

Privacy Impact Assessment

In Respect of a Proposal to Develop a
National Student Index Number

Prepared for the Ministry of Education
by

John Edwards
Barrister and Solicitor

October 2000

Table of Contents

SUMMARY OF KEY POINTS.....	3
OBJECT AND SCOPE OF PRIVACY IMPACT ASSESSMENT	6
BACKGROUND.....	7
MINISTRY OF EDUCATION	7
NZQA	7
DESCRIPTION OF THE PROPOSAL, AND THE POLICY RATIONALE FOR IT	8
POLICY PROBLEM.....	8
THE PROPOSAL	9
DOES THE PROPOSAL INVOLVE THE COLLECTION OF ANY NEW PERSONAL INFORMATION?	11
CONSULTATION	12
PRIVACY ISSUES.....	13
PRINCIPLE 1	13
PRINCIPLE 2	13
PRINCIPLE 3	14
PRINCIPLE 4	14
PRINCIPLE 5	15
PRINCIPLES 6 AND 7.....	16
PRINCIPLE 8	17
PRINCIPLE 9	17
PRINCIPLE 10	17
PRINCIPLE 11	18
PRINCIPLE 12	19
<i>Evolution of NSI into a de facto identity number/ card.</i>	<i>21</i>
<i>Facilitates other breaches.</i>	<i>22</i>
BROADEN THE SCOPE OF THE SCHEME – SUBJECTS	23
BROADEN SCOPE OF SCHEME – AGENCIES.....	23
EXTENSION OF SCHEME - INFORMATION CAPTURED.....	24
TOWARD A NATIONAL IDENTIFIER	25
PRIVACY GAINS.....	27
SINGLE COLLECTION/VERIFICATION	27
SECURITY OF TRANSMISSION	27
GREATER TRANSPARENCY AND ENHANCED ABILITY FOR STUDENTS TO HAVE ACCESS TO THEIR OWN RECORDS, AND ENSURE THAT THEY ARE ACCURATE	27
IDENTIFICATION SUPPRESSED FOR RESEARCH AND ANALYSIS PURPOSES	28
PRECEDENT	29
INTERNATIONAL PRECEDENT	29
DOMESTIC PRECEDENT	30
ALTERNATIVE MEANS OF ACHIEVING THE POLICY OBJECTIVE.....	33
NO UNIQUE IDENTIFIER.....	33
USE OF AN EXISTING NUMBER - IRD/DRIVERS LICENCE/COMMUNITY SERVICES CARD	33
USE OF AN EXISTING NUMBER - RECORD OF LEARNING NUMBER.....	34
VOLUNTARY ADOPTION OF NUMBER.....	34
OPTIONS TO FACILITATE THE SCHEME	36
LEGISLATION	36
CODE OF PRACTICE FOR THE EDUCATION SECTOR	36
A UNIQUE IDENTIFIER CODE OF PRACTICE	36
OVERALL CONCLUSIONS	38

Summary of Key Points

Key Point 1

This is an independent assessment of the actual and potential privacy impact of the NSI proposal, taking into account local and international precedents.

Key Point 2

At the moment government receives detailed information about students from tertiary providers and from students themselves.

Key Point 3

It is very difficult for government to analyse the information it receives at the moment to see how students move through post compulsory education, and therefore what government's policy response to different pathways would be.

Key Point 4

Description of proposal

In order to better organise the information currently collected, and to allow better analysis of that information, it is proposed that every post compulsory student is allocated a single number, the National Student Index Number.

That number will be associated with demographic information about the student.

The returns that providers are now required to make, will be made, using the number, to the Tertiary Data Warehouse.

No one, except for the database administrators will have access to information on the Tertiary Data Warehouse in a way that could lead to any individual being identified.

Key Point 5

Apart from the number itself, the NSI proposal does not involve the central collection of any more personal information than is currently collected.

Key Point 6

The proposal does not breach any of information privacy principles 1 -11 of the Privacy Act 1993.

Close attention would need to be paid to the following principles in the implementation of the scheme.

- Principle 3 - to ensure that students are aware of the purpose of collection of their information, and who will hold it.

- Principle 5 - to ensure that the new system is protected by adequate security safeguards.
- Principle 10 - to ensure that the information connected with the NSI is used only for the purposes for which it was collected.

Key Point 7

- The proposal would breach information privacy principle 12(2).
- It does not automatically follow that this would have an adverse effect on individual privacy. The use of a number does not inherently lessen individual privacy
- The fact that the scheme might be extended does not automatically mean an adverse impact on privacy will result.
- One of the greatest concerns internationally and locally with the use of unique identifiers is that they might grow to become de facto identity numbers.
- Universal identity numbers are viewed with suspicion and anxiety by privacy advocates.
- Given the intended coverage of the proposal (post compulsory students) fears of the NSI becoming a "de facto national identifier" may not be well founded.
- Although the proposed system may be seen as relatively benign from a privacy perspective, there is scope to extend the scheme in ways which might have a more significant privacy impact.

Key Point 8

There are some privacy gains from the proposal:

- It may reduce the number of times students are required to give and verify personal information
- The information may be more secure than is currently the case
- Students may have easier access to their own information
- Identifying information can be suppressed when the information is analysed for policy purposes.

Key Point 9

- There are examples of the use of unique identifiers for education in other jurisdictions.
- These do not appear to have raised significant privacy concerns in those communities.

Key Point 10

- Unique identifiers have been permitted in other areas in New Zealand, most relevantly in the Health sector, and the justice sector. These have been allowed by codes of practice issued under the Privacy Act by the Privacy Commissioner.

- Those codes were not new policy proposals, but enabled existing practices to continue under the Privacy Act 1993.
- Those codes relate to more sensitive information than information about participation in post compulsory education.

Key Point 11

The alternative means of achieving the same policy objective, namely;

- No Unique identifier
- Use of an existing number- IRD/Drivers licence/Community Services Card
 - Record of Learning Number
- Voluntary adoption of number - might be less efficient, have a greater impact on privacy or both.

Key Point 12

The proposal cannot proceed under the existing law. The options to enable the project to proceed include:

- Enact an express legislative provision
- A code of practice under the Privacy Act for the Tertiary Sector
- A code of practice under the Privacy Act covering just the NSI

The main advantages of a code just addressing the NSI is that it could:

- Prescribe the permitted scope of the scheme
- Be subject to the oversight of the Privacy Commissioner
- Provide a real remedy for privacy breaches.

Object and Scope of Privacy Impact Assessment

This privacy impact assessment has been commissioned by the Ministry of Education. Its object is to bring to the forefront, and examine the privacy implications of a proposal to assign a unique identifier to every post compulsory education student.

There is no standard definition of a privacy impact assessment, and no common form for its contents. In New Zealand, the following definitions have been suggested;

“PIA is a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal.

“PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.”¹

This PIA;

- describes the current information flows and requirements of the various participants in the tertiary education sector;
- describes the impetus for and nature of the NSI proposal
- assesses the actual and potential impact on privacy of the proposal
- considers the legal implications of the proposal
- discusses international literature on privacy and education records
- considers other unique identifiers in New Zealand
- assess alternative means of achieving the policy objectives

This report has been commissioned in the design stage of the Tertiary Information Project, and will be available to any individual or organisation wishing to comment on the proposal.

Some consultation has already been undertaken by the Ministry of Education in respect of the NSI proposal, and where relevant, that feedback obtained in that process has been incorporated into this report.

