

MIAP and PIB – the ‘Wider Picture’

A response to comments by DfES

Submitted by John Harrison of Eidentity Ltd in January 2007, with the support of:

Paul Hopkins, Director of Information Systems and Services, Newcastle University

Mike Martin, visiting Professor, Centre for Social and Business Informatics, Newcastle University

Jean Bacon, Professor of Distributed Systems, Computing Lab, University of Cambridge

Brian Collins, Professor of Information Systems, Cranfield University

Table of contents

Introduction & Summary	3
Background	4
MIAP and PIB in brief	4
A paper-based analogy	5
Authentication or identification ?	5
Citizen-mediated plays catch-up	6
The structure of the education sector	6
Issues raised by DfES	7
Does the DfES need to know its customers' legal identity ?	8
Interactions between PIB and legal identity	8
Why should education lead ?	9
Comparison of MIAP and PIB approaches	10
'A true lifelong learner record' ?	10
'Research & analysis'	11
'Service Improvement', 'Efficiency Savings', and 'Bureaucracy reduction'	11
'Wider strategic fit'	11
e-learning	13
Attendance & location	13
Authentication and Single-Sign-On	14
Policy neutrality	15
Business model	15
Support for the less able	16
Cost	16
Conclusion.....	16
References.....	17
Annex A: Financial systems	18
Annex B: Social care systems.....	19

<i>Version</i>	<i>Date</i>	<i>Comment</i>
1.0	15 Jan 07	First formal issue.

Eidentity Ltd
The Millers House
Church Road, Shaw
Newbury RG14 2DL

Contact : John Harrison
E-mail: john.harrison@edentity.co.uk
Telephone: 07801 231 693

Introduction & Summary

1. The Department for Educational Skills (DfES) is proposing, under the banner of the Managing Information Across Partners (MIAP) programme, to issue every learner with a Unique Learner Number and then create a (virtual) national database of learners' qualifications. The programme expects that the various learning providers and awarding bodies in the sector will contribute personal data to a central pot, using traditional inter-organisational¹ techniques in which the ULN serves to match one record against another.
2. Eidentity, a tiny company specialising in the emerging field of user-centric identity management, proposes an alternative approach: that users be empowered – using a concept called Personal Information Brokerage² (PIB) – to aggregate their own qualification data. PIB is described, in some detail, in a submission [R1] to the current House of Lords' Science & Technology Committee Enquiry into Personal Internet Security. The submission was supported by a grouping of senior individuals from across the education, computer science, and telecoms sectors.
3. An official from DfES has kindly stated, by e-mail, that he has “*never suggested that [the PIB concept] is without interest or merit*”. But he went on to state that:

*“it does perhaps need to take account of a **wider picture**. The department (and the other actors in the wider system for which it is responsible) do have a responsibility to know who their customers are. That has to sit alongside the need to allow learners to manage their information. I don't think you would be suggesting to a major bank that they should not have a way of uniquely identifying their customers so as to support service provision. But you seem to come pretty close to suggesting that somehow in education we don't need to – and I disagree”.*

And, in response to a comment that the private sector is generally poor at infrastructure projects:

“I don't think I properly understand your arguments about private sector engagement. The private sector may or may not be good at infrastructure (though it seems, for example, to have been pretty good at information infrastructure in financial services) but it rarely misses service provision opportunities that need filling.”

4. In this note, we:
 - o summarise the MIAP and PIB approaches to data sharing, using non-technical language; offer a paper-based analogy for the two approaches; explain why, in PIB, authentication is more important than identification, whereas for MIAP the reverse is true; and point out that, since PIB depends on personal network access which is only now becoming widespread, the technology is playing catch-up;
 - o argue that the UK education sector (which DfES oversees) is federal in nature, and thus well suited to the PIB approach; whereas the UK welfare sector (in which DfES also plays a role) is monolithic in nature and better suited to a centralised, MIAP-style, approach;
 - o address the ‘identity’ issue raised by DfES in recent correspondence, as described above, and argue that:
 - in its role as overseer of the (narrowly defined) UK education sector, the department has no need to know its customers' legal identities;
 - although the department does need to record its customers' legal identities to discharge its welfare responsibilities, existing or planned databases (such as the extension of NINO to young people, or IS-Index) could serve this purpose, and thus there is no need to duplicate the functionality in a MIAP-style project; and
 - in the long run, PIB will offer individuals a wholly electronic way of giving permission for the transfer of legal identity attributes from a central register, and thus obviate the current need for paper/ plastic certificates and cards. This may be appropriate when learners request direct financial assistance from the state.

¹ Depending on context, we use various terms to refer to these inter-organisational techniques, e.g. ‘traditional data-sharing’, and ‘back-office data sharing’.

² Similarly, we use various terms to refer to PIB and related initiatives in the field of user-centric identity management, e.g. ‘learner-mediated data sharing’, ‘citizen-mediated data-sharing’, and ‘front-office data-sharing’.

-
- address the 'Why education?' issue raised by DfES, arguing that the sector is uniquely placed to benefit from, and lead the development of, PIB infrastructure;
 - provide a detailed comparison of MIAP and PIB, using the goals and claimed benefits of MIAP as the initial criteria, and show that:
 - MIAP's ambition to create a lifelong-learner record is unrealistic, whereas PIB may succeed, to the extent that a learner wishes to maintain a lifelong-learner record in one place;
 - The scope for each approach to produce better data for research and analysis depends, in the long-run, on achievement of the headline goal, i.e. the creation of true lifelong-learner records;
 - PIB is a better strategic fit with other DfES programmes, and with the wider needs of UK e-infrastructure development, than MIAP, provided always that short-term timing considerations are discounted;
 - MIAP's claim to contribute to the e-learning agenda is not supported by the e-learning development community in the UK. PIB enjoys growing support;
 - MIAP intends to deliver efficiency savings by requiring independent organisations to behave as if all are part of a larger organisation. In contrast, PIB should deliver savings of equal or greater magnitude by empowering individuals to deal more effectively with *multiple distinct* organisations. By showing how efficiency can be achieved without centralisation, PIB can make the better claim to be a means of reducing bureaucracy.
5. We conclude by suggesting that, in the MIAP programme, DfES is trying develop an all-purpose system to meet its needs as both an overseer of the UK's education system and as one of the government agencies tasked with delivering welfare services. In doing this, the department risks developing infrastructure for inter-organisational data sharing that is inappropriate for the (narrowly-defined) education sector, conflicts sharply with the sector's history of learner-permissioned sharing, and impedes the development of PIB infrastructure that is needed by society at large. DfES should pause, and review the options, before proceeding.

