PIB-d Ltd: a joint-venture between
the HE sector and entrepreneurs

Giving individuals (initially students) control of their own data (including identity)

. . **both** to enhance their privacy and convenience and to drive efficiencies across the HE, public, & private sectors

November 2013 (a revision to the original, as issued in February 2013)

About PIB-d Ltd

PIB-d is a start-up company, specialising in the design and development of an ecosystem to enable individuals to control the use of their personal data (including identity). Such ecosystems are expected to increase individuals' convenience and privacy while, at the same time, improving data quality and reducing costs for the organisations that serve them.

PIB-d is a joint-venture, part owned by organisations within the Higher Education sector (JISC and the University of Hertfordshire) and part by entrepreneurs – who have led several preliminary initiatives in the identity and personal-data fields, notably (i) the 2008 'Work Group on User-Centric Identity & Personal Information Management', as sponsored by the Information Commissioner's Office and the Technology Strategy Board; and (ii) a group submission to the 2006 House of Lords Science & Technology Committee enquiry into Personal Internet Security. Copies of both reports can be downloaded from www.pib-d.net.

Acknowledgements

PIB-d thanks the many people, both at the University of Hertfordshire and elsewhere, who have given their time to help us develop the project to this stage. We also acknowledge, with gratitude, receipt of grant funding from the Technology Strategy Board.

Scope of - and intended readership of - this paper

This proposal is aimed, initially, at (i) the Higher Education (HE) sector in England; and (ii) public sector entities in England which are adjacent to the HE sector. However, we believe that the ideas are generally applicable, in both public and private sector contexts.

Version Control

Version	*Date*	*Comment*
5.04	Nov 2013	Minor mods to title page
5.03	20 Mar 2013	Certain paras moved to new Annex J; revised Annex C; readability changes.
5.01	21 Feb 2013	Minor changes to improve readability
5.0	12 Feb 2013	Finalised. Approved for restricted circulation.

Contact details

PIB-d Ltd	95A Kidmore Road, Caversham, Reading, RG4 7NH
Telephone:	07801 231 693
E-mail:	john.harrison@pib-d.net
Web:	www.pib-d.net

Contents

Annexes

© PIB-d Ltd 2013

This page has been left blank intentionally.

Summary

This paper describes a proposal to give individuals better control of their own personal information (including identity), starting in the Higher Education (HE) sector and, by so doing: (i) improve their privacy and convenience; and (ii) drive efficiencies in – and provide useful new functionality for - the HE, public and private sectors.

The proposal is consistent with - and indeed takes forward - relevant initiatives being run by central government, specifically the Identity Assurance Programme, Open Data, Midata, and an emerging industrial policy that emphasises the importance of industry-university collaboration and of building on areas of strength. Indeed the strength of the UK's HE sector, and its success in developing shared services (such as UCAS), makes this country a suitable launch-pad for new user-controlled infrastructure that could spread globally. The creation in 2011 of PIB-d Ltd, this paper's author, as a tentative joint venture between parts of the HE sector and entrepreneurs was a good first step.

We envisage that individuals will choose a 'personal information broker' (also known as a 'user attribute agent', a 'personal data store', and a 'personal cloud') from a managed market, or ecosystem, and then use their broker account to: (i) link to, and communicate with, multiple counterparties, both organisations (initially universities) and other individuals (initially other students); and (ii) give explicit permission for the transmission of personal information to, and between, such counterparties.

The new ecosystem offers benefits to all parties. Organisations will see increased data quality, lower operating costs, better targeted marketing, and easier compliance with forthcoming changes to the data protection regulations. In particular, universities will:

- benefit from persistent electronic relationships with their students, all the way from initial enquiry, through application, student life, time as an alumnus, and possible return for postgraduate education;
- gain shared infrastructure suitable for the ongoing shift towards distance / on-line learning.
- begin to move towards a position in which costs can be saved by paying just once for an appropriately secure online relationship with an individual, to be used as a combined channel for personal data, payment and communication

Meanwhile students will gain: (i) a coherent, modern approach to a portable personal electronic record, one that is backward compatible with the Learning Records Service; (ii) a modern alternative to the proprietary social networks, offering far better privacy and superior functionality; and (iii) distributed and interoperable approaches to common online services, such as authentication, calendar, payment, and communication.

If successful in HE, the ecosystem will likely expand down to secondary education; be used for the transitions from school to university, and from education to employment; and also be used for proof of key-identity-attributes to central government, reverse / permissioned marketing applications, and for proof-of-age as required for online purchases and safer social networking. This broad range of uses should render the ecosystem far more cost-effective than the single-purpose systems that currently serve individual sectors. Indeed, the private sector will fund a significant proportion of both capital and running costs because of the potential, once the ecosystem has reached scale, for re-use in the commercial sectors and for export to other countries.

To take the project forward, there is now a need to open the discussion to a broader set of stakeholders, to include: (i) ministers, special advisers and civil servants in central government; (ii) further universities and the remaining HE-sector-wide institutions (in addition to PIB's development partners, the University of Hertfordshire and JISC); (iii) potential brokers; (iv) potential software suppliers; (v) potential financiers of development; and (vi) subject experts, to double-check the privacy and security aspects of the existing technical design.

Invention is easy; but real innovation in this field is only possible when the lead customers – the HE and public sectors - are willing to move forward.

This page has been left blank intentionally.

Foreword on behalf of the University of Hertfordshire

The University of Hertfordshire was pleased to participate in the PIB feasibility study, which has built successfully on an initial concept for a new approach to personal data management, starting in the HE sector. The study was part funded by the Technology Strategy Board and carried out through by a joint venture between independent entrepreneurs, the University and JISC.

PIB aims to address a major issue of growing concern and importance – giving individuals better control of their personal information and its validated use. With the growth of the internet economy and the commercial development of 'Big Data' for competitive advantage, PIB offers a potential regulated and secure 'personal data ecosystem' for our future online world, as well as some interesting possibilities for reducing duplication of effort and increased efficiencies for organisations.