The object of a PIA is not to “sell” an idea which may have adverse privacy implications, but to objectively consider the relative costs (in terms of the adverse effect on privacy) so that the benefits (in terms of the policy objective of the proposal) can be weighed against them by policy makers, the Privacy Commissioner and interested parties.

This report does not make recommendations, but points out some of the privacy concerns, evaluates them against local and international experiences, and suggests some means by which privacy concerns could be addressed if the proposal is to go ahead.

Key point 1

This is an independent assessment of the actual and potential privacy impact of the NSI proposal, taking into account local and international precedents.

¹ Blair Stewart, “Privacy Impact Assessments”, 3/4 *Privacy Law & Policy Reporter* (July 1996) 61.

Background

Ministry of Education

Prior to 1998 government funding for tertiary education providers was based on the number of "equivalent full time students" (EFTS). Each provider was required to submit returns of EFTS to the Ministry of Education three times per year. The returns were entered into spreadsheets, and funding calculations were made to determine the amount of funding each provider would receive.

This information was given to the Ministry by the providers on an individualised student basis. In addition to the returns required for funding calculations, numerous student statistical returns were required to be sent by each provider to the Ministry.

In 1998 the Ministry of Education conducted a review of funding of tertiary education. The government agreed that the sector should move to a single data return for funding and statistical information to and from tertiary providers.

Each tertiary provider now sends its returns with reference to a unique identifier comprised of student number (the number assigned by the provider), and the first four letters of the students name.

This information is sent either by email or by disk.

NZQA

NZQA maintains a "record of learning". This record comprises each student's individual demographic details, together with results of study.

NZQA awards national certificates and national standards, and therefore requires student level information on courses completed in order to establish that a student has completed the necessary courses to qualify for a certificate or award.

Key Point 2

At the moment government receives detailed information about students from tertiary providers and from students themselves.

Description of the Proposal, and the Policy Rationale for It

Policy Problem

At present government does not have good information to measure the efficacy of various interventions in the tertiary education sector, and has no way of knowing the pathways students follow from secondary national qualifications through different tertiary providers.

Tertiary education is provided by state funded tertiary providers, and private tertiary establishments. In the course of a student's tertiary career, he or she may access a range of different tertiary providers, for example, moving from a TOPS course provided by Skill NZ, through to other courses funded by government.

Without having information about the patterns showing which students access the different courses, it is very difficult to assess which courses have been successful, in terms of providing improved access to tertiary education. In particular, there is no way to assess how different policy interventions work with different demographic groups such as older students, Maori, and Pacific Island students.

There are many examples of the limitations of the current data management systems in supporting research, and in informing policy analysis. One recent example involved a report sought by the Minister of Education on the retention rates of Maori and Pacific Islands students in tertiary education. The advice to the Minister contained the following passages;²

"Limited information is available on retention at tertiary institutions by ethnicity.." Students leaving a particular institution in any one year may move to another institution or pick up their studies after a break. The multitude of pathways to achieving a qualification make the concepts of retention and completion difficult to pin down....(at para 6)

The percentage of population attending tertiary education cannot be measured between census years because of the lack of population data by ethnicity. (at para 11)

While the research that can be completed produces better than pure speculation, the research effort is considerable, and the results are subject to a higher than desirable margin of error.

The way in which the information is provided to the central agencies at the moment also means that it is very difficult to get up to date information about changing patterns of study. Information must be handled and reconfigured several times to deal with the funding requirements, and different research objectives.

² ["Research On Student Loan Scheme And Maori And Pacific Islands Retention Rates In Tertiary Education" Briefing Paper to the Minister of Education 26 January 2000](#)

There are other ways in which research can be conducted, which would not involve the use of a unique identifier. Some of these are discussed in further detail in the "Alternative Means Of Achieving The Policy Objective" part of this report.

Key Point 3

It is very difficult for government to analyse the information it receives at the moment to see how students move through post compulsory education, and therefore what government's policy response to different pathways would be

The Proposal

As part of the government's consideration of the funding review, Cabinet also approved the scoping of a National Student Index number, to facilitate the information requirements of the new system.

The proposal involves the maintenance of a two databases of student data. The first is the National Student Index Number database, and would contain demographic data about each student (age, and gender) together with information about the provider through which they are accessing tertiary information.

At this stage, it is proposed that the following information will be captured;

- NSI Identifier (unique identification number assigned)
- Family Name
- First Given Name
- Second Given Name
- Third Given Name
- Alternative Family Name (a surname that the student is also 'known as')
- Alternative First Given Name
- Alternative Second Given Name
- Alternative Third Given Name
- Date of Birth
- Gender
- NZ Resident Status (Identifies if the student is a permanent resident in NZ or not)
- Proof of identity, e.g. birth certificate number (and how it was sighted)
- Preferred Name Indicator (given name a student prefers to be known by)

Every post-compulsory student would be assigned an NSI number. Post-compulsory students include school students working toward a National Certificate of Educational Achievement ("NCEA").³

Tertiary providers would be required to check whether each enrolled student had an NSI number on the Ministry database, and if so, would be required to use that number for enrolment purposes. If the student did not have an NSI number, the provider would be

³ The NCEA will replace school Certificate from 2002, 6th Form Certificate from 2003, and Bursary from 2004

required to assign a number, which would then be that student's number for all future enrolments.

A provider assigning or checking a number would have direct access only to this core demographic data. Later, when returns are made to the Ministry and NZQA, they will be made with the number. In their returns to the Ministry, the provider will be required to forward only the same information as is currently provided. This information would be kept in a separate database. It is anticipated that this separate database would consist of the NSI number and information about the student's enrolment such as course of study, provider, and qualification obtained.

The second database would be the Tertiary Data Warehouse. This would store all the information returned to the Ministry by the providers including further demographic information such as ethnicity. This information would be stored with reference only to the unique identifier, and would not contain any information which could identify any individual student. The unique identifier will be invisible to any user of the warehouse.

The TDW is a multi-dimensional database, or 'cube' where data is plotted on various axes to enable all the possible different combinations of the data to be viewed. The TDW is a read-only, snapshot copy of the data that is processed in operational systems, such as the Tertiary Funding System. Once in the TDW the data can be manipulated to allow for queries, reporting and analysis.

The reports that are currently made to the Ministry with a range of identifiers (including student's name or the provider's unique identifier) would then be made to the Tertiary Data Warehouse using the NSI number.

NZQA would be responsible for assigning NSI numbers to secondary school students registering for national qualifications. At present the schools forward returns to NZQA, which assigns a unique identifier. The NSI number could be used to link this data with other data about students' further studies for the purposes of Ministry and NZQA policy developments.

The separation of the NSI database from the Tertiary Data Warehouse is a key part of the proposal. The separation means that it will be impossible for policy analysts or researchers to "connect" information from the TDW with the identifying demographic information associated with the NSI. There is no proposal to store detailed data about the individual student's experiences, courses of study, or academic record (apart from the NCEA data) in connection with the NSI. This substantive information will be kept only on the Tertiary Data Warehouse. Policy makers and researchers would be able to interrogate the Tertiary Data Warehouse by fields of data, but would not see an individual's name attached to any given record.