Background

6. Public sector organisations in the UK have recognised for some time that their records tend to be locked away in silos, and that sharing of this data would allow them to deliver 'joined-up' services to the public, drive-out cost, and reduce fraud. There are two fundamental approaches to such sharing: the traditional inter-organisational approach; and a modern approach based on the new field of user-centric identity management. MIAP is a fair example of the former, and PIB of the latter.
7. In this background section, we provide brief descriptions of the two proposals, and offer a paper – based analogy to explain, in easy language, how they differ. We then discuss the different emphases given in each approach to the processes of identification and authentication, and finish by looking at the issue of technical maturity.

MIAP and PIB in brief

8. The philosophy of MIAP, as stated in the programme's business case, is to 'Collect Once, Use Many Times, [and] Use By All'. This is to be accomplished by: (i) registering the legal identity of, and giving a Unique Learner Number (ULN) to, every learner in the state-funded system; and (ii) inviting every learning provider and awarding body to contribute learner / candidate records to a (virtual) central pot, where the records will be matched using the ULN as an identifier. The various classes of users (learning provider, researcher, LEA, DfES, learner, etc) will be given access to the (virtual) database appropriate to their role.
9. In contrast, in PIB, a learner is invited to select an information broker from a market of such brokers, and then use his broker to sign-on securely to *multiple distinct* service providers, such as learning providers, and awarding bodies. In addition, he can use a permission hub provided by the broker to give explicit, transaction-based permission for the transfer of personal attributes to, and between, service providers.
10. In the long-run, the likely providers of brokerage services are the banks and mobile telecoms companies, who can provide secure authentication at low cost as a result of their existing activities. Two telecom companies have already expressed interest. In the nearer-term, the role may be fulfilled by public and third sector bodies. To meet the costs of the infrastructure, service

providers pay brokers for (i) a secure e-relationship with the individual, and updates to the attributes that he has chosen to disclose; or (ii) the chance to enter into a secure relationship with the individual. More detail about the PIB concept is given in the recent House of Lords submission [R1].

A paper-based analogy

11. In the paper-based world, there were two ways in which organisations could share data. Either one organisation could send an individual's file directly to another, in a back-office transaction. Or an individual could request a paper certificate from the first organisation, in a citizen-mediated (or front-office) transaction, and then show it to one or more other organisations at her convenience. These are the paper-based equivalents of MIAP, and PIB respectively (although the use of the word 'certificate' in relation to PIB suggests too close a link with PKI³)
12. Although both are suitable in certain circumstances, they each have drawbacks. Starting with the back-office approach, it: (i) requires the receiving organisation to solve the problem – which can be difficult – of matching incoming files against those already held, or with the 'right' individual when he presents himself; (ii) becomes more and more difficult to manage as the number of organisations and individuals involved increases; and (iii) can – if implemented without due care and/or on a large scale – impair privacy.
13. Looking now at the citizen-mediated approach, this (i) is suitable only suitable for attributes that an individual regards as positive, and for transactions that he regards as beneficial; and (ii) can – if implemented poorly - create an opportunity for dishonest individuals to steal certificates held by others, or tamper with certificates they already hold, and profit thereby.

Authentication or identification ?

14. The two approaches, back-office and citizen-mediated data sharing, place different emphases on the processes of identification and authentication. Because back-office data-sharing requires the receiving organisation to match incoming files, or a person in the flesh, against records already held, there is emphasis on the process of identification. A common solution is to create a system of unique identifiers, such as the ULN, that will appear on every record, and thus make the matching process easy. Authentication is less important, only being required to ensure that one individual is not masquerading as another.
15. In citizen-mediated sharing, in contrast, the individual carries his or her own record between organisations, and the receiving organisation is spared the record-matching problem. Hence there is no need to pay attention to identification, and little justification for a conventional system of unique identifiers. However, as the value of information carried on a certificate increases, so too does the risk of theft - whereupon simple possession ceases to be adequate as proof of ownership. Instead there is a need for to authenticate the individual securely as the owner of a certificate.
16. Consider, for example, a proof-of-age card, used perhaps to allow an 18 year-old to buy alcohol. The only information that is required on such a card is a statement that the owner's age is over 18, and a means by which the individual can authenticate herself as the rightful owner. Generally, a photograph serves this latter purpose, and is affixed to the card securely to prevent tampering. Note that: (i) there is no need for a proof-of-age card to bear the owner's name, or any other general identifier; and (ii) that, although a biometric (in the form of a photograph) is used for authentication purpose, there is no problem with privacy because the record against which the authentication takes place is kept in the owner's possession.
17. By extension, it seems unlikely that many people would object to using a finger-print, in lieu of or in addition to a PIN, in order to increase the security of a payment process. Like the photograph on a proof-of-age card, such a print would serve principally to authenticate the individual as the rightful owner of something – a payment card – which is in their possession. It does not serve to identify the individual against some third party register, and thus poses no privacy risk.

³ PKI = Public Key Infrastructure, a security technology, relying upon 'digital certificates', that was originally marketed as 'the' solution to issues of identification and authentication. While successful in corporate applications, it is now widely accepted that PKI may be a useful component of consumer solutions (like a clutch in a car), but is not a solution in its own right (the car itself).

-
18. Three points emerge here, which are worth restating. First, in citizen-mediated data-sharing, authentication of the individual as owner of a certificate can be important, while identification is unnecessary. Second, authentication can be an anonymous process, serving merely to confirm ownership of a certificate. And third, anonymous authentication poses few privacy risks, and thus can – if necessary – make use of biometrics without difficulty.

Citizen-mediated plays catch-up

19. In the paper-based world, citizen-mediated data sharing was easier and cheaper than the alternative, and was used whenever possible. Thus an individual carried medical prescriptions from doctor to pharmacist, exam certificates from school to sceptical employer, and a driving license from DVLA to a car-hire company. Back-office sharing was limited to attributes that were regarded as confidential, such as some medical records; or were negative, such as criminal records.
20. In the network world, the technologies for back-office data sharing have been developed steadily over the last forty years, as organisations started to use computers and exchange data electronically. Private sector organisations, such as the credit-reference agencies, overcame the record matching problem by use of sophisticated pattern-matching algorithms; in the public sector, the favoured solution is to issue a unique identifier for use by all organisations of like kind, e.g. the NHS number, the proposed Unique Learner Number, and the National Insurance Number.
21. In contrast, individuals have only acquired network access in the last few years, and so techniques for citizen-mediated sharing are only now beginning to catch-up. The field is called user-centric identity management, and a key premise is the idea that an individual should have a different e-identity for every distinct service provider with which he deals. Then the goal is to find ways to enable the individual to: (i) sign-on securely and conveniently to *multiple distinct* service providers; and (ii) give explicit transaction-based permission for the transfer of personal information to, and between, service providers.
22. There are now several initiatives to implement user-centric IdM architectures. Examples include Cardspace, a client-side architecture led by Microsoft; and Personal Information Brokerage (PIB), a server-side architecture, led by Eidentity in the UK. Details of both are given in the recent House of Lords submission [R1].
23. User-centric IdM schemes, such as PIB, promise great benefits. But, as with all innovations, they seem difficult at the outset. In the following sections, we argue that the education sector could benefit greatly from PIB, and should make the effort to trial the concept. We start by looking at the structure of the education sector as background for subsequent discussion.

