessation in 1993 of the publication of Victoria University examination results in daily newspapers, and by the redrafting of the University's enrolment forms to accommodate the perceived effect of the legislation. In the same year, the Academic Registrar at Victoria University asked whether the Act might be applicable to university disciplinary proceedings, and if so, could it impede them? This article addresses those two questions.*

---

### I INTRODUCTION

In a paper presented to Education Administrators in Christchurch in July 1993, Penny Fenwick,<sup>1</sup> Academic Registrar at Victoria University of Wellington, raised the following concern:<sup>2</sup>

The application of the principles of the Privacy Act to grievance and disciplinary cases is a difficult one. On the one hand it is difficult to see how the principles of fairness and transparent justice can be served for the student concerned, without the grievance or disciplinary authority having access to the full range of information relevant to the particular case. On the other hand, the Privacy Act requires that we seek students' (and staff) approval before making that information available to the

---

\* Lecturer, Faculty of Law, Victoria University of Wellington.

1 Penny Fenwick "Protection of Individual Privacy: Issues for Tertiary Institutions in the New Legislation" p 9. Paper presented to the Second Conference of the New Zealand Branch of the Australasian Institute of Tertiary Education Administrators, 8 July 1993, Christchurch College of Education.

2 The point will not be taken up here, but it bears mentioning that to deny a tribunal access to certain information is not, in itself, necessarily a bad thing to do. The general (and acceptable) rules of evidence already accommodate such a practice. Much depends upon the information which is excluded, and the reasons for its exclusion. Would its inclusion have a prejudicial effect which outweighs its probative value? "Prejudicial effect" in that equation may be taken to include an effect upon the general policy goal of protection of personal information ("the privacy of the individual"), while "probative value" relates to the specific goal of a result in the particular hearing. However, Ms Fenwick's point is taken: is it possible for a party to a hearing to effectively block the conduct of that hearing by denying access to pertinent information?

hearing. Is it possible in future that we might see situations in which students (or even staff) seek to swing the scales of justice in their favour by denying a grievance or disciplinary committee access to certain pieces of information pertinent to the case?

The short answer is, probably not. As discussed below, the relevant provisions of the Privacy Act 1993 are so drafted that such a stalemate would not arise.

## II THE PRIVACY ACT

The Privacy Act extends the legislation required to deal with the information industry. It builds on the Official Information Act by taking one type of information covered by that Act - personal information - and providing a specifically developed legislative regime to control the collection, storage, use and disclosure of it. In that process, it extends the scope of control to include private as well as public sector agencies.

The Privacy Act lays down twelve information privacy principles to which those agencies must adhere. It should be noted that only one of them contains entitlements which constitute legal rights enforceable by an individual in a court of law: Principle 6 subcl (1) - the entitlement of an individual to obtain from a public sector agency confirmation that it holds personal information relating to that individual, and (where that information can readily be retrieved) the entitlement to have access to it.<sup>3</sup> Adherence to, and breach of, the other principles is covered by Part VIII of the Act, which deals with complaints. If there is a breach of any of the privacy principles, one may allege that the agency's action constitutes "an interference with the privacy of an individual", the first step in complaints proceedings. "An interference with the privacy of an individual" includes a breach of an information privacy principle which, in the opinion of the Privacy Commissioner:<sup>4</sup>

- (i) has caused, or may cause, loss, detriment, damage, or injury to the individual; or
- (ii) has adversely affected, or may adversely affect, the individual's rights, benefits, privileges, obligations, or interest; or
- (iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.

The complaint would be taken to the Privacy Commissioner,<sup>5</sup> rather than to a court, for investigation.<sup>6</sup> If, upon investigation, the Privacy Commissioner finds the complaint to have substance, the Privacy Commissioner has a duty to seek settlement and an assurance against repetition.<sup>7</sup> If settlement and an assurance cannot be obtained,

---

3 Privacy Act 1993, s 11. Victoria University is a "public sector agency": s 2 definition of that term, and s 2 definition of "organisation", paragraph (a)(ii).