Providers too, will be prevented from access to the Tertiary Data Warehouse in any way that would enable them to 'reconnect' information stored there with the name associated with an NSI number. A "Phase II" of the project would enable providers to have access to the warehouse, but only to obtain aggregated information, not in identified by NSI number.

Researchers will be able to analyse data selected from the warehouse by any combination of the variables stored there. For example, to find out the subsequent study patterns of Pacific Island students between the ages of 25 and 35 who enrolled at Whiterea Polytechnic in a given year, the researcher would select each variable, and subsequent enrolments or qualifications, and the warehouse would produce a report for further analysis. The report might show the total numbers of students who did not engage in further tertiary education, those who attained university degrees, and those who took up study in different regions.

The report would not contain identifying information or even the NSI number. The NSI number is necessary only to collate the information, not to report it.

The proposal does impact on one other database. The NZQA "record of learning" database which now records students demographic details, and qualifications achieved towards the National Qualifications Framework, and provides students with ready access to their own progress towards qualifications, would be changed by substituting the NSI number, for the "record of learning number". This change would not alter the way in which that database is organised, nor would it change the information stored on it. The fact that the NSI number is used, would not given any greater access to anyone, to the Tertiary Data Warehouse.

Key Point 4

Description of proposal

In order to better organise the information currently collected, and to allow better analysis of that information, it is proposed that every post compulsory student is allocated a single number, the National Student Index Number.

That number will be associated with demographic information about the student.

The returns that providers are now required to make, will be made, using the number, to the Tertiary Data Warehouse.

Does the proposal involve the collection of any new personal information?

No. Tertiary providers are currently required to collect demographic information about all enrolled students, and to furnish returns of that information to the Ministry of Education.

The new feature of this proposal is the assignment of a unique identifier that will apply to all students in the tertiary sector.

Key Point 5

The NSI proposal does not involve the central collection of any more personal information than is currently collected.

Consultation

In developing the proposal to date, the Ministry has consulted with;

- Individuals from Universities, Colleges of Education, Wananga, Polytechnics and Private Training Establishments (and their national associations have been provided with relevant documentation and progress updates).
- NZQA
- Skill NZ
- E-Government Project Team
- Student Associations (Association of Polytechnic Students, New Zealand University Students Association, Te Mana Akonga)
- Statistics NZ
- Careers Service (has been provided with relevant documentation and progress updates)

Privacy Issues

This part of the paper considers the proposal's actual and potential impact on privacy.

The Privacy Act 1993 requires all agencies to comply with 12 information privacy principles. These principles govern the way in which agencies collect, store use and disclose personal information.

The main thrust of this report is on the issue of the creation and assignment of unique identifiers. Unique identifiers are dealt with under information privacy principle 12. For the purposes of this exercise, it is useful to consider the privacy implications of the proposal with reference to all the information privacy principles.

With the exception of principle 12, the following text paraphrases the information privacy principles from the Act, and should not be taken as a full or accurate record of the law.

Principle 1

Principle 1

Personal information should not be collected unless it is necessary for a lawful purpose connected with a function or activity of the agency.

Once a number has been assigned to a student, that number may be collected by subsequent education providers. Apart from the number itself, the NSI proposal does not involve the collection of any new information from individual students. As such, the only issue arising under this principle is whether it is legitimate for the Ministry, NZQA, and tertiary providers to 'collect' the NSI from students and/or the NSI database once it has been assigned.

Given that the purpose of the scheme is dependent upon the common use of the NSI number, each agency involved would have a legitimate reason to collect that number.

Principle 2

Principle 2

Information should be collected directly from the person concerned.

A number would only be assigned where the individual student had provided the demographic data, and had verified that data with identity documents.

In all cases therefore, the core data would be collected only from the individual.

Principle 3

Principle 3

An agency collecting personal information should ensure that the individual concerned is aware of the collection, of their rights in respect of that information, and of the agencies that will hold or have access to the information.

Responsibility for compliance with this principle is on the agency that collects personal information directly from the individual concerned.

Although neither the information required, nor the agencies that will receive it under the proposal will change in any way, it is desirable that some explanation of the scheme is made to all enrolling students.

One of the criticisms of the National Health Index Number is that very few consumers of health services are aware of its existence or scope. Given the emphasis in the Privacy Act on openness in relation to personal information, it is highly desirable that good information is available to all participants in the tertiary sector as to the nature and purposes of the NSI.

Because the Ministry of Education will not have access to the name and address of the student in the Tertiary Data Warehouse, it will not be possible for the Ministry to write to each student explaining the existence and nature of the NSI when a number is assigned.

If the proposal is to proceed the Ministry could require, through its service level agreements with providers, that each one send a standard form letter to the student when the number is assigned. This statement should be developed by the Ministry and explain what the number is for, how it is used, and who has access to both the demographic information associated with that information and with the statistical information in the database. That letter, in order to comply with information privacy principle 3, should also explain that the use of the number, and the supply of the core demographic information to be associated with it is mandatory.

It will be important for the providers to distinguish between the information privacy principle 3 statement provided in connection with the NSI, and that provided in connection with the other information the collected in the course of enrolling a student. For example, all providers collect information about ethnicity, however, the supply of this information by students is always voluntary.

Principle 4

Principle 4

Agencies should not collect personal information in ways that are unfair unlawful, or by means which are intrusive.

Nothing in the proposal suggests that there will be any risk of breach of this principle.

Principle 5

Principle 5

Agencies are required to protect personal information with reasonable security safeguards.

The security specifications will have to be sufficiently stringent to protect the integrity of the data, both from unjustified browsing by authorised individuals, and from unauthorised access, and corruption by hackers.

The technical specifications of the proposed system are not completed, and a document such as this may not be the most appropriate place for a discussion of technical security measures. However, some of the proposed features to protect the integrity of data, and to prevent unauthorised access include the use of Public-key Infrastructure (PKI). PKI is a combination of software, encryption technologies and services that enables enterprises to protect the security of their communications and business transactions on the Internet by;

- Authenticating identity. Digital certificates issued as part of PKI allow individual users, organisations and web site operators to confidently validate the identity of each party in an Internet transaction.
- Verification of Integrity. A digital certificate ensures that the message or document that the certificate "signs" has not been changed or corrupted in transit online.
- Ensuring confidentiality. Digital certificates protect information from being able to be read if intercepted during internet transmission
- Authorising transactions. With PKI solutions, access privileges for specified online transactions can be controlled
- Support for nonrepudiation. Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction, such as a purchase made on a web site.⁴

Procedural steps such as regular computer "prompts" reminding users of security and privacy issues, and random "audits" of access, combined with standards in administrative documents such as service agreements and memoranda of understanding, can reduce the risk of abuse, and security breaches.

One of the security concerns generally raised by new database proposals is the ability of individuals with authorised access to the system to undertake unauthorised searches, or to have access to information not directly relevant to the task legitimately to hand. Where possible, opportunities for "browsing" records should be minimised in the system design. The NSI system would be open to this sort of abuse at the level of the providers assigning or verifying NSI number. To some extent, the potential for abuse

⁴ Security details are extracted from Ministry of Education National Student Index - Initial System Implementation Options.

is most appropriately dealt with in the processes followed and supervision at provider level.

Software is available that can inhibit the potential for unauthorised browsing, by requiring only individual searches. Such systems report back a single name when an enquiry is made, rather than a screen full of close matches for the operator to then scroll through. It is intended that searching software that limits the information that can be seen in response to a specific query is used with the NSI database.