The structure of the education sector

24. Working within DfES, it must be tempting to see the education sector as a ‘monolith’, for which an analogy with a retail bank is apt. Most modern retail banks offer a standard array of services to consumers nationwide via a branch network. Since an individual’s primary relationship is with the national organisation, rather than with any particular branch, there is a clear need for the head office to maintain a single comprehensive register of its customers, and to authenticate customers against this register every time a payment request is received.
25. The alternative view of the education sector is that of a loose ‘federation’ of independent organisations. Here, every school, FE college, university, and awarding body is autonomous, serving its own group of customers, and must maintain its own register. And DfES acts as a source of finance for some organisations, and may set standards and require inspections, but it is no sense the head office of a monolithic sector, and thus has no absolute need to maintain a single national register of learners.
26. Reality lies, as always, between these two extremes. The sector is not homogenous: its organisational model varies, both by the level of education, and according to the purpose of DfES’s interventions. Looking first at the variation by level of education:
- at the primary and secondary level, state-funded educational provision accounts for about 93% of the total, and private provision for 7%. By definition, the private schools do not regard themselves as a part of the state education sector. In contrast, and because DfES controls

their funding, it is just about possible to regard the state-funded schools as branches of a national monolith.

- at the tertiary level, the universities – especially those that are long-established – receive a significant part of their income from sources independent of DfES, and so consider themselves to be largely autonomous.
- much education and training takes place outside the formal education sector, either as work-based training or as various forms of adult and continuing education. Funding for, and governance of, these activities is diverse, and many of the providers are partially or wholly autonomous. Examples range from licenses to practice awarded by the General Medical Council to the qualifications of the British Cleaning Council, and from gas-maintenance qualifications awarded by CORGI to PhDs awarded by universities. Only a small proportion of these activities are directly funded by the state.

27. Looking now at the different roles that are, or could be, fulfilled by DfES:

- Defined narrowly, the department's role could be limited to that of oversight of the UK's education system. If learners (or parents acting on their behalf) were to be given a voucher by HMRC each year that could be used to 'pay' for part or all of their education at an institution of their choice, then learning provision could be left largely to the charitable and private sectors. DfES's role would then be limited to setting standards, and carrying out inspections. The sector would naturally organise itself as a federation.
- But the DfES's role is, in fact, defined much more broadly than the bare minimum described above. As well as working with other agencies – such as the DWP, the NHS, and the social care departments of local authorities – to ensure child protection, the department is also involved in the delivery of welfare-style benefits to a significant proportion of the population. These include: (i) free nursery, primary and secondary schooling for the 90% or so of children who are not home-schooled or educated privately; (ii) payments under the Education Maintenance Allowance Scheme to young people from low income families who remain in education post 16; and (iii) low-interest unsecured loans to students attending HE courses.

28. What do these differences imply? The comments about the levels of education suggest that a monolithic view of the sector is almost tenable for state-funded primary and secondary provision. But even here, the logic of a single-organisational approach has not been taken as far it might: there is no suggestion, for example, that all state-funded schools should carry the branding of a 'National Education Service', akin to the NHS in the health sector; nor is there any move to make learners authenticate to a central register, as happens in banking, every time they transact with a learning provider. Also a monolithic view of the sector is clearly not tenable for many universities, for independent schools, and for much of workplace, adult and continuing education.

29. In short, it would seem that the predominant organisational model in the (narrowly-defined) education sector remains that of a loose federation, as it always has been. Within such federations, personal data is generally only shared with the consent of the individual, using either paper certificates, or by references issued at the individual's request. Historically, this has certainly been the case in the UK education sector.

30. However, the DfES also plays role in the provision of child protection and welfare services. The organisational model for these services – despite the number of agencies involved – is essentially a monolithic one, since it may be necessary for the agencies to share data without explicit consent.

31. In determining IT strategy for the sector as a whole, we would suggest that it is necessary to bear the twin roles of DfES – as overseer of a federation, and as a participant in the provision of child protection / welfare services – in mind.

Issues raised by DfES

32. In this section, we respond directly to the two reasons cited by DfES for not taking PIB seriously, and also take the opportunity to air a third issue, which is relevant in this context. We start with a question of identity.

Does the DfES need to know its customers' legal identity ?

33. We have just established that DfES plays a role in two different organisational structures: it acts as the overseer of a federal education sector; and also as one of the agencies tasked with delivering child protection and welfare payments.
34. Starting with its oversight role, the short answer is that DfES has no need to maintain a central register of all learners in the country. Pursuing the analogy with the financial services sector, the DfES should play the role of the Financial Services Authority (FSA), with each learning provider being the equivalent of an autonomous financial institution. The FSA does not attempt to maintain a central register of all individuals with bank accounts, and of the money they hold in each account; nor should the DfES attempt to maintain a central register of all learners, and of the qualifications they have earned from different awarding bodies.
35. Those inclined to dispute this view might point out that the FSA has no need to maintain a central register, because that role is fulfilled in the financial sector by the credit reference agencies. In one sense, this is true. The credit reference system does establish biographical identity, which is closely linked to legal identity. But, as pointed out in Annex A, the credit reference system was designed 40 years ago. A system designed in the modern day, now that individuals enjoy secure network access, might rely upon distributed variants of Paypal-style immediate person-person payments, and an e-bay-style trust system based on a record of successful transactions. In such modern infrastructure, there would be no need for credit reference agencies at all.
36. Turning now to DfES's child-protection and welfare role, the situation is very different. Here there is a need for back-office data sharing, both because individuals may not be willing to divulge negative data, and in order to prevent fraud. As discussed earlier, back-office sharing requires a system of unique identifiers – such as legal identities – to overcome the record matching problem.
37. Two registers of legal identities for children and young people either already exist or are planned. For child-benefit purposes, the Department of Work and Pension has already extended the National Insurance Number (NINO) database to cover children and young people. And, as described in Annex B, the DfES is creating the new IS-Index database for child protection purposes. It is surely more sensible to make one of these databases into a single secure register of all children and young people in the UK, rather than creating a second partial register, covering only participants in state-funded secondary and FE education. Then, at the age of 16, young people will apply for an ID Card, and be transferred from this secure children's database to the ID Card Register.
38. What we are suggesting is the need for a balance in the approaches to data sharing: empower the citizen to aggregate and share data where – for scalability and privacy reasons – he or she is best placed to do so. And have public-sector organisations share data directly, using legal identity as the common identifier, only where there are compelling reasons to exclude the citizen. For the education sector, this means using citizen-mediated techniques initially for qualifications, contact details, and calendar /attendance; and using back-office techniques, and legal identity, for child protection, and the prevention of fraud.