4 Above n 3, s 66.

5 Above n 3, s 67.

6 Above n 3, s 69.

7 Above n 3, s 77(1).

the matter may be referred to the Proceedings Commissioner who may institute proceedings before the Complaints Review Tribunal.<sup>8</sup> The remedies, if the complaint is proven, include a declaratory order, a restraining order, damages, and an order to perform specified acts.<sup>9</sup> In awarding damages, the Tribunal may take into account the individual's pecuniary loss, loss of any benefit (monetary or not), and humiliation, loss of dignity and injured feelings.<sup>10</sup> There are limits on the damages which the Tribunal may award,<sup>11</sup> the exceeding of which would require reference to the High Court, or the agreement of the parties, or abandonment by the parties of the excess.<sup>12</sup>

An individual cannot, then, deny the university disciplinary committee access to certain pieces of information. The individual can claim that a particular practice is a breach of one of the principles, and initiate a complaint accordingly. It is possible that the university disciplinary committee could continue its investigation or hearing until it had a report from the Privacy Commissioner or the Complaints Review Tribunal indicating that the complaint was proven, and therefore that the manner of operation was in breach of the privacy principles. However, in keeping with the spirit of the Act, the preferred course of action would be for the matter to be frozen until that report was made, unless the agency had strong, independent grounds for believing that the practice did not breach any privacy principle (eg a legal opinion or a precedent ruling to that effect).

### III THE APPLICABLE PRIVACY PRINCIPLES

Of the twelve principles, there are six which are likely to have immediate application during a university disciplinary hearing: Principles 1, 2, 3; 9, 10 and 11. The university disciplinary committee should be fully aware of the requirements of those principles in order to avoid possible breaches. The requirements of the other principles should not be forgotten, of course, but it is submitted that their impact on university disciplinary proceedings is less urgent. That some of the principles seem more applicable than others is understandable. This is a piece of legislation designed to cover a particular activity - the collection, storage and subsequent treatment of personal information - but an activity which is performed by a variety of different institutions in a variety of different contexts. The importance of the various principles will vary from context to context. Provisions which might present absolutely no problem in the context of a bank collecting information about its customers, for instance, can nevertheless throw up issues when those same provisions are applied to a context such

---

8 Above n 3, s 77(2), (3) and s 82. The Complaints Review Tribunal is established under s 45 of the Human Rights Commission Act 1977, and the Proceedings Commissioner is appointed under s 7(2A) of that Act. The aggrieved individual is not an original party to the proceedings, and may only be joined in the proceedings if the Tribunal so orders: s 82(5).

9 Above n 3, s 88.

10 Above n 3.

11 Human Rights Commission Act 1977, s 41, made applicable by the Privacy Act 1993, s 89.

12 Human Rights Commission Act 1977, ss 42 - 44.

as that in which a university disciplinary committee operates. If the purpose of the legislation is kept clearly in sight at all times, however, the necessary variations in approach can be made to accommodate those issues.

#### IV CASE STUDY

The application of those principles is best illustrated in context. Take hypothetical student, John Smith. Smith enrolls at Victoria University in 1992. The University is an "agency" for the purposes of the Act.<sup>13</sup> In the process of that enrolment, he gives to the University certain information about himself: name, date of birth, address, ethnicity, academic record - all of which constitutes "personal information" for the purposes of the Act.<sup>14</sup> During 1992, the University accumulates further information about Smith, namely the grades he achieved in the work done during his courses, and at the end of 1992 his final examination results also go into that pool of information. It does not matter whether the University Registry or simply his lecturer or tutor holds that information; for the purposes of the Act, it is personal information held by the agency.<sup>15</sup> Similarly, it does not matter who collects the information; collection by an employee constitutes collection by the agency.<sup>16</sup>

In August 1993, one of Smith's lecturers receives a complaint from another student. The complaint is that Smith is attending lectures while drunk and, because of that, is creating a nuisance.<sup>17</sup> Two other students independently approach the lecturer with the same complaint. The lecturer writes down the details of their complaint.<sup>18</sup>

The lecturer then makes her own enquiries into the matter by raising it with her Chairperson and with Smith's other lecturers. She also asks other class members - perhaps the class representative - for their feelings about the matter. The lecturer records

---

13 Section 2, "Agency", (a).

14 Section 2, "Personal information" means information about an identifiable individual.

15 Section 3(1).

16 Section 4.

17 Victoria University of Wellington Disciplinary Statute, s 2(a). (The Statute is reproduced annually in the VUW Calendar).