Principles 6 and 7

Principles 6 and 7 Individuals are entitled to have access to, and to correct their personal information.
--

In this respect the proposed system has potential to be more transparent than the existing system..

A centralised data system enables the student to ensure that subsequent users of information will not have access to incorrect information. Under the current system, it may be very difficult for a student finding an error to have confidence that the error has not been perpetuated in other record systems. If a student wishes to change or update any of the demographic information recorded on the NSI database, he or she will be able to do so easily, and with confidence that the record has been permanently changed.

Given that there will be no direct link between the data warehouse and the NSI database, it will not be possible for students to readily access the personal information stored there. There are two legal consequences of the manner in which information is stored on the Tertiary Data Warehouse. First, it could be argued that the information stored there is not about an "identifiable individual", because no identifying information is stored there, and that it is collected in one place purely for the purposes of statistical analysis and research. This would be a debatable assertion, given that there must be a mechanism to extract data with reference to one unique identifier, and then ascertain the identity of that person through the NSI database.

However, the fact that there are considerable technical impediments to reassociating the information stored in the warehouse with information that enables an individual to be identified might well mean that the information is "not readily retrievable", and therefore placed outside the reach of the right of access provided by information privacy principle 6.

On its face this consequence is a privacy adverse outcome, as an individual's right to know what information is held about him or her is a cornerstone of privacy regulation around the world.

However if the data is used only for statistical purposes the real impact of difficulty in each individual gaining access to the data should be negligible.

Paradoxically, if the system were designed to facilitate such access, and thereby achieve an apparent privacy benefit, the risk would be that it would be easier for administrators,

researchers, and others with access to the systems to abuse the privacy of subjects by reassociating the demographic, identifying NSI data, with that held in the warehouse.

Principle 8

Principle 8

An agency should ensure that personal information is correct accurate, complete, up to date and not misleading before using it.

As mentioned above, the core data needs only to be entered into the system once, thereby reducing the possibility of errors with multiple reentry.

Students will be able to ensure that the information is accurate, and if not to ensure it is updated.

There would seem to be nothing in the proposal that would indicate a risk under this principle.

Principle 9

Principle 9

An agency should keep personal information only for as long as necessary.

The intention of the NSI is to create a "longitudinal record" of students' interactions with tertiary education providers.

Existing paper and electronic records are covered by the Archives Act. The coverage of the Archives Act means that principle 9 has limited relevance to public sector agencies.

There are no plans to purge either the NSI database or the Tertiary Data Warehouse. Given the policy intent of information privacy principle 9, this can be seen as privacy adverse, as the records may be kept for longer than are relevant.

The Ministry's policy view of this question is that the intention is to provide for a record of lifelong learning, and as such individual records may be retained for decades after a student has had his or her last interaction with post compulsory education.

The Ministry's policy objectives might well justify an open ended retention of data. Having data accumulated over decades might well enable better analysis of long term outcomes of tertiary education.

Principle 10

Principle 10

An agency that holds personal information should use it only for the purpose for which that information was obtained.

While there is nothing to suggest that the scheme could not be undertaken in compliance with this principle, concerns over alternative uses for information, once that information has been organised in a centrally held, and readily retrievable manner are likely to be at the root of any privacy concerns surrounding the proposal.

The purposes for which the information is to be used are at this stage, clearly defined. That is, the information derived stored and organised with reference to the NSI is to be used in the same way the information is currently, for the analysis and development of policy.

The issues of concern about "function creep", that is, the development of new uses for the personal information, are considered in more detail below.

It is accurate to say that based on the proposal as outlined to date, the development and use of the NSI would not in itself breach principle 10. If any of the agencies with access to the system were to use the information for new purposes, any person affected would be entitled to make a complaint of breach of this principle.

If there is a concern about compliance with this principle, it is more to do with potential, than proposed uses of the student information. It is not possible to consider the full range of potential uses of the data, and to determine the extent to which they would comply with, or reach this principle.

Principle 11

Principle 11

Agencies should not disclose personal information unless the disclosure is one of the purposes for which the information was obtained.

Again, the fact that the NSI does not create any new information flows means that there is no breach of this principle inherent in the proposal.

The fact that a central database is established however does always increase the risk of an improper disclosure of information. Unscrupulous system operators in other databases have used official data as a means of gaining private income through selling information to (among others) debt collectors. There may be limited scope for such activities in relation to the NSI, as it is not proposed that current contact details (either address or telephone number) are to be included.

Key Point 6

The proposal does not breach any of information privacy principles 1 -11 of the Privacy Act 1993.

Close attention would need to be paid to the following principles in the implementation of the scheme.

- Principle 3 - to ensure that students are aware of the purpose of collection of their information, and who will hold it.

- Principle 5 - to ensure that the new system is protected by adequate security safeguards.
- Principle 10 - to ensure that the information connected with the NSI is used only for the purposes for which it was collected.

Principle 12

Principle 12

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of section 8 of the Income Tax Act 1976.

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

Parts 1, 3 and 4 of this principle are not an impediment to the development of the proposal.

The 'necessity' for the assignment of the identifier in terms of information privacy principle 12(1) is defined in the section "Policy Problem", above. If the proposal proceeds, providers will be required by the Ministry to assign the number in order to claim EFTS based funding in respect of a student.

As the NSI will also replace the "record of learning" number in the NZQA database, students will 'need' an NSI number in order that their progress toward qualifications on the NZQA National Qualifications Framework is maintained.

In relation to information privacy principle 12(3), it is proposed that the process of assignment will require some form of verification, such as by the presentation of authenticated documents of identity. No standard verification procedure has yet been developed by the Ministry of Education.

However, the proposal must be in breach of information privacy principle 12(2), because once a tertiary provider has assigned an NSI to a student, every other provider that student enrolls in will assign the same number.

It should be noted at this point that a breach of a privacy principle is not taken in the law automatically to mean that a person's privacy has been breached.

The Privacy Act sets a threshold for liability in respect of "interferences with privacy". Under section 66, an action is only an interference with privacy where the action involves a breach of one of the information privacy principles, *and* that breach causes some harm, loss damage, adverse effect on benefits, significant humiliation, significant injury to feelings or significant loss of dignity⁵. That is not to say that if the Ministry is confident that despite noncompliance with the principle no harm is likely, it is entitled to proceed. All agencies are required to comply with the principles, and government especially, must uphold the rule of law.

However a discussion of section 66 demonstrates that in law, as well as in practice it does not automatically follow that the fact that the proposal would be in breach of information privacy principle means that privacy would be breached under the scheme.

In order to get at the actual impact on privacy it is necessary to understand the policy objective behind information privacy principle 12, and then to analyse the proposal with reference to this objective.

Dr Paul Roth of Otago University has attempted to classify the different objectives represented by information privacy principle 12. His classification has been adopted, for descriptive purposes, by the Privacy Commissioner⁶. Dr Roth suggests four distinct features. They are summarised by the Privacy Commissioner as follows;

"Accuracy and use of personal information

Principle 12 is in response to concerns about the accuracy and use of personal information where a unique identifier is assigned. In particular, the risk is that if one unique identifier is used for a wide variety of authentication and identification purposes in both the public and private sectors this would amount to a de facto universal identifier. De facto universal identifiers have been viewed as unsatisfactory because they are unreliable and a threat to individual privacy.