Interactions between PIB and legal identity

39. Although not raised specifically by DfES, there is a further point that needs to be aired here. If both approaches to data-sharing are implemented, there is a risk that a learner will (i) use his permission-hub to sign-on securely to learning providers and awarding bodies, update the contact they hold, and aggregate records; but that (ii) the learner's entry in the secure national database will be left untouched, and so become inaccurate.
40. The solution to this problem requires another shift in thinking. Instead of seeing the legal identity register as an oppressive thing, it becomes useful to think of it as just another entity that provides services to the individual – in this case enabling him to prove legal identity remotely. Then it becomes clear that an individual would benefit by maintaining a relationship with the legal-identity registrar using her permission hub.
41. There are two points at which the relationship could be established. The first is at initial issue. Information brokers could be required to issue brokerage accounts in which the relationship with the legal-identity registrar is already in place. But this risks being too heavy-handed: it would require too high a level of initial authentication, and would give the impression that PIB could only

be used for public-sector transactions, rather than as an enabler of secure transactions across society.

42. The alternative is to encourage learners to discover at an early age, say from 12, how they can use brokerage to sign-on to their school's systems, swap data with friends, communicate with teachers, collect qualifications etc. A low-level of authentication, such as username-password, would suffice.
43. They would only be encouraged to make the link between their permission-hub and the legal identity register when legal identity first becomes important in the (narrowly-defined) education sector, i.e. when learners first apply to the government for direct financial assistance. The two assistance schemes kick in at different ages: the Education Maintenance Allowance is available from 16; while university students apply for loans one or two years later.
44. To apply for financial assistance to an awarding body, a learner would :
 - i) upgrade to two-factor authentication for his broker account, probably using a mobile as the second factor;
 - ii) establish a relationship between his brokerage account and the legal-identity register. This process would be similar to the way in which relationships are set up from a Government Gateway account to HMRC's (or other departments') back-office systems, i.e. (a) the individual sets up a Gateway account, and enters HMRC customer reference number; (b) HMRC sends an activation code by conventional mail to the individual's home address; and (c) the individual enters the activation code and the service goes live.
 - iii) apply from his brokerage account for the desired financial assistance, i.e. either the EMA or a student loan. In making the application, the learner would use his permission hub to give the awarding body access to (a) legal-identity attributes, as recorded on the legal identity register; and (b) bank account details, as stored personally within his permission hub.

On receipt of an application, the awarding body would process it, and then communicate the result by secure mail back to the applicant's brokerage account.

45. The use of PIB in this way eliminates the need for an individual to rely upon physical /paper certificates to establish legal identity. In this electronic age, such reliance was beginning to seem increasingly anomalous, especially when – as was the case for student loan applications – it was necessary to send original certificates by post in support of an application made remotely.

Why should education lead ?

46. The second major concern of DfES seems to boil down to the question of 'Why us ?'. Why should the education sector be the first to implement PIB infrastructure, rather than another government department or sector of the economy ?
47. The answer is simple. Education is the sector where the many PIB applications will deliver the most immediate benefit. It also meets all the criteria for a successful implementation of PIB, specifically:
 - o customers are actually expected to move from one service provider to the next, and so the need to empower them to deal with multiple distinct service providers is acute;
 - o there are clear benefits to be won from improved data sharing;
 - o most of the data shared is positive, and thus suitable for a permissioned approach;
 - o the organisations in the sector wish to retain distinct relationships with their customers, rather than being subsumed within a de-facto single national organisation;
 - o the organisations in the sector, despite wishing to retain their independence, have the capacity to act in concert to adopt common infrastructure;
 - o the customer base is, predominantly, young and technically literate; and
 - o the sector is not locked into an organisation-centric data-sharing model, as exemplified by the financial services sector, and designed in a different technical era 40 years ago.
48. Looking now at the other possible candidates for the initial PIB implementation, all prove to be unsuitable for one reason or another:

-
- *Central government.* The government departments with which individuals must maintain a lifelong relationship are the Home Office (the Identity & Passport Service), the Department of Work & Pensions, the Department of Transport (DVLA), and Her Majesty's Revenue & Customs. These organisations already share personal data through the back-office, and thus are best regarded as different facets of a single organisation, with which the individual will maintain a single relationship and be identified by the ID card.
 - *Local authorities.* Current efforts to sort out the secure single-sign-on problem for local authorities (LAs) are being led by the Government Connects (GC) programme, and are based on the Government Gateway system used by central government. However, as described elsewhere in this document, GC's plans are immature. The picture is further complicated by the fact that LAs provide a wide range of services, sometimes acting as an agent of central government (e.g. for the administration of housing benefit), and sometimes as autonomous organisations. Thus, in the long run, a mix of back-office and citizen-mediated data sharing is indicated.
 - *Health.* In a different country, where there is a greater diversity of healthcare provision, and in 20 years time when most of the population will be technically literate, PIB could well be appropriate for the health care sector. Indeed a stripped-down version, using smart cards for authentication, is already used in France. But attempts to persuade the NHS of the merits of giving an individual control over his own records failed in 2003, and there is unlikely to be a further opportunity for some years.
 - *The social care and welfare service,* which is delivered by a consortium of public sector agencies (DWP, DfES, and local authorities). For child protection purposes, and in order to detect fraud, all these organisations can share personal data without explicit consent, and thus are best regarded as branches of the central government monolith.
 - *The financial services sector.* As stated earlier, a modern payment and credit reference system would look like distributed versions of Paypal and e-bay respectively, and would be consistent with PIB. But the banks designed their current systems some 40 years ago, before the advent of the internet, and – while they continue to make high profits – have scant incentive to change.
 - *The commercial sector (excluding financial services).* Even though there are clear applications for PIB in the private sector, such as intelligent mail redirection, permissioned marketing and secure single-sign-on, there is little prospect of ever developing sufficient consensus to allow PIB to reach critical mass.

Comparison of MIAP and PIB approaches

49. In the paragraphs below, we compare MIAP and PIB. We start by commenting about the efficacy of each approach in delivering against the 4 goals and claimed benefits of MIAP, as described in the business case [R2]. We then continue the comparison, using a number of further criteria.

'A true lifelong learner record' ?