18 This is not information "collected" by the agency; it is unsolicited. See s 2 "collect". It becomes, however, information "held" or "obtained" - terms used but not defined in the Act. Presumably the distinction is simply based on the ordinary meaning of those two words: "collected" - which has a statutory meaning - means obtained as the result of soliciting; "held" means in the possession of the agency, regardless of how it was obtained; and "obtained" means brought into possession, whether solicited or otherwise. "Held" and "obtained" are almost interchangeable; their distinction seems to be that "obtained" implies some positive activity on the part of somebody - the agency or an informant - whereas "held" covers information which, one might say, simply emerged as a result of the nature of the institution, eg grades and marks for terms work and examinations. That view of "obtained" has some judicial support: see *Re Woods, Woods v Woods* [1941] St R Qd 129, 137, Philp J (Australia), who felt that "obtain" means to come into possession by one's own efforts or request.

the results of those enquiries, thus adding to the personal information held by the agency and relating to Smith. Finally, the lecturer approaches Smith to discuss, and hopefully to resolve, the problem. Despite such efforts by the lecturer, and later by the Chairperson, Smith's misbehaviour continues. The Chairperson finally hands the matter over to the Convenor of the university disciplinary committee, who decides to hold a hearing. It is inevitable that the university disciplinary committee will wish to traverse the facts of the incidents - which can only be done if the relevant personal information is placed before that committee.

1 *What is the effect of Privacy Principles 1, 2, 3, 9, 10 and 11?*

As a preliminary step in this consideration, reference must be made to section 8: the question of which principles apply depends, to an extent, upon timing. Thus, Principles 1 to 4 only apply if the information was collected after 1 July 1993; Principles 5 to 9 and Principle 11 apply to information held by an agency regardless of when it was obtained; Principle 10 applies only to information obtained after 1 July 1993.<sup>19</sup> Further, Principle 3 does not apply if the printed form used for collecting the information was printed before 1 July 1993 and that form is used no later than 1 July 1995.

Let us assume that the complaints about Smith and the ensuing enquiries occur after 1 July 1993.

2 *Principle 1: Purpose of collection of personal information*

Briefly, this requires that personal information only be collected for a lawful purpose connected with the agency's functions or activities, and that the collection be necessary for that purpose. Disciplining of students is a statutorily recognised function or activity of the University,<sup>20</sup> and a hearing has a lawful purpose connected with that function or activity. Information collected for a disciplinary hearing is information collected for a lawful purpose connected with an activity or function of the University. Indeed, information collected in circumstances where one hopes to resolve the problem without a hearing is, it is submitted, also collected for a lawful purpose connected with the University's function, "good government and discipline of the institution"<sup>21</sup> being wide enough to encompass control other than by way of formal hearings.

As for the second limb of Principle 1, there seems little room for doubt that the collection of pertinent information is necessary for the purpose of fairly exercising discipline within the University, be it exercised by way of formal hearing or by informal discussions.

---

19 On "collected", "held" and "obtained", see n 18 above.

20 Education Act 1989, s 194(1)(a).

21 Above n 20.

## 2 *Principle 2: Source of personal information*

This principle has as its premise the proposition that agencies shall collect personal information directly from the individual concerned.<sup>22</sup> Is the information, obtained from witnesses and relating to the hypothetical Smith incidents, "personal information" (ie, "information about an identifiable individual"; section 2 definition), or is it information about the incidents rather than about the person? If it is the latter, there is no breach of Principle 2. If it is the former, or includes it, then in the Smith hypothetical that basic proposition was both honoured and breached: honoured, in so far as some information was collected from Smith; and breached, in so far as some information was gathered from students other than Smith. The basic proposition is, however, subject to exceptions,<sup>23</sup> and it is submitted that the actions taken in the Smith hypothetical - as regards the possible breach by collecting information from students other than Smith - fall into one or more of them.<sup>24</sup>

## 3 *Exceptions to Principle 2*

Specifically, it could be argued that it is not necessary to comply with the principle because the University believes that compliance would prejudice the purposes of the collection of the information:<sup>25</sup> it is necessary for the information to be sought from the complainants and witnesses, as well as from Smith, if the University is to get a full picture surrounding the incidents. Further, it could be said that (full) compliance is not reasonably practicable in the circumstances of the particular case:<sup>26</sup> it is not impracticable to collect information from Smith, but it is impracticable to collect all the necessary information from him if a balanced picture is to emerge.