Through the study, the first step has been taken towards fleshing out PIB and identifying its possible parameters and benefits. But it is now clear that wider engagement, expert contributions and further investment are needed if the concept is to step from the drawing board towards realisation.

We invite you to read this paper and reflect on the PIB concept's future potential and benefits for both individuals and public services. We hope you will then open a discussion with John Harrison* with your comments and suggestions.

Professor Di Martin	Professor Bruce Christianson
Chief Information Officer	Head of the Centre for Computer Science and Informatics Research
University of Hertfordshire	University of Hertfordshire

**Contact details on page ii*

© PIB-d Ltd 2013

This page has been left blank intentionally.

Foreword by Matthew Dovey on behalf of JISC

JISC's vision is to make the UK the most digitally advanced education and research nation in the world.

Our investment in PIB-d Ltd, made in 2011, was part of our programme of innovation in access and identity management, and supplemented grant funding from the Technical Strategy Board.

PIB-d seeks to create a new kind of 'user-centric' infrastructure, starting in the HE sector. The company believes that this new infrastructure is both necessary and potentially very useful, but cannot be developed by conventional means: a typical start-up might have the ideas, but could never win cooperation from established organisations quickly enough; and established organisations tend to view the IT landscape from their own perspective, and so would not see the user-centric opportunity.

Further, PIB-d points that it is only the education sector that measures success by its ability to move customers on, giving each one new personal information - qualifications - that are meant to be shown to other parties. Since most other sectors try to, or behave as if they will, retain their customers indefinitely, and thus have scant motivation to share their customer records, education is particularly suitable as a launch pad for user-controlled data sharing.

There's also a point about values. John Naughton, Emeritus Professor of the Public Understanding of Technology at the Open University, maintains that the successes of the internet and the world-wide-web can be ascribed, in large part, to the values of the academics who created them. They designed for - and achieved - openness, distribution, and scalability. It may be that our generation can do a similarly good job, this time working closely with the private sector to ensure the 'identity layer' needed by the internet/ web is not only open, distributed and scalable, but also privacy-enhancing and well suited to the needs of the HE sector.

We encourage you to provide feedback on the proposal direct to John Harrison of PIB-d. His contact details are given on page (ii).

Matthew Dovey
Programme Director for Digital Infrastructure, JISC

[#] 'A brief history of the future', John Naughton, ISBN-10: 075381093X

This page has been left blank intentionally.

Introduction

1 Now that broadband is approaching ubiquity, and many people have their own personal computing devices, there is an opportunity for collaboration between the Higher Education (HE) sector and the private sector in the UK to create a new kind of electronic infrastructure, one that places individuals, initially students, at the centre - and in control - of the flows of their personal information.

2 If successful, the result would be greater convenience and privacy for individuals, a radically simpler information architecture for the HE sector, and the triple benefit of enhanced data quality, lower operating costs, and improved functionality, for its constituent organisations. Further, the private sector would bear a substantial proportion of the capital and operational costs, because of: (i) the potential for re-use of the same infrastructure in other sectors, and as a tool for collaboration between universities and industry; and (ii) cost savings resulting from the streamlining of the recruitment process following university.

3 The idea is simple: an individual should be able to choose a ‘personal information broker’ from a managed online market, and then use his broker account to: (i) link to, and communicate with, multiple counterparties, both organisations (initially universities) and other individuals (initially fellow students); and (ii) give explicit permission for the transmission of trustworthy personal information to, and between, such counterparties. Candidates for the broker role are banks, mobile network operators, start-ups, and – possibly – the current web-majors, such as Google, Facebook and Linked-In.

4 Note that terminology in this field remains in flux. Our working name for the new managed market, or ecosystem, is ‘Personal Information Brokerage’, but other current terms - in what is a fast developing area - include ‘personal data store’, ‘personal data ecosystem’, ‘user attribute agent’, ‘personal cloud’, and ‘life management platform’. Since none of these terms exactly suit the need, we are open to suggestions for change. But, for simplicity, we will use the PIB phrase throughout this paper.

5 PIB-d Ltd, the joint-venture company set up to explore this opportunity, is now nearing the end of its initial feasibility study. In this proposal, intended for discussion with central government departments, we describe the issues – for universities, students, and at the sectoral level - when dealing with personal data, mention current initiatives that provide partial solutions, outline the design of a new ecosystem of brokers to address the bigger picture, describe a phased approach to implementation, show that the proposal is consistent with government initiatives in others areas, describe other applications for the ecosystem outside HE, and propose a series of discussions to develop the consensus necessary for a pilot. But we start with the background.

Background

6 The entrepreneurs behind PIB-d began work in this area some years ago, initially under the banner of an earlier start-up, Edentity Ltd. We carried out some consulting work, and wrote two papers that received reasonable support: the first was a submission to the 2006 House of Lords’ Science & Technology Committee enquiry into personal internet security; and the second the 2008 report of the ‘Work Group on User-Centric Identity (& Personal Information) Management’ as sponsored by the Information Commissioner and the Technology Strategy Board. Copies of both can be obtained from PIB-d’s website[1].

7 In the course of that initial work, we recognised that collaboration across sectoral boundaries was a pre-requisite for progress, and so were delighted when the Technology Strategy Board

[1] See http://www.pib-d.net/

offered grant funding towards the costs of an initial feasibility study. This success helped convince JISC and the University of Hertfordshire to join with us to form - in August 2011 - a tentative joint venture, PIB-d Ltd. The company's initial remit was to determine the feasibility, in both business and technical terms, of a pilot of PIB in the HE sector. Because we are a joint-venture, we can do things differently, both issuing papers (such as this one) inviting discussion, and also - if there is support - raising funding from across the HE, public and private sectors to take the project forward.