50. The headline goal of MIAP is to 'provide a life-long record of all post-14 participation and achievement (and retention and destination within education) for every learner'. There are good reasons to doubt whether this is achievable using the proposed architecture:
- The scope of the current proposal requires the merger of data from just two pots: the National Pupil Database, which is held by DfES, and covers all learners in state-funded secondary schools; and the Individualised Learner Record, which is held by LSC and covers all learners in courses financed by that institution (essentially vocational and FE). Although there is an ambition to merge further pots of data to create a true life-long record, covering all learners, the MIAP business case states that to do so is *'feasible in the long-term'*, but *'there are too many practical unknowns for a reliable cost-benefit analysis and programme to be defined'*. Thus, despite the headline, we cannot be sure that the current project will produce anything other than a partial longitudinal record for that fraction of learners enrolled in state-funded secondary and FE courses.
 - Further, MIAP relies upon the ULN to facilitate record matching. It seems unlikely that learning providers and awarding bodies outside the direct control of DfES will be easily persuaded to adopt the ULN, or to contribute their data to the central store. These organisations are too numerous to ignore: the universities, especially the long-established ones, guard their

autonomy carefully; independent schools make up 7% of the total at primary and secondary levels; many learners study overseas for some part of their education; and much professional and vocational training is funded privately and overseen by autonomous professional bodies.

- o References can form a valuable part of an individual's record of learning and achievement, and are similar to qualifications, save that the awarding is another individual. MIAP does not offer the individual the capacity to request, store, or give access to references electronically.
- o Social networking websites, such as Myspace and Facebook, have shown that the success of personalised services depends on giving the user control over content and access. This is echoed in experience accumulated by the e-portfolio development community in the UK. There is a significant risk that the MIAP strategy of centralising data by fiat will alienate learners, and cause them to shun the service as far as they are able.

51. In contrast to MIAP, PIB is designed around the principles of user control and privacy, and is thus scaleable. Rather than have organisations aggregate data using back-office data sharing, each individual learner is empowered to aggregate data from learning providers, and others, to the extent that he finds it beneficial. And rather than use top-down funding, which results in a contractual straight jacket, PIB meets its costs by charging institutions transaction and periodic per-capita usage fees. Thus it can follow the learner wherever he or she wishes to go, and learning providers may well be persuaded to participate by customer expectation.

'Research & analysis'

52. A further goal of MIAP is to provide better data sets for research and analysis. DfES already maintains a National Pupil Database (NPD), which records factual details of every child in state education in England. Similarly the LSC gathers data about learners from the providers that it funds, to create an Individualised Learner Record (ILR). Both data sets would seem to be justified, at least in part, by the needs of statistical analysis.

53. MIAP can be seen as a natural progression from NPD and ILR, in that it will allow statistical analysis of learners' longitudinal records, across the secondary and FE sectors. Indeed, it may be that the desire for tracking and analysis is the principal driver behind the entire programme.

54. PIB offers a similar potential for rich analysis, although researchers may need to set about their tasks somewhat differently. A PIB permission hub can be regarded as an agent of the individual. In the network space, as in the real world, a researcher must ask the individual (or his agent) whether he is willing to provide data, and is more likely to get a positive response if anonymity is guaranteed. Practically, it should be possible to set up new permission-hubs with a default relationship to a statistical agency. Provided that the agency offers guarantees of anonymity, and is trusted, most individuals will allow such a relationship to persist, and the data gathered should be at least as good as that obtained from a MIAP-type scheme.

'Service Improvement', 'Efficiency Savings', and 'Bureaucracy reduction'

55. The fourth goal of MIAP is to deliver general improvements in efficiency and levels of service, coupled with a reduction in bureaucracy. There is an inherent contradiction here. While it is certainly possible to argue that a merger of independent data stores can deliver time savings, it is hard to argue that there will be a simultaneous reduction in bureaucracy – which is defined in the Oxford dictionary as 'government by *central* administration.' The best we can hope for is a reduction in 'red tape', i.e. the time required of citizens and organisations to comply with the requirements of ever-more centralised bureaucracy.

56. MIAP delivers efficiency savings by requiring independent organisations to behave as if all are part of a larger organisation. In contrast, PIB should deliver savings of equivalent or greater magnitude by empowering individuals to deal more effectively with *multiple, distinct*, organisations. By showing how efficiency can be achieved without centralisation, it is surely PIB that can justly claim to be the means of reducing bureaucracy.

'Wider strategic fit'

57. DfES claims that MIAP is justified, in part, by a fit with other DfES strategies or programmes. These are named as: 14-19; Success for All; E-Strategy; Skills Strategy; Vocational Qualifications Reform; FE Reform White Paper; New Relationship with Schools; UK Framework Development; Exam Deliver Integration Programme; and Agenda for Change.

-
58. While many of these initiatives are calling for, or delivering, radical change, there can only ever be modest changes to the nature of the fundamental relationships between learner, learning provider, and awarding body. Such changes as are evident include trends towards: (i) course-based assessment, as opposed assessment by final exam; and (ii) unitisation of courses, giving a learner the ability to build qualifications from fragmented learning experiences. Both trends emphasise the need for data sharing between organisations, but are agnostic about the methods used – either back-office, or learner-mediated.
59. Turning now to PIB, it too can claim to be consistent with the general thrust of DfES policy, in that it provides infrastructure for data sharing between institutions. But the concept is also of more general use, providing infrastructure to fix long-standing problems in the way that individuals interact with *multiple distinct* service providers, and other individuals, over electronic networks.
60. Perhaps the best example, since it is highest on DfES's own shopping list, is the Youth Opportunity Card (YOC). This new initiative is designed to give young people additional funds to spend on 'constructive activities', such as sport. It requires the development of a constrained payment system, i.e. one that will only allow participants to spend their YOC money at approved providers. To meet this need, the consultants working for DfES are proposing that a Paypal-type internet payment system should be developed. As matters stand, this will require yet another database of young people, and will have no link whatsoever to the MIAP databases. In contrast, PIB can easily be extended to offer payment functionality
61. Other problems addressed by PIB, but not by MIAP, include:
- *Secure authentication.* We lack a means to enable *multiple distinct* service providers to share the cost of securely authenticating the individual, while retaining – for privacy purposes – their own systems of identification. This is needed to allow an individual to access sensitive information (such as education, health and social care records) online, and may also play a part in improving the security of on-line banking, and the modernisation of payment systems. More on this later.
 - *Secure communication.* We lack the means to enable secure electronic communication between individual and service provider. E-mail is not secure, and so cannot easily be used for 'sensitive information', such as exam results, anything connected with exclusion, health, etc. Instant messaging and voice-over-IP are secure, but current systems are balkanised by commercial suppliers, and so cannot easily be used between the public sector and the citizen. PIB offers individuals and organisations the opportunity to select their own supplier of these services, and yet be assured of interoperability.
 - *Delegation.* We lack the infrastructure necessary to allow 'delegated authority', i.e. for an adult to act on behalf of a child, or an elderly relative. PIB addresses this issue by enabling an individual with a particular role (say parent, or teacher) to control the permission hub of a dependent, acting from his own permission hub. This will also fix the problem of how to give parents access to their child's electronic school records.
 - *Validation.* We lack the means to enable a relying party to validate claims by an individual about attributes for which third parties are the attribute authorities. PIB fixes this, and thus enables:
 - Validated CVs, as part of a national approach to e-portfolio
 - Instant CRB checks. Currently anyone seeking to work with children, or vulnerable adults, must undergo a CRB check before starting work. PIB will make it possible for someone with a positive, i.e. 'all-clear' check, to show this instantly to a potential employer, and for the employer to receive immediate updates should the situation change
 - Safer chat-rooms. Paedophiles have been known to 'groom' young people in internet chat rooms. PIB will make it possible to set-up up chat-rooms in which entry is restricted to individuals who can prove – without disclosing their full legal identity – that they are under a certain age (say 16).
 - *Updating of common personal attributes.* We lack the means to enable an individual to update common attributes (such as name, contact details, etc) held by *multiple distinct* service providers in one easy transaction. All current solutions to this problem (such as Plaxo, Linked in, etc) are balkanised by commercial suppliers, and so cannot easily be used between the public sector and the citizen. PIB offers individual and organisations the opportunity to select their own supplier of these services, and yet be assured of interoperability.
-