There is also a possible argument that the University need not comply, because non-compliance is necessary for the conduct of proceedings before any court or Tribunal (being proceedings that have commenced or are reasonably in contemplation).<sup>27</sup> This argument requires that "any court or Tribunal" include the university disciplinary committee.

Is a university disciplinary committee a court or tribunal at all (in a general sense; Privacy Act definitions to one side for the moment)? It is established and controlled by

---

22 Privacy Act 1993, s 6, Principle 2 subcl (1).

23 Above n 22, Principle 2 subcl (2).

24 The onus of proving the exceptions lies on the defendant: s87.

25 Privacy Act 1993, s6, Principle 2 subcl (2)(e).

26 Above n 25, Principle 2 subcl (2)(f).

27 Above n 25, Principle 2 subcl (2)(d)(iv). Note that the interpretation of "agency" in the Act excludes "in relation to its judicial functions, a court [or Tribunal]": s 2, "agency" (b)(vii) and (viii). This differs from s 6, Principle 2 subcl (2)(d)(iv), which relates to "the conduct of proceedings before any court or Tribunal" - and so includes counsel and parties to an action - rather than to "judicial functions" - which is limited to the court or Tribunal itself. Thus, while the university disciplinary committee might not be an agency, and therefore not subject to the Act, the lecturers involved in our hypothetical - and through them, the University itself - are.

the University's Disciplinary Statute, which in turn has as its source the Education Act 1989.<sup>28</sup> It is a committee of the University's Academic Board, which also has as its source the Education Act 1989.<sup>29</sup> It is not an investigatory body,<sup>30</sup> it operates according to conventional court procedures,<sup>31</sup> it serves a judicial function,<sup>32</sup> and is subject to appeal.<sup>33</sup> It may be said to be a court in all but name. However, it does differ from, say, the District Court or the Disputes Tribunal<sup>34</sup> in certain important characteristics:<sup>35</sup>

... the University legislation does not ... make the distinction, familiar in Court and tribunal proceedings, between those who initiate the proceedings and those who decide. The legislation at least contemplates (if it does not require) the possibility that the one body ... will be substantially involved throughout.

Despite, or because of, that conflation, such committees are as subject to the obligations of fairness and natural justice as are "the bodies, independent from the parties and without a specific interest in the conflict, which provide the normal settings for [such] obligations."<sup>36</sup> It cannot be suggested that the conflation renders the university disciplinary committee any less a court or tribunal. If a university disciplinary committee is subject to the obligations of courts or tribunals, it can be argued that it should benefit from those rights or privileges of courts and tribunals which can be, without strain, applied to it - such as the Privacy Act exemption currently under discussion.

As for whether "any court or Tribunal" includes the university disciplinary committee, the Act is unclear on the point; the terms are not defined. Does the use of upper case "Tribunal" suggest that only the immediately obvious and/or formally nominated tribunals were intended to be included - the Disputes Tribunal, The Tenancy Tribunal, etc? If so, this raises the question of whether the accompanying "court" should be read in that light, and therefore be limited to the "immediately obvious and/or formally nominated" courts (the District Court, the Family Court, etc); or whether it should be contrasted on its lower case distinction, and therefore extend to include any body - not immediately obvious, and not formally nominated - which exercises a judicial function. That latter category would include university disciplinary committee. For the following reasons, it is submitted that "any court or Tribunal" should be interpreted to include any judicial body.

---

28 Education Act 1989, s 194(1)(a).

29 Above n 28, s 182(2).

30 VUW Disciplinary Statute, Note (e) to s 1(g).

31 Above n 30, s 7.

32 Above n 30, s 8.

33 Above n 30, s 10.

34 Also creatures of statute: the District Courts Act 1947 and the Disputes Tribunals Act 1988.

35 *Rigg v University of Waikato* [1984] 1 NZLR 149, 222.

36 Above n 35, 213. The statement was made in the context of the University Council, but applies equally to University committees.

During the second reading of the Privacy of Information Bill (as the Privacy Bill was formerly called), the Minister of Justice, the Hon D A Graham, noted that there were "some obvious exceptions for constitutional reasons - for example, the Bill does not cover the Governor-General or judges in their judicial capacity."<sup>37</sup> If it can be inferred that the Minister was speaking of formal office-bearers, then his words may be taken to support the proposition that "court or Tribunal" is limited to the immediately obvious, formally nominated. On a more general level, however, the Minister later points out that agencies may be exempt from compliance with the collection principles "in special circumstances when the interests of privacy are outweighed by other considerations."<sup>38</sup> The inability of a university disciplinary committee to satisfactorily and efficiently perform its function if it cannot gather information about a person from a source other than that person is a consideration which may be put on the balance across from the interests of privacy. The wider interpretation of "any court or Tribunal" is also supported by the long title, which clearly indicates that this Act, and its principles, should apply to public and private sector agencies: that would encompass the "immediately obvious and/or formally nominated courts" (ie the public system) and any other judicial body (including the less public University judicial system).