Issues - for universities, students, and at the sector level

8 PIB-d worked with staff and students at the University of Hertfordshire (UH) to identify current flows of personal information across the UH perimeter, and agree what works well, and where there is scope for improvement. In the notes below, we summarise the issues as seen by the university as a business, in its teaching role, and in its research role. We then look through the eyes of students, and finally look at the picture of data flows across the HE system as a whole.

Issues for the university as a business

9 Like any other organisation, UH has to ensure that it functions efficiently as a business, and so is always keen to reduce costs and improve communications with potential customers. In discussions about potential applications of the new infrastructure, five areas for improvement were identified:

- Duplicate records. A single individual may have multiple relationships with a university, either concurrently or sequentially. For example she may, at various times, be an applicant, a current student, a short-course participant, an alumnus, an employer, or a placement supervisor for other students. These multiple relationships, and their different timings, can easily lead to multiple records on a university's corporate system, resulting in both a poor experience for the individual, and significant costs as the university checks for, and eliminates, duplicate records.
- Inaccurate contact details. The university wishes to maintain contact with its alumni, but – because they now have other preoccupations – many neglect to notify the university when contact details, such as street or e-mail addresses, change.
- Ad-hoc requests for proof of qualifications. Staff spend considerable amounts of time responding manually to requests from recruiters for confirmation of an alumnus's qualification, or simply the fact of attendance at the university. (The pros and cons of DARE, as a solution to this issue, are discussed in Annex J).
- Transitions following completion of undergraduate study. The issue with ad-hoc requests for proof of qualifications is, in fact, a symptom of a broader problem: that there is no coordinated system for use by individuals to apply for their next activity – whether postgraduate study or employment – following an undergraduate course. Many individuals make multiple applications, calling upon essentially the same information; and the organisations receiving the applications must go through similar routines to check and validate such information.
- Cost reduction. In the current economic climate, UH - like every other organisation - is searching for ways to reduce operating costs. The university can see the potential for cost savings by paying for a single service that will supply application data, maintain the currency of contact data, and – where necessary – validate identity.

Issues for the university in its teaching role

10 Like other universities, UH now offers some courses via online distance learning, and sees the new channel as being increasingly important in the future. Development was led by the School of Computer Science, which has now just conferred its thousandth online BSc degree. The schools of law, business studies, and environmental management are now following suit.

11 Looking at online learning more generally, Martin Bean, vice-chancellor of the Open University, describes[2] - perhaps using a little hyperbole - the present time as ‘the Napster moment’ for higher education. Online provision is growing fast, driven both by increased online offerings by established universities and by the entrance of new university-based ventures, such as Coursera, edX, and Udacity in the USA, and by FutureLearn in the UK. Eduventures, a US consulting firm, estimates that - by 2014 - 20% of all students (both undergraduates and masters) in the USA will enrol on fully-online programmes. Precise figures for the UK are not available, and may well be smaller, but the trend is clear. Further detail, and references, are given in Annex A.

12 All of the organisations offering on-line courses face a common set of infrastructural problems. Because their Virtual Learning Environments (VLE) are all standalone ‘stovepipes’, the organisations have no easy way to prove the ‘real’ identity of their online students, either at registration or when taking exams; nor can they give successful students electronic qualifications in a form that can be combined into a validated CV and shown to any counterparty of their choice. Further, the ‘stovepipe’ nature of the VLEs means that the common services that they offer - such as communication, calendar and groups - can only be used between academics and students registered on the same VLE, rather than as general purpose tools to enable relationships between an individual and any counterparty.

Issues for the university in its research role

13 Researchers at UH needs to collaborate with other researchers, both at other universities and in industry. Thus there is a need for individuals, from different organisations, to work together as a ‘virtual team’, or a ‘virtual organisation’, using software tools to collaborate and share proprietary /confidential information securely. As yet there is no standard set of software tools for these purposes, and so every collaboration requires agreement on an ad-hoc approach. There is clear scope for improvement.

Issues for students

14 For students, whom we engaged with both in a focus group setting and more casually, the areas of immediate concern are rather different:

- Authentication. In common with the majority of the population, students dislike having to remember a further username and password to gain access to each new IT service (such as the university’s IT systems), and would welcome a more user-friendly approach.
- Coherent communications. Many students prefer not to use e-mail, communicating between themselves via a social network account and SMS text messaging. And yet e-mail, together with its own enterprise messaging system, remain a university’s principal channels of communication with current students. Although SMS and the social networks are being used increasingly for digital marketing and keeping in touch with alumni, it could be said that the overall picture lacks coherence and integration.
- Privacy. According to a survey by McCann Erickson, summarised in Annex H, 65% of the total population are concerned about privacy, and would like greater control over their own data. Students are likely to share these concerns, and so will expect institutions – throughout the HE sector, as elsewhere - to allow them online access to, and control over, their personal data.
- Personal education record. Students, when asked, consider it strange that they still have not been given a way to collect qualifications and certificates electronically, much as they can do using paper.