-
- *Calendaring.* Most organisations' IT systems offer calendaring functionality. But since this is not accessible to a user's friends and relations, who are outside the corporate perimeter, many users have to keep at least two calendars, one organisational and the other private. PIB fixes this by providing calendaring directly to the individual, who can then give access to whomsoever he sees fit, and download data to a personal device. This will be particularly useful as learning providers begin to automate timetabling, and make calendar information available to learners electronically.
 - *Mail redirection.* We lack the means to enable an individual to control the process of mail delivery, so that postmen do not continually attempt to deliver parcels and letters when no-one is at home, or to outdated addresses. PIB fixes this, using an application called 'Intelligent Mail Redirection'
 - *Permissioned marketing.* We lack an infrastructure that will enable an individual to control, and profit from, the desire of merchants to send them marketing material. PIB fixes this, using the Active Yellow Pages and Permissioned Direct Mail applications. The revenue generated may well pay for a significant part of the infrastructure's costs.
62. It is strange that DfES is so resistant to the idea of leading the development of PIB infrastructure for the benefit of society at large. The reason may be that IT developments – such as Customer Relationship Management – have traditionally been pioneered by the private sector, leaving public sector organisations to play catch-up. But the IT industry has now reached a point where network access is fast becoming ubiquitous, and thus there is a need for government to lead system design for the good of society at large, rather than just striving to achieve ever-more efficient internal processes.

e-learning

63. In 2005, DfES published its e-learning strategy, under the title 'Harnessing technology: Transforming learning and children's services' [R4]. One of the commitments in this document was to develop a national approach to what is called an 'e-portfolio', essentially an on-line space in which learners can store validated qualifications, samples of their own work, and reflections about their progress. In time, it is expected that a learner will use her e-portfolio to take exams, and to make applications, from school to university and then from university on into the workplace.
64. MIAP does not claim that its lifelong learner record is an 'e-portfolio'. However, it does maintain that the record will provide a qualification record 'component' of an e-portfolio service. This is dubious, at best. There has been no coherent attempt to explain how MIAP will be integrated with the other necessary components of an e-portfolio. And, although the UK e-portfolio development community is somewhat fragmented, there is agreement that top-down, centralised, approaches to the problem are not successful. Thus the level of support for MIAP in the e-learning community is close to zero, and the programme's claim of a strategic fit with the 'Harnessing Technology' e-learning agenda must be discounted.
65. In contrast, PIB is seen by some e-portfolio practitioners as consistent with current thinking in the community, particularly in its emphasis on the convergence between e-portfolio and techniques for user-centric identity management. An e-portfolio service based on PIB would: follow the learner from school to university and on into the workplace; allow easy integration of formal qualification data with references and informal reflection; and be useable as the fixed point from which a learner undergoes the various forms of e-assessment.

Attendance & location

66. One possible extension of MIAP, beyond the centralisation of qualification data, is to centralise – and act as a conduit for – attendance data. At present this is needed by DfES for the administration of the Education Maintenance Allowance (EMA), which is a payment of up to £30 a week made to young people between the ages of 16 and 19 who come from low-income families and choose to remain in full-time education. Actual daily attendance is a condition of payment, and so schools and colleges must forward attendance data to a central payment agency.
67. Because of the trend for learners to take courses, or course components, from more than learning provider, collection of this data is likely to become more complicated in the future. The ULN is seen as a way of reconciling attendance reports from different learning providers, and thus enabling efficient administration of the EMA. However, one might question whether the use

of centralised systems to track an individual's whereabouts is desirable, or in fact somewhat Orwellian.

68. The alternative is to adopt PIB, and so empower the learner to: (i) aggregate his own attendance data; (ii) request learning providers to correct any errors; and (iii) then share it with the EMA payment agency on a weekly or fortnightly basis. The agency could calculate the monies due, take bank account details from a different 'page' within the learner's brokerage account, and inform the learner in real time that a payment of a specified size would land in his account on a given date. As a means of motivating a learner to become computer-literate, reducing errors, and making explicit the link between attendance and payment, this approach would seem attractive.
69. As a final point, the network operators can now derive an individual's location from mobile 'phone signals. In certain circumstances, it may be both possible and desirable to infer attendance at a learning provider from location. In time, PIB should make it possible for a learner to combine such mobile location data with data from a conventional attendance register to create an enriched record for submission to the likes of the EMA payment agency. This flexibility would seem desirable, even though it may not be used for some years.