There is one other ground on which non-compliance with Principle 2 may be permissible, although it is something of a last resort. Section 54 of the Act provides that the Privacy Commissioner may authorise collection of personal information in breach of Principle 2 if, in the special circumstances of the case, the public interest in that collection, or the benefit (of the in-breach collection) to the individual concerned, outweighs the interference with the privacy of the individual. That authority may be conditional,<sup>39</sup> and cannot, in any event, be given if the individual has refused to authorise the collection of the information.<sup>40</sup> To be in a position to refuse or consent,

---

37 New Zealand Parliamentary Debates, 1993, 14721.

38 Above n 37, 14722.

39 Privacy Act 1993, s 54(2)

40 Above n 39, s 54(3). The relationship between s 54(3), on the one hand, and Principle 2 subcl (2)(b) (and Principle 10 subcl (b), and Principle 11 subcl (d)), on the other, is unclear. "Privacy of the individual" is a general concept, interference with which may be authorised if the public interest in the (principle-breaching) collection of information, or the benefit of that collection to the individual concerned, outweighs the interference with the privacy of the individual: s 54(1) and (2). In either event, however, the individual concerned is given a power of veto; notwithstanding the dominant public interest or the benefit to the individual, the Commissioner cannot grant authority for the (principle-breaching) collection if the individual has refused to authorise it: s 54(3). Principle 2 subcl (2)(b), permits the collection of information in breach of that principle if the individual concerned authorises that breach. Presumably, then, recourse is made to s 54 if the individual has not authorised the breach; if the individual has authorised it, the approach to the Commissioner is unnecessary. However, if the individual has not authorised it, the approach to the Commissioner is pointless, given s 54(3).

Perhaps s 54(3) could be given effect by taking "refused to authorise" to mean "expressly refused to authorise" rather than merely "has not authorised", where the latter could simply be the result of the individual not having been asked to authorise.



the individual concerned should be fully aware of the matter. Full awareness would require that, at least, the individual be advised that the collection is contemplated, why it is contemplated, and that the information would later be made available for rebuttal.<sup>41</sup> Those basic requirements would cover expectations aired during the second reading of the Bill.<sup>42</sup>

The privacy principles included in the legislation make it clear that people have a right to know what information is being collected about them, and also the purpose for which it is being gathered. They also have the right to access that information and to have corrections made.

This process of seeking the Privacy Commissioner's authorisation is seen as a last resort because it makes provision for the hypothetical Smith to refuse to authorise the collection of information other than from him.<sup>43</sup> If that were to happen, then Ms Fenwick's fears would be well-founded. However, it is submitted that the Smith hypothetical is outside Principle 2 for the other reasons covered above.

#### 4 *Principle 3: Collection of information from subject*

The thrust of this principle is that where an agency collects personal information from and about the individual concerned, that individual should be made aware of that

---

The use, in s 54(3), of "has refused to authorise" rather than "has not authorised" supports that approach, and would overcome the difficulty, outlined above, of the relationship between s 54(3) and Principle 2 subcl (2)(b). By that means, it would be possible for the individual not to have authorised the collection (thus the exemption within Principle 2 subcl (2)(b) would not apply) but not to have expressly refused to authorise the collection, and so the Commissioner could still grant the authority. This, however, has the unpalatable result that it may encourage agencies - or the Commissioner? - not to approach the individual for authority, thereby avoiding the risk of a refusal. Besides, given that s 54(3) gives the individual concerned the opportunity to refuse, it can be inferred that the individual is to be made aware of that opportunity.