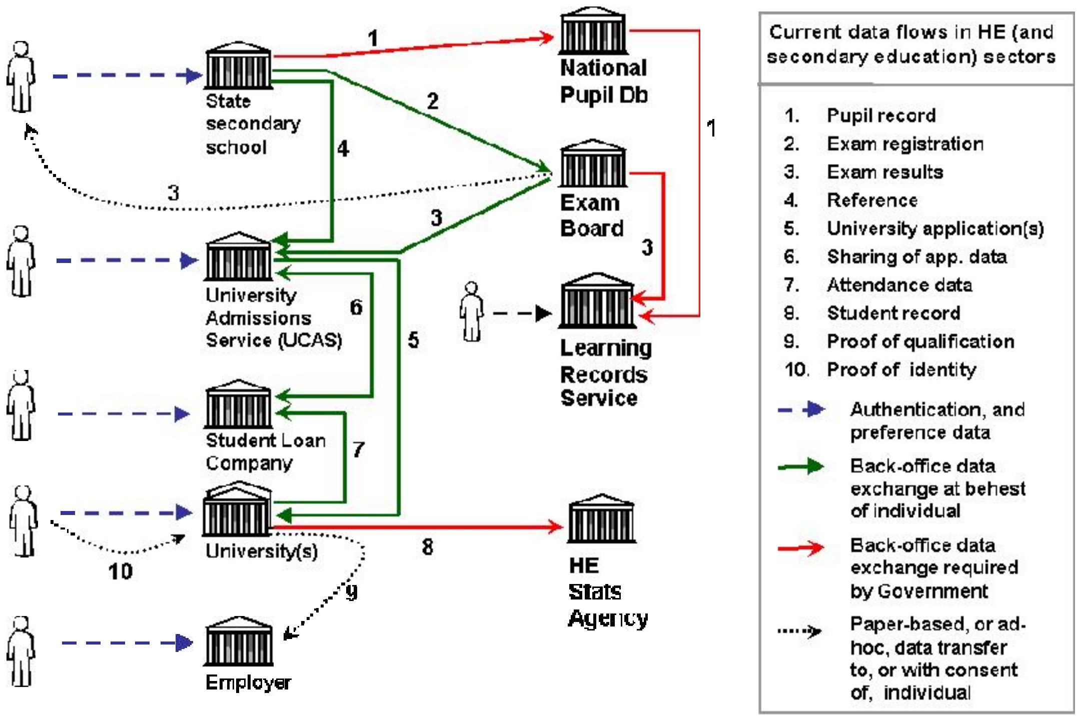
[2] See http://www.guardian.co.uk/education/2012/dec/03/massive-online-open-courses-universities

- Calendar. Many students now use an online calendar, synched to a calendar application on their smart phone. It would be useful if a university could be given permission to write time-table commitments to this calendar, rather than – as many currently do – merely place such commitments in a single purpose calendar within a student's university IT account.
- Update of contact details. Many students now use social networks to update friends and family about changes, such as a change of address or contact details. They would find it convenient to able to update the university's records at the same time, but are – instead – required to log-in to the university's student record system for the purpose. Many forget, particularly alumni for whom the university may not be front-of-mind.
- Proof of student status. Students would find it convenient to have a cheap and ubiquitous way of proving their student status online, as required to prove eligibility for merchant discounts. Current schemes, such as the NUS Extra card, must be paid for, and are incomplete in their coverage.
- Proof of age. Although not strictly an education issue, merchants are required to check that an individual purchasing certain goods – such as alcohol – is above the statutory minimum age. They, and students as their customers, would welcome better - i.e. cheaper and more ubiquitous – ways of doing this.

15 At the heart of students' concerns is the fact that they have moved on, beyond e-mail and simple web sites, to a new world of online interaction over the social networks. Yes, they may be concerned about privacy on these networks, but they wish to go forward, not revert to the old way of doing things. The universities are aware of this shift, and are experimenting with new approaches, but – for reasons of security, trust, lack of supplier choice, lack of account portability, and product bundling – they cannot simply invite students to use the social networks as a front-end to their own IT systems. More detail on this in Annex G.

Issues at the sectoral level

16 As well as looking at the issues faced by individual universities and students, PIB-d also studied the pattern of - and logic for - data flows in the education system as a whole. Our findings are shown in the graphic below, and are best conveyed by describing the experience of an individual as she progresses from secondary school to university and then into the workplace.


State secondary school
National Pupil Db
Exam Board
University Admissions Service (UCAS)
Learning Records Service
Student Loan Company
University(s)
HE Stats Agency
Employer
1
2
3
4
5
6
7
8
9
10
Current data flows in HE (and secondary education) sectors
1. Pupil record
2. Exam registration
3. Exam results
4. Reference
5. University application(s)
6. Sharing of app. data
7. Attendance data
8. Student record
9. Proof of qualification
10. Proof of identity
Authentication, and preference data
Back-office data exchange at behest of individual
Back-office data exchange required by Government
Paper-based, or ad-hoc, data transfer to, or with consent of, individual

- Once an individual has taken GCSE exams, her results are returned to her as a paper certificate, but also sent by the examination board for storage in electronic format on a government database, the Learning Records Service (LRS).
- A year or so later, she takes A-level exams, and applies to university. Her A-level results are, again returned to her on paper, and again spirited away for storage in electronic form on the LRS database.
- But this time, the exam board also sends copies to UCAS, which forwards them to any universities who have made her a conditional offer of a place. Having forwarded the exam results, UCAS (presumably) deletes its copies, while the university which the pupil eventually attends may keep a copy on file, but makes no further use of it.
- During, and at the end of her degree course, the university sends copies of personal data, including results of university exams and coursework, to the Higher Education Statistics Authority, which stores them on another central database, this time to be used mainly for statistical analysis. HESA will not allow recruiters to access this information, even if authorised by the student, because such use would lie outside the purpose for which the data was collected.
- Upon completion of the degree course, the university gives the individual a degree certificate on paper, but does not send an electronic copy to the Learning Records Service. Instead, the university may - if it has implemented DARE (see Annex J) - give the student the means to show others her degree certificate in electronic form, provided that she retains and remembers her university username and password.

17 For individuals, the situation described above is far from satisfactory. They still do not feel ownership of, and control over, a single electronic qualification record, allowing them to use a single set of software tools to create and share trustworthy CVs as they apply from school to university, and from university to employers. Instead their data is spirited away and stored in centralised databases over which they have no sense of ownership, and which they do not use.

18 Meanwhile universities receive qualification data from UCAS, send their qualification data to HESA, and still have to respond to ad-hoc requests from recruiters, or install another system (DARE) to automate the process. And there is little evidence of thought about, or preparation for, a future in which distance learning may become as important as traditional face-to-face teaching. PIB-d suggests that there is a better approach, based not on building ever larger central databases, but on building infrastructure to give individuals control of trustworthy personal information.