Technical reliability

Because a de facto universal identifier is not designed to be a true universal identifier it can be technically unreliable and vulnerable to falsification or error.

Facilitation of privacy breaches

Any unique identifier that facilitates the exchange and matching of personal information held by different agencies and within different record systems is perceived to be a threat to privacy. This may also lead to the socially undesirable practice of compiling composite profiles of individuals which may

⁵ The one exception to this rule is in respect of breaches of information privacy principle 6 and 7. Where an information privacy request is not dealt with according to law, the agency concerned may be liable whether or not any harm ensues.

⁶ Necessary and Desirable Privacy Act 1993 Review 1998 Office of the Privacy Commissioner p 88

lead to any and every aspect of their lives being open to potential scrutiny by governments or private enterprise.

National Identities by increments

The fear is that a de facto universal identifier emerging could ease the way towards a requirement of a national identity card or document. This brings with it a variety of concerns about inaccuracies and such like and the constraint on liberties. For some the idea of a national identity card is equated with mechanisms of a Police State where identification can only be authenticated and entitlements made on presentation of the card. Loss, lack or confiscation of such a card makes the individual a "non-person".

It is important to observe that none of these rationales for the regulations of unique identifiers point to any *inherent* privacy breach by the use of unique identifiers. This is significant. From this it might be surmised that from a policy perspective, it does not necessarily follow that the use of unique identifiers will result in a breach of privacy, in the same way as, say, the use of an information matching programme will.

The privacy breach is potential, and contingent upon subsequent uses of the number, and the technology supporting it. This point is underscored by The Privacy Commissioner of Canada. Commenting recently on a proposal to assign a unique identifier to medical student residents and physicians across Canada, he summarised his concerns in the following terms:

“ past experience has shown that personal information in an accessible form is subject to "function creep". Despite protections built into any system, the mere existence of the number will prompt creative and unrelated uses. Once all medical students and physicians are issued a number, there is a real likelihood of unauthorized access to their personal information using this number as the key. And when many organizations use any common identifier, the possibility increases that information from disparate sources will be combined into comprehensive profiles. Unique personal identifiers and powerful technologies may appear to solve immediate administrative problems but they pose long-term threats to individuals' privacy, a fundamental value in a democratic society.”⁷

The assignment of a unique identifier here, and in Dr Roth's analysis is a stepping stone to negative privacy impacts, and may facilitate privacy unfriendly practices.

It is useful to consider the NSI proposal with reference to Dr Roth's categorisations, and the concerns expressed in Canada.

Evolution of NSI into a de facto identity number/ card.

The proposed NSI is not universal. It would be applied only to post-compulsory students. Given that a substantial majority of the total population do not access tertiary education, the likelihood that the NSI could be a stepping stone toward a universal identifier is not be significant. Compared with the proportion of the population that has IRD numbers, the coverage of the NSI will be very small.

⁷ Privacy Commissioner of Canada Annual Report 1999/2000

Facilitates other breaches.

It is true that the NSI will make the transfer of information between central agencies (Ministry of Education, NZQA, and Skill NZ), and tertiary providers easier, the proposal does not increase the amount of information which already flows between those agencies.

One feature which is different is that tertiary providers will be able to access limited details of the other providers an enrolling student has attended. The core NSI database will record the name of the provider that assigned the number, and the provider that last updated the record. This does not however amount to an increase in the information that provider will normally require. Details of previous study are sought from students already for the purposes of cross crediting papers, or ascertaining that prerequisite requirements have been met. For a student that enrolls initially with one provider, and then undertakes study with another for a course that is unrelated, or does not require any cross credit or prerequisites, the second provider will have access to a small amount of information that they but for the NSI scheme would not necessarily have been aware of, or had any need to collect.

At present, each student must give core demographic and identifying information to each agency with which he or she enrolls. As designed, the system would not increase the amount of personal information required by each provider, or the amount shared between central agencies and providers.

The system would not permit any greater level of information matching, than is currently open to the providers concerned. Were any proposal to use the NSI system for an information matching proposal which could have an adverse impact on individual students, authorising legislation would be required under the Privacy Act.

The problem of potential "function creep" is slightly different, and is discussed further below.

This exercise suggests that the actual privacy impact of the proposal appears negligible. However, given the emphasis in the literature on *perceptions*, and the *potential* for adverse privacy effects the debate on the net utility of the proposal once privacy concerns have been taken into account would be best served by an open discussion of ways in which the scheme might be extended.

Much anxiety about central aggregations of personal data is concerned with the "big brother" factor, a sense that even if the intentions of the systems designers are worthy, and the those responsible for maintaining the system are trustworthy, another government, or another administration may approach the efficiently organised central database with less honorable intentions.

The speculative nature of such objections to new proposals means that a comprehensive list of potential extensions, or 'abuses' of the scheme cannot be compiled. Individuals who are innately distrusting and suspicious of proposals such as the NSI may be able to conceive of a multitude of improper purposes for and hidden agendas behind the development of the NSI.

It is not beyond belief that at some stage policy makers may consider extensions or alternatives uses for the number and database. Indeed, it may be that future policy makers find the temptation to extend the scheme irresistible. For the purposes of conducting a privacy impact assessment it is appropriate to consider some of the implications of possible extensions of the scheme, notwithstanding that they may not form part of the scheme's rationale or objectives in the design stage.

Broaden the scope of the scheme – subjects

Once tertiary providers take up the scheme, the advantages of having one tracking number assigned to all school students, who may or may not go on to tertiary education, may become apparent.

Such an extension may be entirely consistent with the policy intention of the scheme in 2000, however, further uses when applied to school students might soon become apparent.

One such use would be tracking students through the secondary education system to detect truancy, and to follow up as necessary. It should be noted that a 1996 feasibility study concluded that a database of all school students was not viable in terms of the cost. Such an extension would clearly not be warranted in terms of the current proposal, which is limited to the post compulsory sector.

Such an extensive database may have considerable appeal for use by other agencies to track not only children, but people associated with children, such as parents, siblings or caregivers. Such a system might well come under pressure by government agencies (such as Child Youth and Families Agency, Department of Work and Income, Police and others).

A further potential would be that a database, accessible by tertiary providers, which contains details of school students might be able to be used for marketing tertiary education to those children.

In addition to the official pressure on such an extensive database, the temptation on individual administrators to use such a valuable information resource for personal profit may be irresistible. One only needs to look at recent examples of the sale of personal data from IRD's information system, by IRD staff to debt collectors to see how a comprehensive database can be abused for personal gain.

This potential currently exists and although it can be legislated against the legislation itself does not always prevent people from acting improperly. Despite sanctions there are limits on the ability of legal constraints to act as a check on individual behaviour. Any scheme, consistent with information privacy principle 5, would need sufficiently robust security to reduce the opportunity for misuse, and increase the likelihood of detection.

Broaden scope of scheme – agencies

A single database of tertiary students might have uses beyond macro level funding and policy analysis. Of greatest interest to those concerned with privacy would be uses of the information in a way which might have an impact on the individual subjects.

Other agencies may see the value to their operations of such a database. There may be possible uses of the system by the Department of Work and Income, for verifying eligibility for benefits, or for administering the student loan system. Similarly, the Inland Revenue department may see some use in its part in collecting student loan debt.

It is impossible to know, at this stage how those agencies would derive a benefit from the NSI.

A general concern might be that every extension of access to the system will increase in the number of people who would be able to obtain information for improper purposes.