Authentication and Single-Sign-On

70. MIAP seems to regard learner authentication as a necessary nuisance, and will address the issue in the short-term by issuing learners with a further username and password, to be used to gain access to their learner record. Thus learners will be expected to remember separate usernames and passwords for every learning provider and awarding body with which they deal, and also for their new learner record.
71. This said, there does seem to be some acknowledgement within MIAP of a potential future need for a single-sign-on service, and for more secure methods of authentication. As an example, consider that a doctor's licence to practice, which is issued by the General Medical Council and logically forms part of his qualification record, may in the future be used as one of the criteria for access to health records.
72. To address these needs, the programme appears to be relying on the Government Connects (GC) initiative, which is tackling similar issues in the local government sector. However, this reliance may be misplaced, since GC's plans for its own sector are problematical, and become more so if extended across sectors.
73. Secure authentication requires that users be given a physical token (typically a smart card, or a one-time-password key-fob), to be used in addition to a shared secret (typically a password). GC is far from clear about how this is to be achieved in the local government sector.
 - o One possibility is that they will persuade every local authority (LA) to issue interoperable smart cards to its population. But (i) there is no sign that LAs are willing to bear the cost of such an approach; (ii) smart-cards cannot be used for remote authentication without a further card reader device; and (iii) learners may find it odd using an LA branded card to gain access to a learner record.
 - o A second idea is to rely upon the promised national ID Card. But (i) this will only be issued to individuals over 16, and so will miss the 14-15 year old group within the MIAP age-range; (ii) smart-cards cannot be used for remote authentication without a further card-reader device; and (iii) learners may find it odd using a card issued by the Identity and Passport Service to gain access to their education records.
74. Going further, the Information Commissioner has stated that general identifiers may be used within particular sectors, such as education or health, but should not be used in a cross-sector manner. Put otherwise, he does not wish to see the UK follow the US example, in which the social security number has become, by default, a general-purpose x-sector identifier. At present, GC does not appear to accept the legitimacy of multiple e-identities, and thus has not yet made a clear distinction between the processes of identification and authentication. Until it does so, and begins to offer an anonymous authentication service onto which other sectors can strap their own identification processes, there is little hope of compliance with the Commissioner's requirements.
75. Turning now to PIB, the concept was conceived on the basis that: (i) authentication and identification are separate processes; (ii) authentication is, potentially, a pure web service that can – and should – be outsourced to specialist authentication service providers; and (iii) that,

eventually, the logical suppliers of secure authentication are the mobile network operators, and perhaps the banks, who will develop the capability at low cost as a result of their other activities.

76. Further, PIB takes no position about the level of authentication required for any given application, save to observe that: (i) the risk of 'identity theft' - and thus the need for security - will rise with the number of relationships managed by the individual from any given point; and (ii) it makes better sense for a number of service providers to contribute towards a secure single-sign-on service, than for each to issue, and maintain, their own insecure username / password.

Policy neutrality

77. MIAP relies upon the ULN to match learner records. In contrast the PIB infrastructure permits institutions to require that learners proffer certain data fields, such as a ULN, but does not depend on the ULN for record-matching. Thus PIB, like any good design for IT infrastructure, is policy-neutral: it allows use of a unique identifier across certain parts of the education sector, but does not dictate such use.
78. Going further, MIAP seems to be predicated upon the current division of responsibilities between the various government departments. In the future HMRC or DWP could take over responsibility for the welfare aspects of the DfES's current remit by (i) financing schools through a voucher system; and (ii) delivering the Education Maintenance Allowance and student grants through the benefit or tax systems. Should this happen, the DfES's role would be simplified to that of sponsor of a (narrowly-defined) education system, and its need to 'know its customers' – as discussed above – would vanish. Good design for IT infrastructure should surely be neutral about such an arbitrary (and rapidly changing) thing as departmental remits. MIAP is not, whereas PIB is.

Business model

79. MIAP has been conceived as another top-down public-sector IT project, to be financed principally by large and ongoing subventions from the Treasury. There are provisions in the procurement specification suggesting that some beneficiaries may be required to pay for MIAP services in the future, but these are ill-defined.
80. The use of central funding in this way may well prove to be a further constraint on the scalability of the MIAP proposal. Not only will it be difficult to persuade learning providers outside the direct control of DfES to use the ULN, it will also be hard to justify spending public money on the incorporation of their results within the state-sponsored qualification record.
81. An analogy with payment systems may be useful. The MIAP proposal is akin to HMRC creating a payment system, say the equivalent of Maestro / Switch, to be used solely by individuals when paying their annual tax bill. And, instead of accepting shared ownership and adopting a transaction-fee business model (as all electronic payment systems to date have done), HMRC insists on letting a top-down contract to a system integration house for a turnkey solution. Yes, the result may meet HMRC's immediate needs. But it is an expensive, and inconvenient, substitute for a well-designed system that could be used by an individual to pay anyone for anything.
82. A further analogy, this time with the postal system, may also help. At some point in the development of the postal system, government may well have considered whether it made better sense to: (i) persist with a wholly-controlled, centrally financed, government mail system, to be used for delivery of letters between public sector organisations, and those sent by such organisations to the public; or (ii) develop the general post office, which is financed by transaction fees, and tasked with the delivery of all letters, regardless of origin or destination. It is evident now that the second option was the more sensible. Similarly, in a few years' time, the choice between PIB and MIAP may appear obvious.
83. Unlike MIAP, and like the postal system, PIB is funded on a transaction fee basis, and thus is infinitely extensible. The proposition for learning providers is simple: pay a small fee per learner per year, and receive a wide variety of necessary learner-centric services, as detailed above. The question for DfES is whether it wishes merely to develop systems essentially for its own use, or whether it is willing to work with others on the bigger problem of developing true user-centric multi-application IT infrastructure, for use throughout the entire education sector and further afield.

Support for the less able.

84. One possible criticism of PIB is that, while it is clearly suitable for those individuals who are computer literate and able to take responsibility for their own education, it is less suitable for those among us who are disabled in some way. According to this line of thinking, MIAP is to be preferred because it takes responsibility away from the individual, and prepares a qualification record for everyone, able and disabled alike
85. In reply, we would say that PIB is designed to allow a guardian, parent, carer, or support teacher to manage a permission-hub on behalf a dependent individual. And it is surely better to place responsibility for the education of such an individual clearly in the hands of a named individual, rather than rely upon the impersonal hand of state for the same task.

Cost

86. As a final point in this comparison of MIAP and PIB, we come to cost. MIAP is a top-down public sector IT project, to be funded by direct and ongoing subventions from the Treasury. PIB, in contrast, is infrastructure for society at large and will be funded by transaction payments made by the various beneficiaries, without the need for ongoing Treasury subventions. And because the range of applications for PIB is so much greater than for MIAP, the cost per application should be significantly lower.

Conclusion

87. By combining its roles as a sponsor of the education sector and as an agency delivering welfare payments, the DfES is at risk of developing – under the MIAP programme – infrastructure for inter-organisational data sharing that is inappropriate for the (narrowly-defined) education sector, conflicts sharply with the sector’s history of user-centric permissioned sharing, and impedes the development of PIB infrastructure that is needed by society at large. DfES should pause, and review the options, before proceeding.
-

References

R1	Submission to the House of Lords S & T Committee enquiry into Personal Internet Security, led by Eidentity with support from a grouping of senior individuals from the fields of computer science, telecoms, education and information security. Available from www.edentity.co.uk .
R2	MIAP Strategic Business Case, version 1.1, dated 7 Aug 2006, available from DfES.
R3	'Children's Databases – Safety & Privacy', a report prepared by the Foundation for Information Policy Research for the Information Commissioner. Available from www.fipr.org
R4	'Harnessing Technology: Transforming Learning & Children's Services', published by DfES in 2005. Available from www.dfes.gov.uk
R5	'Every child matters', a green paper published by Her Majesty's Government in 2003. More information available from www.everychildmatters.gov.uk