In summary

19 All these issues – as faced by universities, by students, and at the sectoral level – can be regarded as symptoms of an underlying problem: that the online world has yet to develop a general-purpose trust infrastructure that allows individuals to show trustworthy personal information, recorded about them by one counterparty, to another. Offline, everyone is familiar with using paper certificates - such as passports, exam certificates, and prescriptions – for this purpose. But, as yet, there is no online infrastructure to do same job, even though the necessary technology has been available for some years.

20 Fixing the problem requires cooperation between different cultures. Internet entrepreneurs like to make progress quickly; whereas the organisations that hold the kind of trusted information that individuals might wish to show to others online are, typically, long-established, and rightly cautious about adopting new technologies, particularly when associated with new procurement, business and organisational models. Some are experimenting with 'point' solutions that treat one or more of the symptoms above: examples include Dare, Moonshot and Office365, as described in more detail in Annex J. But few have begun to see the problem from the point of view of the individual, who needs the new infrastructure to deal with multiple organisations and give permission for the transfer of personal information between them.

Designing a user-control ecosystem

21 Entrepreneurs have now been working on better approaches to personal data for some years, and there is general agreement that the requirements cannot be fixed by creating new stand-alone businesses. Rather there is a need for a new industry, or infrastructure, or 'ecosystem'.

22 Work to create this industry is being led by PIB-d, and by other start-ups in the USA and the Netherlands. We are making reasonable progress, as can be seen from the industry overview given in Annex B. But problems still remain, not least a clear route to critical mass. The following notes describe the emerging consensus about the requirements, and the way to meet them.

Requirements

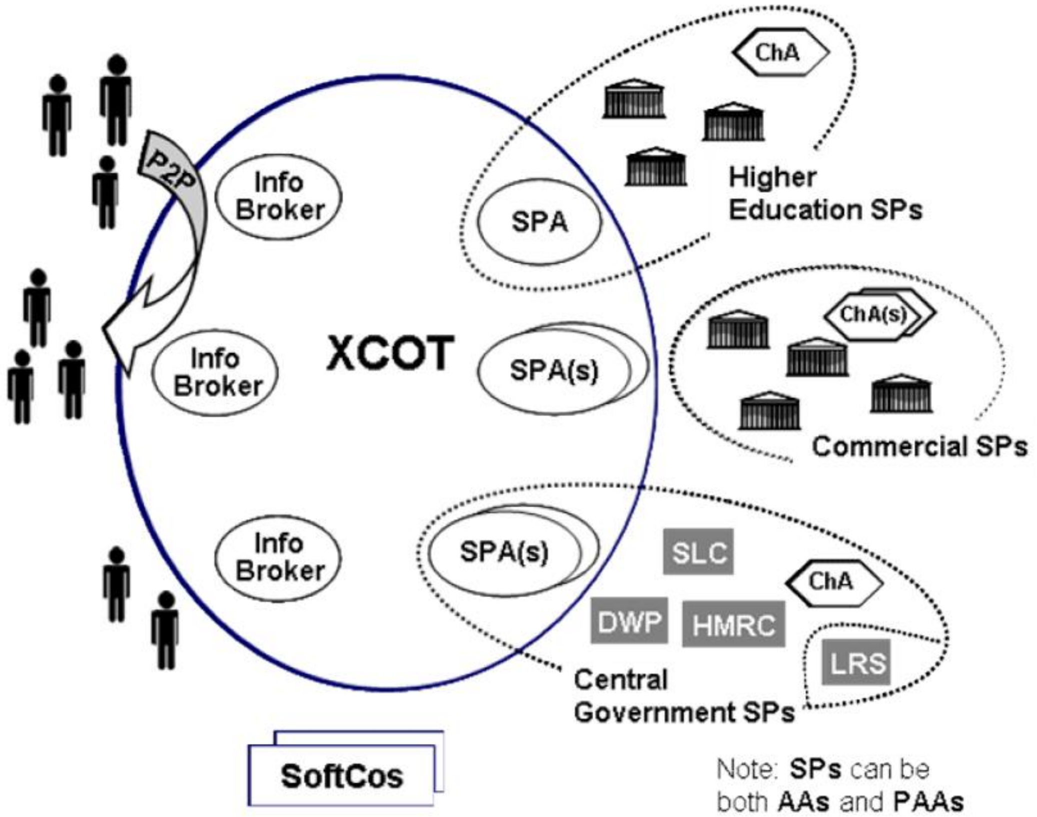
23 There is general agreement that the new industry should:

- Offer **choice** for individuals. The individual should be able to choose between brokers, just as he can choose a retail bank or a mobile network provider from their respective markets. Also, an individual should be able to port his account, complete with all established relationships, from one broker to another, much as he can port a mobile phone number between operators, or the direct debits set-up in his current account between banks.
- Be offered **free at the point of use** for individuals. Since we intend that individuals will use their broker account as an intermediary in relationships with service providers from the public sector, as well as from the private sector, it is necessary that a basic brokerage service be available to all individuals free of charge; instead the service providers will bear the costs. However, certain brokers may choose to bundle brokerage with other products and charge a fee.
- Offer a **single point-of-contact** for service providers. To avoid an excessive burden in dealing with multiple brokers, small service providers - such as universities - should be offered a single point of contact with the ecosystem and, if they so desire, a choice between such points of contact.
- Work at **multiple levels of security / assurance**. Since individuals will be able to use their broker account to transact with many different kind of service provider, controlling the flow of data of very different sensitivities, the ecosystem should be able to work at different levels of security, i.e. minimal, in order to promote take-up, when the data is low sensitivity, and higher whenever deemed necessary by the individual or a service provider.
- Enhance **privacy.** To avoid risks to individual privacy: (i) the individual needs a way to control access by his broker to the contents of his broker account; and (ii) ecosystem design should not rely upon identifiers that are shared between multiple parties. Such common identifiers should only be transmitted over the ecosystem with the explicit consent of the individual.
- Offer the **bare minimum of functionality**. To avoid conflict with service providers, and so speed take-up, the ecosystem should offer the bare minimum of functionality, leaving all 'nice-to-haves' to be provided by specialist service providers. As well as information sharing, this bare minimum logically includes single-sign-on, communication, and payment (which can be regarded as a specialised form of information sharing).
- Be **scaleable**, so that it can be used by the individual to interact with service providers, and other individuals, no matter where they may be, without impediments from either sectoral or national boundaries.
- Be **governed in the public interest**. To win wide acceptance, the ecosystem needs to be trusted. This is most likely to be achieved by ensuring that the governance structure is not-for-profit, and that both service providers and individual users are adequately represented.