One possible development adverse to privacy would be the adoption of the NSI number by providers as their primary means of recording information generated within their institutions. This would provide a theoretical "link" between the institution based information, which might include information about a plethora of non education related services and activities such as access to health or social services provided on camps, or disciplinary matters.

Feedback from providers to date has indicated a considerable resistance to this idea, mainly because of the cost of migrating students from the numbers they have already been allocated on an institution by institution basis, to a new numbering system. As such, it does not pose a predictable threat to privacy.

Nonetheless, it would be a simple matter for a code of practice to specify the purposes for which the identifier may be assigned, and proscribing the use of the identifier for other purposes.

Extension of scheme - information captured

The current proposal requires the assignment of a number to basic demographic data, and the central storage of that data.

Arguably the privacy implications of the scheme as described are minimal. The 'longitudinal record' generated tells analysts that the person with number X has certain demographic characteristics, and has participated in a list of tertiary courses.

Although privacy is an inherently subjective value, many people may not consider information of this nature to be "private". Some may consider that participation in tertiary education is a relatively public activity, as most campuses (apart from private training institutions) are open, public spaces. The increasing uptake of distance learning, and the greater potential for study to be undertaken anonymously via the internet may diminish the weight of such assertions.

Outside manifestly improper uses, such as the use of data by marketing companies, financial providers or debt collectors, it is difficult to see how the efficient management of data already collected could have an adverse impact on individual privacy.

On the other hand, there is an increasing awareness, and sensitivity among individuals about matters of personal and information privacy. Many people would regard any new centralised database as being inherently privacy adverse, regardless of the apparently innocuous nature of the personal information stored therein.

However, it would be open for the system to capture increasingly sensitive information. For example, it would not be a large technical leap to have the academic record form part of the core data. In terms of the policy aims, this might indeed make sense. A true analysis of the value of certain courses compared to others might well be enhanced with a record of not only attendance, by actual achievement.

Other expansions of the scope of data could include disciplinary matters such as suspensions.

Toward a national identifier

Privacy discussions internationally about unique identifiers are more often concerned with the dangers of individuals being assigned an official single number, or a number in common use being used as a de facto universal identifier.

Many jurisdictions have prohibitions on compulsory disclosure and use of unique identifiers other than for the strict purpose for which they were originally assigned. In Canada, the tax file number is protected in statute. In the United States rules apply to the use of the Social Security Number. The Senate Report for the 1974 Privacy Act (USA) noted that;

'the extensive use of Social Security Numbers as universal identifiers in both the private and public sectors is "one of the most serious manifestations of privacy concerns in the Nation."⁸

Proposals for identity cards have not proceeded in New Zealand or Australia, because of privacy concerns. The anxiety engendered by the use of unique identifiers is largely because of the ability they give to accumulate and centralise information about an individual's dealings with the state.

No doubt there would be immense efficiencies for Government in assigning a common number (such as the IRD number) as the key for accessing for a range of government services, including tertiary education. That the use of an existing number is not proposed for the education sector is an acknowledgement that perpetuating fragmentation of data across government is a social objective which although arguably 'inefficient', promotes privacy.

The use of sector specific identifiers can be seen to promote privacy by further embedding that fragmentation. The fact that the proposed NSI is sector specific, and

⁸ Privacy of Education Records David A. Banisar, *esq.* January 1994 Electronic Privacy Information Centre

will be one among several sector, or service specific numbers means that the likelihood of any only of those number becoming a de facto universal identifier is diminished.

The contrary position is put by the Canadian Privacy Commissioner in the example recorded above. In that case he expressed publicly his concern about a unique identifier that related only to physicians and medical students. It is relevant however that the disquiet he expressed was again based on the incremental and cumulative effect that such proposals have on privacy and the role of unique identifiers in becoming de facto identity systems.

Key Point 7

- The proposal would breach information privacy principle 12(2).
- It does not automatically follow that this would have an adverse effect on individual privacy. The use of a number does not inherently lessen individual privacy
- The fact that the scheme might be extended does not automatically mean an adverse impact on privacy will result.
- One of the greatest concerns internationally and locally with the use of unique identifiers is that they might grow to become de facto identity numbers.
- Universal identity numbers are viewed with suspicion and anxiety by privacy advocates.
- Given the intended coverage of the proposal (post compulsory students) fears of the NSI becoming a "de facto national identifier" may not be well founded.
- Although the proposed system may be seen as relatively benign from a privacy perspective, there is scope to extend the scheme in ways which might have a more significant privacy impact.

It is clear from the foregoing paragraphs that much of the privacy concern is derived not from the limited proposal under consideration, but from potential extensions of the scheme.

Having considered potential privacy threats, it is necessary to consider how those threats may be mitigated, and what (if any) privacy gains might be made from the proposed system.

Privacy Gains

Single collection/verification

Each time a student enrolls with a tertiary provider, he or she must give the same information as on previous enrolments. This includes verification of identity. Some students may regard the requirement to regularly produce documents such as a birth certificate or passport as intrusive, and even oppressive. For some it is expensive, inconvenient, and can lead to delays in completing enrolment. One of the concerns brought out above is the discomfort in privacy literature with requirements to compulsorily produce documents of identity (particularly in the form of an identity card).

The NSI would mean that the student would need only to provide the detailed information once, and only verify their identity once. On subsequent occasions, he or she would either present their NSI number, together with verifying information, or the person taking the enrolment would enter the personal data necessary to locate the record, and then verify the person's identity by asking questions from other fields, such as confirming their date of birth and residential status.

The requirements for verification of identity on initial presentation vary in different sectors, and across agencies. In the education sector it is common for tertiary providers to require enrolling students to produce a certified birth certificate. One possible reason for the development of this practice is the requirement in section 224 of the Education Act relating to the eligible age of enrolling students.

In terms of verification of identity, it is arguable that all such an requirement achieves is to confirm that a person, with the name on the certificate has been born. This process does not confirm that the holder of the certificate is that person. Nonetheless, it is an established practice, and providers and students consulted by the Ministry of Education in the course of developing the proposal have welcomed the possibility that the system will dispense with the inconvenience of producing attested documents after the initial enrolment.

Security of Transmission

Unique identifiers also enable the efficient and accurate transmittal of information about individuals, and can afford privacy protection, by sitting in the place of a name when the information is being processed or analysed.

Greater transparency and enhanced ability for students to have access to their own records, and ensure that they are accurate

There are numerous and disaggregated information flows under the existing system. Students may not be aware of the recipients of the information, or the purposes for which their information is used.

The NSI system, with its single central database may make it easier for students to know the range of uses to which their information is put. There is an opportunity in the implementation of the scheme to publicise more widely the sector information requirements and to impose clearer disclosure requirements on data capturing providers.

Identification suppressed for research and analysis purposes

Storage of the information already required by central agencies with reference only to a number would mean that officials undertaking research would not automatically see information in a form which could identify the subject.

In a relatively small country, where researchers would be tertiary qualified, and would certainly know many of the data subjects, this would afford greater level of privacy protection than is currently the case.

Key Point 8

There are some privacy gains from the proposal:

- It may reduce the number of times students are required to give and verify personal information
- The information may be more secure than is currently the case.
- Students may have easier access to their own information
- Identifying information can be suppressed when the information is analysed for policy purposes.