Annex A: Financial systems

1. For the purposes of learning how 'to do e-government', the financial sector is a mixed blessing. On one hand, it has spent a lot of money, and achieved a very high degree of task automation. But on the other, the major decisions about the architecture of the current financial infrastructure were taken back in the 1960s, and thus take no account of the potential impact of the internet and mobile phones – which together, and for the first time, give the individual secure electronic access to the rest-of-the-world.
2. Banks deal with two kinds of data. The first is money itself, which can be regarded as both anonymous (digits in a bank account say little about a person), and personal (in that they belong to someone). Ownership is important, since only the owner has the right to dispose of the money. To determine ownership, the banks rely principally on authenticating an individual against their own register of customers. They have no need to prove legal identity, perhaps by inspecting a national ID card, whenever an individual wishes to pay for something. As evidence of this, note that the predominant financial authentication method, the use of a chip-card and PIN, tells a merchant nothing about the legal identity of a customer.
3. The other kind of financial data sharing concerns information about the way in which an individual has conducted an account. The banks' main motivation is a desire to improve lending decisions, based on knowledge of an individual's credit history. Back in the 1960s, when the design decisions were taken, individuals did not have network access, and so the banks had little choice but to create the credit-reference system as we now know it. Each bank contributes records about the conduct of accounts to a credit reference agency, which uses sophisticated algorithms to match them up and so create an aggregate record. The contributing banks can then request sight of a customer's aggregate record when necessary.
4. Note that the credit reference system can, in theory, work well even for an individual who is known to banks by a name that is not consistent his national identity card. What is important in credit reference is not legal identity, but rather consistency of name and address information over a number of years, and across a number of well-conducted financial accounts.
5. Note, also, that anyone designing financial systems from scratch in the modern day would not repeat the decisions taken 40 years ago, when the current payment and credit reference systems were designed. Paypal shows how the internet enables individuals to make secure, immediate, person-to-person payments, and contrasts sharply with the 3-day account-to-account service still offered by the retail banks. And e-bay shows how individuals with network access can build an online reputation as a trusted buyer or seller, without any reference to legal identity.
6. The one reason why banks require absolute proof of legal identity is to ensure compliance with the 'Know your customer' regulations. These were introduced some years ago by the government in order to combat money-laundering. There is no equivalent of money-laundering in the education sector; nor, for that matter, is there any significant evidence of one individual impersonating another in order to obtain, or benefit, from educational qualifications,
7. In pursuing the current MIAP plans, the DfES seem to be trying to emulate architecture for the financial services sector that is outdated, and in need of reform. Why such reform is blocked is an interesting question. The short answer would seem to be that (i) since the banks have a system that is 'good enough' and enables them to make significant profits without major capital investment, many must think 'Why change it?'; and (ii) payment systems development requires consensus, and thus laggards can frustrate progress by the entire industry. This said, the banks are now finally updating their systems to provide 'immediate payments', rather than persisting with the 3-day BACS payment cycle.

Annex B: Social care systems

1. In the past few years, there have been major developments in government policy re the protection of children, and the promotion of their welfare. The implementation of policy has required significant IT investment to enable data sharing. A fair overview is provided in a report [R3] prepared by the FIPR for the Information Commissioner.
2. In summary, it would seem that there are two main strands of thinking in this area. The government has long accepted a responsibility to protect children from actual physical harm. In consequence, the agencies providing children's services recognise that they have a duty to share information, with or without consent, whenever there are child-protection concerns. This duty was emphasised by the 2003 Laming report into the tragic death of a young girl, Victoria Climbié.
3. The second strand of thinking, about the welfare of children, is relatively new. In the 2003 Green Paper, 'Every Child Matters (ECM) [R5]', the government stated that *'We need to shift away from associating parenting support with crisis interventions to a more consistent offer of parenting support throughout a child and young person's life.'*
4. ECM marked a dramatic growth in the government's ambition for children's services. It now aims to ensure that all children, whatever their background or circumstances, have the support they need to: be healthy; stay safe; enjoy and achieve; make a positive contribution; and achieve economic well-being. To achieve these goals, government believes it necessary to take a more active, interventionist, approach to child development, and thus to family life.
5. Since intervention requires information, much effort has been devoted to creating IT systems that will collect data, and then enable professionals in children's services to share it more effectively. To summarise the key components, which are at varying stages of development:
 - o Common Assessment Framework (eCAF) – a standard, IT-enabled data collection template, to be completed by any professional who considers that a child has needs that require the involvement of other services.
 - o Integrated Children's System (ICS) – an electronic case management system for workers in social care.
 - o CCICS and APIR – these databases are used by the local Connexions services, which replaced the Careers Advisory Service in 2000. CCICS is a listing of all young people (>13) in the local area; while APIR is a case-management system used by a Connexions personal adviser when working with a young person.
 - o Information Sharing Index (IS Index) – a new database that will contain (i) basic details (name, address, contact) for every child in England; (ii) for each child, the names and contact details of every professional in contact with him or her; and (iii) an ability for a professional to flag concern about a child, and thus a desire to collaborate with other agencies. The database is to be divided into segments, each to be administered by a local authority.
6. Most of these new systems can be seen as necessary initiatives to standardise and modernise professional practice that has evolved over many years. ICS and APIR are simply case management systems for social-work and career-advice professionals respectively. And CAF standardise the language and format of existing tools for data sharing.
7. CCICS and IS Index are, however, intended to be comprehensive databases of all young people, within certain age ranges, in a particular area. As such, they represent a departure from traditional practice, and merit some comment. The first obvious point is that the systems overlap, and it seems likely that the Connexions Service will eventually use IS Index, rather than maintain their own, less comprehensive, database of potential clients.
8. Focusing now on IS Index, this project had its genesis in 2002 when John Denham, the minister for Children and Young People at the Home Office, announced what was initially referred to as the 'Identification, Referral and Tracking' (IRT) system. It was intended to identify children at risk of offending, drug taking, and teenage pregnancy.
9. Subsequently, responsibility for the project was transferred to DfES, a statutory basis was established in the Children Act 2004, and a less Orwellian name was (thankfully) devised. Note also that ministers have justified the project as a means of preventing a repetition of the Climbié tragedy. However, FIPR points out that the professionals in that case were aware of each other's

involvement; their failure to act had other causes. What IS Index will do is provide a professional with an alternative to asking a child's parents about other services/ help that they may be receiving.

10. Although no official pronouncements have been made, IS Index (or its equivalents in the devolved administrations) can be seen as a natural complement to the proposed Identity Card Register. Together, they will provide complete coverage of the UK population, the first capturing everyone between the ages of 0 and 16; and the second everyone from 16 upwards. We will finally have what amounts to a population register. This is long overdue.