Ecosystem design

24 To meet these requirements, there's a need for an ecosystem in which - as maturity is approached - there will be multiple distinct roles. In the graphic of the ecosystem below:

- **Individuals** are shown on the left-hand side, and are persons acting in their private capacity. When dealing with government, learning providers, merchants, hospitals, bus companies and other service providers, they may become - respectively - citizens, students, customers, patients, passengers . . . . .



- **Information Brokers** compete to serve individuals as their agent in the ecosystem, and exist within a managed market. An individual will select a broker, and then use her broker account to: (i) link to, and communicate with, multiple Service Providers and other individuals (jointly 'counterparties'), all at the right level of security and using just a single, stepped, authentication process; and (ii) give explicit permission for the transmission of different 'profiles' of personal information to counterparties. Profiles can include not only information recorded by the individual himself (such as preferences), but also cached copies of, and pointers to, attributes (such as a qualification, or proof of name / address / age/ student-status) held on the databases of existing Service Providers (such as a university, school, merchant, healthcare provider, government department, etc).
- **Service Providers (SPs)** are shown on right-hand side, and are grouped by kind. Groups might comprise: Higher Education institutions; merchants; schools; central government departments; local authorities; and healthcare providers.
- A **Characterising Authority (ChA)** is the entity that defines membership of each group of Service Providers. These serve two purposes: (i) they enable service providers (say an employer) to check that attributes released by an individual (say qualifications) were issued by an organisation entitled to do so; and (ii) they may serve to assist an individual to select the right profile of attributes for release to a given service provider (say a CV to a employer, or – in time – a list of medical prescriptions to a pharmacist).

- Note that Service Providers may also be **Attribute Authorities (AAs)** if they act as the authoritative source for certain information about the individual, e.g. DVLA is the authority for the driving licence attribute; and a university would be the authority for a degree qualification. Further, certain Service Providers may act as **Proxy Attribute Authorities** (**PAAs**), whose role is to verify attributes available only in paper form because the relevant Service Provider has not yet joined the ecosystem.
- **Service Provider Acquirers (SPAs)** are the PIB equivalent of the merchant-acquiring function in the credit-card industry, and will compete to sign-up service providers. Certain large service providers may choose to provide the SPA function in-house: the development by DWP of what it calls 'the hub' for the Identity Assurance Programme is a step in this direction.
- The **eXtensible Circle of Trust (XCOT)** is responsible for the maintenance of a 'trust frame work', defining certain necessary common operating procedures and standards for Information Brokers, Service Providers, and Service Provider Acquirers. The XCOT also controls the industry co-brand, and is responsible for the sharing of fees and liabilities between SPAs and brokers, akin to VISA for credit-cards. In terms of structure, the XCOT may well be a charity or a community-interest-company.
- **Softcos** are software development companies that compete to supply standards-compliant software to the various other stakeholders in the ecosystem.

Brokers and IdAP 'identity providers' compared

25 To avoid confusion, it is worth emphasising here that a broker goes much further than the concept of an 'Identity Provider (IdP)', as used in the Cabinet Office Identity Assurance Programme. In PIB terminology, as outlined above, an 'Identity Provider' combines two functions: (i) it resembles a Proxy Attribute Authority for certain key attributes (name, address, gender, age); and (ii) it also provides an authentication service. What is missing from the IdAP scheme is the broker functionality that enables an individual to control the flow of attributes between counterparties. Despite these differences, there is no reason why a broker cannot appear to function as an IdP within IdAP. For further discussion on this point, see Annex D.

Business model - when mature, and to finance development

26 When a PIB-type ecosystem is mature, its running costs will be met by service-providers (such as universities, government departments, and merchants) who will pay either: (i) modest periodic fees for the provision of an (appropriately) secure e-relationship with the individual **and** updates on the information that the individual has chosen to disclose; or (ii) fees for the chance (i.e. reverse marketing) to enter into an e-relationship.

- The fees paid by service providers will be split into three parts: one to be kept by the service provider acquirer (or used instead by a service provider to pay for the function to be delivered in-house); the second to pay the costs of the XCOT; and the third to pay the fees of the brokers.
- In the early phases of ecosystem development, certain specialist service providers will act as Proxy Attribute Authorities. Since they will contribute more value to the ecosystem than they receive, they will require to be paid. Examples include credit reference agencies, and other organisations, that will verify key attributes (such a name, address, etc) issued by service providers who have not yet, or will not, join the ecosystem in their own right.

27 This business model can be seen as a generalisation of the business model used in the credit-card industry, replacing a single kind of trusted personal data (money) with a multiplicity of data types, and a single kind of relationship (a payment transaction) with a spectrum of relationship types (anonymous / pseudonymous /disclosure of full identity, and transient / long-lasting). Indeed, if payment is offered as a PIB application, it may be necessary to offset PIB relationship fees against payment transaction fees.