41 Indeed, more is probably in order. Principle 3 subcl (1)(a) - (e) and (g) provide a comprehensive list of matters which could constitute what should be made known to the individual concerned (for s 54 purposes, if not also for the purposes of the exemptions based on individuals' consents within Principles 2, 10 and 11) if full awareness (and therefore informed consent) is the aim: (a) the fact of collection; (b) the purpose of collection; (c) the intended recipients of the information; (d) the name and address of the collecting agency and the holding agency; (e) the law, if any, under which the collection of the information is authorised, and whether or not the supply of it is voluntary or mandatory; (g) the rights of access to and correction of the information. Indeed, if the points made at n 40 above are sound, and it were thought that the Commissioner should be able to authorise a breach of Principle 2 despite the refusal of the individual concerned, that change could be softened by a requirement that, where practicable, reasonable steps be taken to ensure that the individual concerned is aware of (a) - (e) and (g).

42 Ms L Dalziel, MP, New Zealand Parliamentary Debates, 1993, 15213.

43 See text accompanying n 40 above.

fact, and of the purpose of the collection, the identification of the holder of the information, the rights of access to the information, etc.<sup>44</sup> In the context of the Smith hypothetical, there is little of concern in Principle 3; the University can easily satisfy this requirement without jeopardising the disciplinary proceedings, or the investigation leading up to them.<sup>45</sup>

A question of timing, however, might arise. Subclause (1)(b) requires the individual to be made aware of the purpose for which the information is being collected. In the context of an interview with Smith in the aftermath of the complaint, Smith would, at that time, be made aware of the purpose of the information collection - namely, to determine whether there will be disciplinary proceedings, and for use in those proceedings if they occur. However, prior to the disciplinary incident, the University may have collected information which is now to be used in the disciplinary proceedings, eg at the most simple level, name and address; at a more substantial level, a student's previous academic record, which could now be relevant to disciplinary proceedings for misconduct under, say, the Examination Statute (not the Smith case). When those pieces of information were collected, was the student made aware of the purpose of the collection, ie for possible use in later disciplinary proceedings? Principle 3 prefers the individual to be made aware of the purpose of collection before the information is collected, or, if that is not practicable, then as soon as practicable after the collection.<sup>46</sup> Would "as soon as practicable after the collection" include making the individual aware of the purpose some years after the original collection - eg for use in disciplinary proceedings now being conducted in relation to a recent incident?

Perhaps it could be said that compliance with the principle is "not reasonably practicable in the circumstances of the particular case",<sup>47</sup> but that is debatable. It is practicable in so far as the University can make it clear in all information-collecting activities - whether by printed forms or by interview - that the information may be used for any legitimate University purpose by the branch of the university associated with that purpose (subject, perhaps, to ethical considerations of confidentiality which might put information collected by Student Health Services and Student Counselling Services in a separate category, preventing it being passed on to other branches of the university).

##### 5 *Principle 9: Agency not to keep personal information for longer than necessary*

The heading to this principle is largely self-explanatory. "Longer than necessary" is explained as "longer than is required for the purposes for which the information may lawfully be used."

---

44 Privacy Act 1993, Principle 3 subcl (1).

45 If it were thought that the proceedings might be jeopardised, the exemption permitting non-compliance if necessary for the conduct of court or Tribunal proceedings is repeated in Principle 3 subcl (4)(c)(iv). That, of course, is subject to the discussion above regarding the meaning of those terms.

46 Privacy Act 1993, Principle 3 subcl (2).

47 Above n 46, subcl (4)(e).

This is best approached step by step:

- To what end is the information used (ie what is the purpose of its use)?
- Is that a lawful use? (NB not "lawful purpose", but this may be splitting hairs; lawful purpose may be taken as read.<sup>48</sup>)
- To be used for that purpose, how long need the information be kept?

The answers to those questions depend, of course, upon the type of information involved. For example, Smith's name, address, date of birth, student identification number and academic record constitute information used for the purpose of identifying the student and recording his progress at university. That is a lawful use of that information - indeed, it is essential to the operation of any educational institution. For what length of time need that information be kept, if it is to fulfil that purpose? Arguably, from the moment Smith enrolls until the date of his death. Given contemporary patterns of life-long education, with one or more returns to the same or to other institutions for further studies, there is a need for universities to keep some information indefinitely; both the university and the student may have a continuing use for it. In addition, even if they have no intention of returning to study, graduates may wish copies of their records - maybe for employment purposes or simply out of personal interest. The need for the University to keep the information probably disappears upon the student's death, unless the next-of-kin, executors of the will, historic researchers, or the University itself have some lawful use for it.<sup>49</sup>