Precedent

International precedent

Many Canadian provinces use unique identifiers in the education sector for purposes similar to the proposed NSI.⁹ In British Columbia the Personal Education Number (PEN) was introduced in 1994. The information attached to the PEN includes name gender place and date of birth, primary language spoken, and program/grade participation.

The scheme was extended to the post secondary school system in 1998. A privacy impact assessment completed by the Ministry of Advanced Education Training and Technology recorded the purposes of the extension as to:

- Provide the government with reliable information for decision-making purposes;
- and
- Provide the government with an accurate means to measure and report on accountability within the publicly funded provincial education system.

The Privacy And Information Commissioner of British Columbia has investigated one (reported) complaint involving the PEN. In that case, the PEN was not directly in issue, however the Commissioner was concerned about a proposal for a curriculum time requiring children to compile information about their families and peers, and to include the PEN in their reports. The Commissioner did not uphold the complaint, but after discussing its concerns with the Ministry, the Ministry agreed that the PEN number should not be attached to detailed student work produced under the Ministry's Career and Personal Planning curriculum.¹⁰

The absence of complaints may indicate that the systems have not lead to privacy intrusions, or that the public in those communities does not regard information about participation in education as having high privacy value. There may be other explanations, such as that these systems are not widely known, or are strictly limited in their purposes.

There is nothing to suggest that the use of the number in itself has raised privacy concerns, or is in breach of the (very similar to New Zealand) British Columbia privacy law.

In the United States, education information is governed by the Federal Education Records and Privacy Act 1974. That legislation imposes limits on the disclosure of education records, but does not directly address unique identifiers.

The US Department of Education¹¹ notes that

⁹ Alberta, Manitoba, Saskatchewan, Ontario, Quebec and Newfoundland all use a central numbering system

¹⁰ Investigation Report P97-008 www.oipcbc.org

¹¹ US Department of Education National Centre for Education Statistics *Protecting the Privacy of Student Records*, NCEES 97-527 Oona Cheung, Barbara Clements, and Ellen Pechmen, Washington DC

"Using unique identification codes would

- Allow the records to follow the correct students when they move within the state
- Provide the flexibility of merging data from different files to promote efficiency without threatening privacy."

On using the social security number as an identifier for student purposes, which many providers do, the Department says

"The social security number has the advantage of being unique to students and does not change when they move to another city or state. It is useful across schools districts and states. Using the social security number thus can make it easier for schools to locate the appropriate transcript or student information when they receive a request."

On the other hand, the department points out some of the shortcomings of or cautions in using the social security number;

- Schools can ask for the number, but cannot require it
- Schools must inform parents that they do not have to provide the number
- Schools cannot refuse any services or privilege because a student has not provided the number
- Schools that use the social security number should be prepared to assign an alternative.
- Parents may not recall their number, or may give an inaccurate number
- Confidentiality of the number is paramount.

The precedent value of the United States example is limited, given that it relates to a cross sectoral number, which is used to access a wide variety of government services. The equivalent in New Zealand would be using the IRD number, or community services card number to refer to post compulsory education.

It is interesting to note that even given that it is an offence under the Federal Privacy Act 1974 to require the disclosure of the social security number, its utility as a voluntary identifier in the education sector is acknowledged at Federal level, and is growing.

Key Point 9

- There are examples of the use of unique identifiers for education in other jurisdictions.
- These do not appear to have raised significant privacy concerns in those communities.

Domestic Precedent

While there may be limited precedent value in existing unique identifiers which have been permitted either by the Privacy Commissioner through Codes of Practice, or

through other legislation, it is useful to see what has gone before, partly in order to glean the level of use, and acceptance of such devices in the community.

For the purposes of this proposal, little assistance is to be gained from considering identifiers such as the IRD number, or the Drivers licence number, except to say that the privacy concerns raised by extensions of those numbers are likely to be far more profound than a new identifier applied to tertiary students. In the case of the IRD number, the universality of application is almost total. In the latter case, the requirement for drivers to carry their license with them while driving adds another privacy dimension, in the form of a de facto identity card.

More apposite are the sector specific identifiers which have been authorised post Privacy Act by way of codes of practice. Three have been authorised. They are

- The National Health Index (NHI)
- Law Enforcement Agency Record Number (LEARN)
- A Superannuation number

The superannuation number is not directly relevant to the NSI proposal, as it simply legitimises a practice in the administration of superannuation schemes. There are parallels with the NSI proposal in the former two codes, authorised respectively under the Health Information Privacy Code 1994, and the Justice Sector Unique Identifier Code 1998.

The Health Information Privacy Code allows health agencies to assign and use a "National Health Index" number. The Justice Sector Unique Identifier Code allows justice agencies to use a common number for identifying people as they pass through Police, Department for Courts, and Department or Corrections processes.

Although the Privacy Commissioner's office has expressed disquiet about the expanding use of the NHI number in the health sector¹², the sanctioning of the concept acknowledges the need to ensure good data is available about individuals at a national level. The use of the number does act to protect privacy in one sense because the "transactional" information is separated from information which would identify an individual consumer of health services.

There are limitations to using these codes as persuasive precedents for allowing the development of further unique identifier, index number systems. On one hand, each code legitimises an activity which is underway prior to the passage of the Privacy Act. They are not new activities which have been developed in the post Privacy Act policy environment. The fact that the practices have been allowed to continue under the 'new' legislation does not mean that there is an acceptance that such systems should be allowed to proliferate.

¹² Medical Record Databases. Just What you Need? A Survey of Practice and Plans in New Zealand for the Collation and Retention of Health records about identifiable individuals, with Particular Reference to the Implications for privacy Arising from the Increased Use of National Health Index Numbers
Office of the Privacy Commissioner 1998

On the other side of the argument, it may be that the level of privacy threat represented by the Justice and Health systems, compared to the proposed NSI number, is significantly more substantial.

Although, given the very subjective nature of the privacy, qualitative judgements about relative privacy values are difficult, it is clearly arguable the proposed NSI involves “less sensitive” information.

Health information in particular, and to a lesser extent, information revealing individuals involvement with the justice sector would generally be considered to be “private” information. In a field where there is no unanimity of views, information about the health services one accesses would almost without exception be considered to be of the most private nature.

There is less likely to be the same level of agreement about information associated with ones interactions with tertiary providers. To a considerable degree, participation in tertiary education is a public activity. Society as a whole might well be likely to see a lesser privacy value in such information, than in say information about ones financial transactions, health, or consumer records.

Key Point 10

- Unique identifiers have been permitted in other areas in New Zealand, most relevantly in the Health sector, and the justice sector. These have been allowed by codes of practice issued under the Privacy Act by the Privacy Commissioner.
- Those codes were not new policy proposals, but enabled existing practices to continue under the Privacy Act 1993.
- Those codes relate to more sensitive information than information about participation in post compulsory education.

Alternative Means of Achieving the Policy Objective

Any privacy impact assessment should consider, given the privacy implications identified during the evaluation process, whether the policy aim could be achieved by means that are less likely to have the same level of privacy impact.

No Unique identifier

One way of achieving the aim of improving information available to policy makers would be simply to require each agency to forward to the Ministry full demographic details of each student, and for the Ministry to manually cross reference the enrolment details to “track” patterns. In other words, all returns would be made using the student’s name, reported in a uniformly standard way.