28 While the description of the mature business model above is clear, the means by which such an ecosystem can developed from scratch to maturity are far less obvious. There is a need for significant investment to create the necessary software, and pay for other tasks - such as recruitment of early service providers, and marketing to consumers. What is suggested is a joint venture model in which:

- a sector of the economy, such as HE, sees the need for the new infrastructure, and co-invests with the private sector to form a joint-venture development company, so demonstrating commitment.
- the JV has responsibility for the development of the ecosystem, to include set-up and initial running costs of the XCOT, production of open-source reference implementations of the necessary software components, development and publication of the necessary technical standards, and so on.
- in return for accepting these responsibilities, the JV is given rights to develop and exploit the commercial applications for which the new infrastructure can be used, over and above those applications of direct interest to the initiating sector, i.e. HE (and, for that matter, the public sector). Put otherwise, this means that the JV is given the right to be, or license others to be, the SPA for all applications outside the public and HE sectors.

Who will be the brokers ?

29 At this point in the discussion, it's normal for people to ask 'Who will be the brokers?' There are many candidates, some of which have already shown interest by bidding to become IdPs in the current IdAP procurement.

- Start-ups can react to new opportunities very quickly, and would be able to craft a brand perfectly suited to their purpose. One early UK example is Mydex, a community interest company that believes its not-for-profit status will help it win trust and therefore custom. Other UK start-ups include PAOGA and Allfiled. More information about the start-ups is given in Annex E.
- Mobile Network Operators (MNOs) are well placed to become brokers, given that they control the handsets that will be the most common end-points for a broker account. Also they are concerned about the possibility of becoming commoditized 'dumb bit pipes', and so some are already looking for opportunities in the personal-information field. Note also that, in time, individuals may be enabled to 'kiss' Near-Field-Communication (NFC) - enabled mobile handsets, both against each other to set up peer-peer relationships (the equivalent of exchanging business cards), and against fixed readers to set-up relationships, and /or pay, organisations.
- Banks are also well placed to become brokers, given that a broker can - as described earlier - be described as a kind of modernised current account, enabling an individual to transfer attributes, or money, or a combination of the two. The payment system providers - which often lead technology developments for the banks - are now investing some time in this area.
- Education sector institutions, such as UCAS or JANET, might also become brokers, perhaps - like Mydex - using their non-profit status as a means of winning trust and thus custom. However there are arguments to suggest that these institutions have other, unique, roles to play in the ecosystem. More on this later.
- Technology providers and credit reference companies could also become brokers, building on - respectively - their mastery of the technology, and their ability to verify Key Identity Attributes[3] remotely.

[3] 'Key Identity Attributes' is the term used in this paper to mean the 'Matching data set', a term established in GPG45 'Validating and Verifying the Identity of an Individual in Support of HMG Online Services', available at http://www.cabinetoffice.gov.uk/resource-library/identity-assurance-enabling-trusted-transactions. The question

- Finally, the dominant social network providers / internet businesses - such as Google, Facebook, Amazon, and Linked-In – may also be interested in becoming brokers, although it is uncertain as to whether they would be willing to agree industry standards for account portability and interoperability, or shift to a more complex, multi-party, business model.

Getting to critical mass

30 As already stated, the design for a personal data ecosystem is now broadly agreed, and much of the necessary software is now - or will soon be - available. But there is one vital ingredient missing before critical mass can be achieved: there is a need for a large group of existing organisations who see the need for the new infrastructure, and are willing to work with the emerging industry to bring it into large scale use.

31 The best candidate for this role - by far - is the Higher Education sector. Why? Because it comprises a large number of organisations, which (like the private sector) are generally unable to share data without consent; but which (like the public sector) can cooperate to implement common infrastructure when a good case is made.

32 The HE sector in the UK has a particularly strong record of collaboration, and in consequence, has a good shared infrastructure. As an example, few - if any - other countries have a centralised admission service as well developed as UCAS. But just as UCAS (or, strictly, its predecessor UCCA) was a significant innovation in the early 1960s, so there is now a case for further innovation, building on the strengths of UCAS to implement the user-control infrastructure made possible by current technology.

Implementing user-control in HE (and, eventually, in schools and colleges)

33 We suggest that HE should take a measured, step-by-step approach towards the implementation of PIB, so minimising risk. The first step, as described later in this document, would be further discussions with stakeholders in order to allow completion of a formal proposal for review by the sector. Then, if the proposal is accepted, there would be a second step in which PIB-d and partners would develop and test the necessary software. Then, once the software is accepted as fit for purpose, the first of two implementation phases could get underway .