Information gathered during a disciplinary hearing - the complaint, the material resulting from the investigation, the notes of the hearing, and the penalty (if any) - falls into a different category. It is not so easily asserted that life-long retention is required for the purposes for which that information may lawfully be used. The purposes for which that information may lawfully be used obviously include the immediate hearing and the imposition (and monitoring) of penalty. How much further they extend is a moot point. Equally unclear is what information may be kept for those extended purposes. For instance, it may be that certain information may be kept beyond the hearing for the purpose of simply recording the fact of the hearing and the penalty imposed. That could be submitted to be a lawful use, provided that the information was not later used in determining guilt or innocence in connection with a later allegation,

---

48 It is possible to have lawful purpose but unlawful use. For example, information collected in order to collate an academic record has a lawful purpose; transferring that academic record from one institution to another without the individual's consent may be unlawful use of that information. It is less likely that there could be lawful use but unlawful purpose - eg a university employee lawfully printing out a student's academic record (lawful use?) with the purpose of subsequently presenting it as his own is probably unlawfully using that information.

49 Use of information about a deceased individual raises some separate issues. "Individual" is defined in the Act as "a natural person, other than a deceased natural person": s 2. In some circumstances, personal information may be given to someone other than the individual concerned - see Principle 11 - but if that would breach a Privacy Principle the disclosure must be authorised by that individual. No mention is made of the next-of-kin or executor being able to give that authority.

but only used in fixing the later penalty. Consequently, all that need be kept for that purpose is the briefest of information: the complaint, the decision, and the penalty imposed. The complainants' statements and any notes of evidence need not be.

The next question is, for how long should that briefest of information be kept if there is to be no breach of Principle 9? There are three options:

- (i) get rid of the information immediately after the penalty has been discharged (ie after the fine is paid or the period of suspension is completed; if no penalty is imposed, the information need not be kept beyond the end of the hearing);
- (ii) get rid of it after a set period of time has elapsed;
- (iii) keep it indefinitely.

The first is the minimum, and would not breach Principle 9. The other two are premised upon it being lawful for a university to keep a record of a student's disciplinary breaches for later reference purposes. It is submitted that this is a lawful use of the information. It is information that could later be relevant for at least two purposes: (i) in fixing a penalty in the event of a subsequent breach of discipline; (ii) in informing the Deans of those Faculties (eg Law) who are, as a matter of routine, called upon to issue a certificate of character in respect of their graduates (eg, those seeking admission to the Bar). The Deans need not refer to the breach in that certificate if they consider the matter irrelevant to the purpose of the certificate (and that will often be the case), but the information should be available to those Deans. (Having said that, it should be noted that there may be other problems raised in this regard by Principle 10, which may result in that information *not* being available to the Deans.<sup>50</sup> Nonetheless, purpose (i) above still stands.)

If retention of information relating to discipline is permissible for the purposes described above, there may nonetheless come a time when the student is entitled to have the slate wiped clean. That is the rationale for the second option - keeping the information for a set period of time only. The setting of that period requires consideration of the following questions:

- after what period of time should a student's previous misdemeanours be forgotten?
- should that period vary according to the type of misdemeanour, eg breach of Disciplinary Statute in contrast to breach of Examination Statute?
- should that period vary according to the gravity of the misdemeanour?

The answers, unless guidance is given by the Privacy Commissioner, are largely policy matters for the University to determine.

---

50 See the discussion under Principle 10, below.

6 *Principle 10: Limits on use of personal information*

This principle states that personal information obtained for one purpose is not to be used for any other purpose, unless any of the exceptions to this principle apply.

The specific issue here is determining the purpose in connection with which information was obtained.<sup>51</sup> Again, much depends on the particular information itself. Name, address, student identification number, etc, all have a fairly general purpose: identification, location, and contact by the university on any matter relating to the student's University activities. Consequently, they may be used only for those purposes. They should not, for example, be passed on by the University to, say, an insurance company wishing to contact all recent professional graduates.

For what purpose is information regarding a disciplinary matter obtained? If it is obtained for the purpose of resolving that specific matter, then it cannot be used for a later disciplinary matter, either for assisting in determining guilt (a practice not recommended, regardless of the Act) or for determining penalty (a common and not ill-conceived practice). Under Victoria University's present statutory system, the information might be used in a concurrent or consequent hearing related to the same incident. For instance, information gathered during a sexual harassment matter, dealt with under the Statute on Sexual Harassment, might be used in consequent dismissal proceedings under the Disciplinary Provisions of the Standard Individual Contract. That "double usage" is covered by the Privacy Act's exceptions to Principle 10,<sup>52</sup> as the purpose for which the information is used (discipline under the Standard Individual Contract) is directly related to the purpose in connection with which the information was obtained (discipline under the Statute on Sexual Harassment, relating to the same incident).