There would be three main disadvantages to this approach. First, there would be a greater likelihood of duplication and error, as providers may misreport the name, result in multiple records of the same student. This may have adverse privacy implications, in that it may be more difficult for the student to trace all the information about him or her. Secondly, such a system would be far more labour intensive, and therefore inefficient from the perspective of the central agencies.

Thirdly, such a system would mean that readily identifiable individual information would be held in a central agency. Analysis conducted on the data could not be undertaken without using the student’s name.

Another alternative to having a warehouse comprising a comprehensive record of all participation in post compulsory education would be for policy analysts and researchers to commission surveys of students to ascertain data for analysis. This has the advantage of obtaining information directly from the source, with a disclosure as to the precise purpose for which the information is sought.

There are however, practical and privacy disadvantages in such an approach. First, in order to select an appropriate sample, with the attributes that the researchers want to study, the researchers would need detailed information of the type proposed for the warehouse. Second, that information would need to be linked to identifying information so that individual contact can be made. This would increase the information to be collected (address and telephone number would be necessary). The student population is transient in nature, so the response rates may be lower than necessary for a statistically valid result. In addition, many people regard surveys as intrusive. From a researcher's point of view, they are also very expensive.

Use of an existing number - IRD/Drivers licence/Community Services Card

There are a number of other ways in which the policy might be achieved. Some of these would have a greater impact on privacy. For example, using a unique identifier that is already in use, such as the IRD number would increase fears about the ability to cross match disassociated data.

Use of numbers such as drivers licence would involve increasing the reach of that document as a national identity card, which was not anticipated when the new licenses were proposed. In addition to the obvious privacy implications, such a proposal would not provide universal coverage, as not all students hold drivers licenses, so the value of the data would be diminished.

Similar problems exist in respect of the community services card, with the added disadvantage that the data would be incomplete in respect of those students not receiving state assistance.

These options would be unlawful without a code of practice exempting the practice from information privacy principle 12 or specific legislation.

Use of an existing number - Record of Learning Number

NZQA assigns an RoL number to every student participating in the National Qualification Framework. Students receive regular updates of the qualifications they have received at which time they have an opportunity to update their personal details. In addition numbers are also assigned to candidates for national secondary qualifications.

The number is not used in the university sector, but as the National Certificate of Educational Achievement rolls out, more and more university students will already have a number.

Using the RoL does not resolve any of the issues identified in this paper, and would not be permitted under existing legislation, as requiring the assignment of the same number used by different providers would still be in breach of information privacy principle 12.

A further complication would be that the RoL already records the educational achievements of 500 000 students. This information has been collected over the last ten years, on the basis that its sole purpose is to enable students to keep track of their 'credits' toward national qualifications.

Voluntary adoption of number

It may be possible to trial a voluntary system of assignment. There may be sufficient benefits for students to see the value in having one number for all their tertiary education purposes. For example, the identity documents required for enrolment would only need to be sighted and verified at the first enrolment.

The disadvantage of a voluntary system is that the value of the information resource for research purposes would be limited by the extent of participation. Given the expenditure involved in the IT infrastructure, officials and politicians may be disinclined to proceed when the value of the information output cannot be guaranteed.

A voluntary unique identifier system would also increase compliance costs for providers, who might need to maintain dual systems for administration and reporting.

The alternative means of achieving the same policy objective, namely;

- No Unique identifier
- Use of an existing number- IRD/Drivers licence/Community Services Card
- Record of Learning Number
- Voluntary adoption of number - might be less efficient, have a greater impact on privacy or both.

Options to Facilitate the Scheme

Legislation

Specific legislation to enable the use of the NSI would have the advantage of being sanctioned by Parliament, and would therefore be an open and transparent process in which the public could participate.

The main disadvantage is that new legislation could take a long time to be passed.

A legislative provision would override the Privacy Act, and might therefore provide limited oversight as to the management or extension of the scheme.

Legislation could either be enabling, or prescriptive. Enabling legislation might have greater privacy concerns, because the scheme would be able to expand its scope without further reference to parliament.

On the other hand, prescriptive legislation can cause difficulties in respect of new policy initiatives, because the law needs to be in place before the system is developed, and therefore might not accurately reflect the technical requirements of the system as they are revealed in the process of actually designing and building the necessary information systems.

Code of Practice for the Education Sector

Another option is a code of practice which amends all the information privacy principles to take into account the particular features of the education sector. This is the approach taken with the Health Information Privacy Code. Included in such a code would be a provision modifying principle 12 to enable the assignment of a common unique identifier.

The past 7 years of the operation of the Privacy Act has not suggested that the education sector has sufficiently distinct features from any other sector to warrant a purpose designed Code of Practice.

A section of the tertiary education sector, through the Vice Chancellor Committee, did consider a code of practice applying to universities, but the need was not considered such as to warrant the effort required to obtain a code.

A Unique Identifier Code of Practice

The third option would be to ask the Privacy Commissioner to issue a code of practice amending only information privacy principle 12 to enable the NSI as currently envisaged.

This is the approach that was followed in respect of the Justice Sector Information Privacy Code 1998.

There are several advantages to this approach. First, the proposed code would focus only on the NSI number. This would enable submissions to be tightly focussed on the privacy implications of the unique identifier proposal only.

Secondly, it would leave oversight of the development of the Code, and consideration of the submission in the hands of the Privacy Commissioner, an independent privacy advocate. As such it would have credibility, and consumers could have confidence that the privacy implications had been thoroughly traversed. By way of contrast, the driver license photo id card, which was enabled by legislation, has aroused considerable suspicion, and has lead to High Court challenges.

Concerns over possible "function creep" could be mitigated by the need to seek the Privacy Commissioner's authorisation for any extension of the scheme, by way of amendment to the Code. Any of the possible extensions considered above would need to go through a rigorous process of privacy impact assessment, and public consultation on the code amendments.

As with other codes, a review process could be built in to enable the evaluation of the scheme form a privacy perspective in two or three years time.

Key Point 12

The proposal cannot proceed under the existing law. The options to enable the project to proceed include:

- Enact an express legislative provision
- A code of practice under the Privacy Act for the Tertiary Sector
- A code of practice under the Privacy Act covering just the NSI

The main advantages of a code just addressing the NSI is that it could:

- Prescribe the permitted scope of the scheme
- Be subject to the oversight of the Privacy Commissioner
- Provide a real remedy for privacy breaches.

Overall Conclusions

- The proposal does not involve the collection of any more information than is currently required for tertiary education funding and research.
- There are privacy implications in the assignment of a single identifier to students. These are:
 - Students must be fully informed about the scheme, aware of the purposes of collection of the information, the proposed uses, and the purposes of the unique identifier;
 - Central databases heighten concerns about misuse of personal data.
- These privacy concerns should be addressed by;
 - A systematic information programme at the point at which numbers are assigned to students (in compliance with information privacy principle 3;
 - High levels of security standards promulgated either by a code of practice, or as part of the service agreements between the various participating agencies.
- There is a general unease in privacy circles about the widespread use of unique identifiers because:
 - The enable data to be compiled and resorted from different databases more easily;
 - Pressure can be applied to find new uses, or extensions for the schemes;
 - Unique identifiers have the potential to become de facto universal identifiers.
- These concerns could be addressed by
 - Enabling the scheme to proceed by way of a code of practice which prescribes the agencies which may assign information;
 - Requiring any proposed extensions of the scheme to be authorised by the Privacy Commissioner