There is some room for manoeuvrability in the interpretation of "purpose" when the University seeks to refer to the information obtained during Smith's incident for a purpose not directly related to that incident. For example, had Smith been a law student, and the Dean of the Faculty was later required to issue a certificate attesting to Smith's good character, could the fact of a guilty finding be conveyed to the Dean (who might use it to refuse Smith his certificate)? It was information obtained for the purpose of, in the first instance, dispensing with the immediate complaint. Could that purpose be widened to, say, "maintaining, in the public eye, a high moral and behavioural standard of Victoria University's students and graduates"? If so, the information would be available to the Dean for use to that end. It is submitted that such an extension of "purpose" is unsafe. It is possible to generalise most purposes in that manner, and in so doing widen immeasurably the use to which information could be put. That, however, is contrary to the spirit of the Act. There will be grey areas on the question of the purpose for which information was obtained, and it is submitted that the University should be guided by the essential purpose of the Act - protection of individual privacy - rather than by the exceptions to the principles.

---

51 "Obtained", not "collected", thus unsolicited information is included.

52 Privacy Act 1993, s 6, Principle 10 subcl (e).

7 *Principle 11: Limits on disclosure of personal information*

This principle limits the circumstances in which an agency may disclose information to any other agency, person or body.

In the Smith case, it is unlikely that disclosure outside the University would be contemplated. It may be, however, if a student were tried in a public court for the same incident. For example, this happened in Wellington in 1992, in a case in which the defendants were charged under section 248 of the Crimes Act for a personation incident which occurred during examinations on campus. That incident also constituted a breach of the Examination Statute. Had a guilty finding been reached under the latter statute, that information may have been released to the District Court on the basis that the University believed it necessary for the conduct of proceedings before any court.<sup>53</sup>

Issues do arise in the Smith case if one section of the University holds information about Smith and another section wishes that information to be disclosed to it. The Act makes it clear that information held by an employee of the University (in the capacity of employee) is deemed to be information held by the University,<sup>54</sup> and that information disclosed to an employee (in the performance of that person's employment duties) shall be treated as having been disclosed to the University.<sup>55</sup> Consequently, information about Smith held by Counselling Services is information held by the University, and information disclosed to the Counsellor (by Smith or another) is information disclosed to the University. Should the Disciplinary Committee wish to use that information, there is no problem about a breach of Principle 11. There may, however, be a problem regarding Principle 10: can it be said that information obtained in connection with the purposes of counselling is information collected for the purpose of a disciplinary proceeding? If not, do any of the exceptions to Principle 10 apply?<sup>56</sup>

Having said that, it must be noted that Principle 11 (and the exceptions to Principle 10) merely permit such disclosure; they do not require it. Thus, information obtained by Counselling Services during the Smith case might be used by the university disciplinary committee, but its release and use cannot be insisted upon by that committee. The principles, and their exceptions, do not demand that some parts of the University release information to others; they simply accommodate it. Professional ethical considerations continue to operate, and they may inhibit the cross-flow of personal information.

---

53 Above n 52, Principle 11 subcl (e)(iv).

54 Above n 52, s 3(1).

55 Above n 52, s 4.

56 Depending upon the facts of the case, possibly subcl (c)(iv) - non-compliance is necessary for the conduct of proceedings before any court or Tribunal; or subcl (d)(ii) - non-compliance is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another individual; or subcl (e) - that the purpose for which the information is used is directly related to the purpose in connection with which it was obtained.

## **V CONCLUSION**

The University can operate within the Privacy Act 1993. However, as said, it is a piece of legislation designed to cover a variety of institutions; it is not tailored to the University environment, nor to the even narrower context of disciplinary proceedings. There is a definite need for a Code of Practice to be issued under Part VI of the Act, a Code which would either relate only to Victoria University or to universities or tertiary institutions as a group. Meanwhile, the Act fulfils the functions of protecting individual privacy, and does not appear to obstruct the University's disciplinary proceedings in the process.