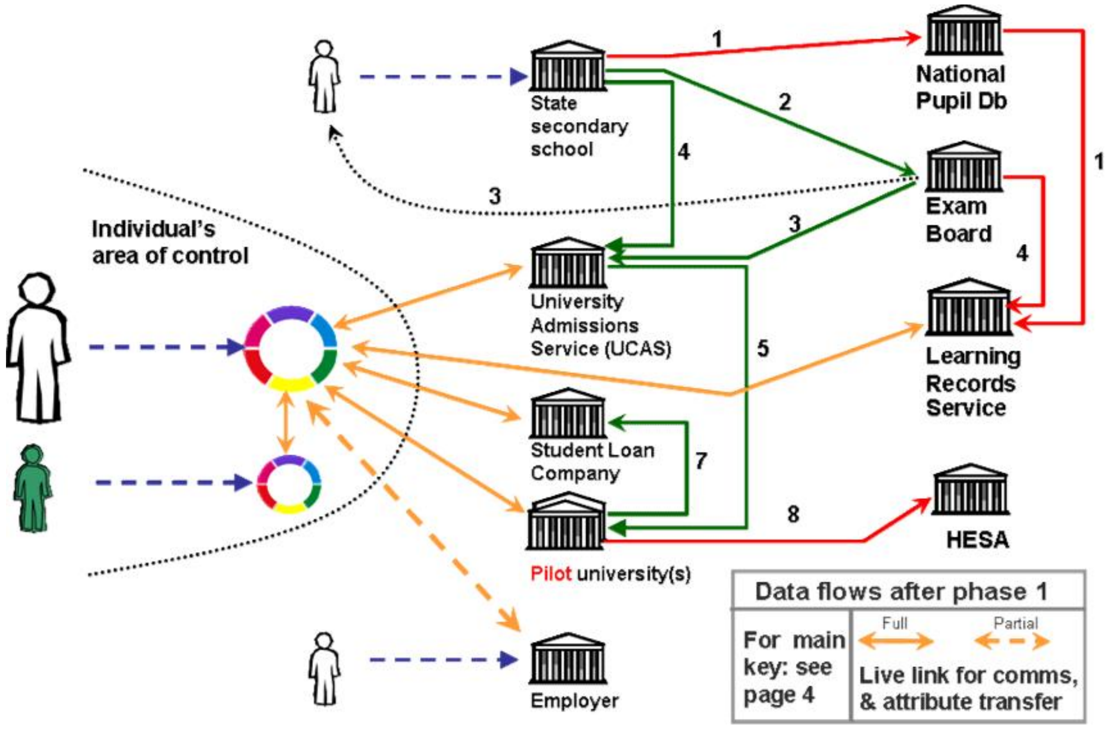
Implementation - phase 1

34 The first phase of implementation is designed to achieve two objectives: (i) demonstrate the power of the deep integration with the new ecosystem at one or more pilot universities; while (ii) also demonstrating the intent to reach national scale quickly by integrating - in a shallow and reversible way - with systems operated by UCAS and the Student Loan Company. The graphic below shows the changed data flows. Following the student journey:

- All individuals wishing to apply to UCAS and the Student Loan Company are invited, before commencing their applications, to select a broker from the managed market. Then an individual uses his broker account to authenticate to the first of the two organisations, and - as he completes that organisation's application form - a copy of the information supplied is retained in his broker account. Subsequently, he uses the same broker account to authenticate to the second organisation and - instead of re-entering the same information a second time - he gives permission for the information to be transferred directly from his broker account.
- UCAS and SLC communicate with the individual by means of secure message to his broker account, which can be set to send him alerts by either e-mail or SMS.

of which attributes to be included within the data set is still not settled, but likely candidates are: name, address, previous address, gender, date-of-birth, e-mail.

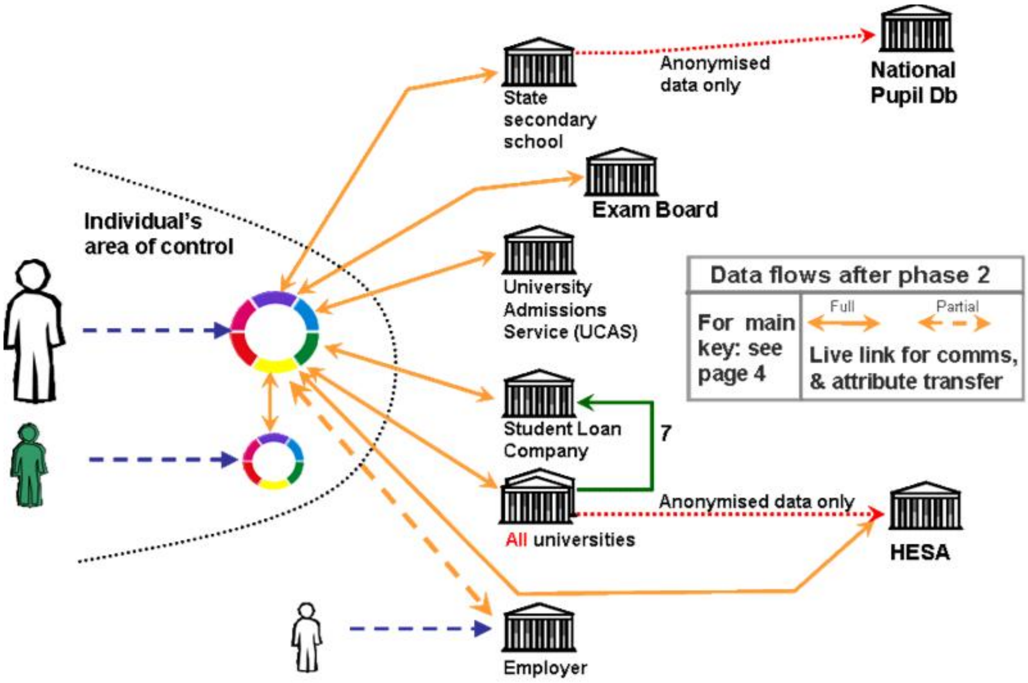
- After completing the UCAS and SLC application processes, and accepting an offer of a place, certain individuals will receive e-mails stating that their chosen university is piloting deeper integration with the PIB ecosystem. Then, in accord with the suggestions in the e-mail, each of these individuals authenticates to his broker account, navigates to the university's website, and clicks a button to request that his broker account be 'live-linked' to the record already created about him by the university (on the basis of data from UCAS). He may also supply further information, such as his term-time address. At this point, the university changes the individual's status on its system to 'pre-registered'.



- Before finally leaving secondary school, the individual may - if he wishes - link his broker account to the Learner Record Service (LRS), relying upon the school to confirm to LRS that he is indeed the correct owner of the cited Unique Learner Number. Once complete, he can 'suck' GCSE and A-level exam results from LRS into his broker account. More detail on integrating PIB with LRS, and extending PIB to serve schools, is given in Annex C.
- On the first day of the academic term, the individual arrives in person at the university, and presents proof of identity (e.g. a passport). University staff verify the proofs, record that they have done so on the university's student record system, and update the individual's status on that system to 'registered student'. The individual's broker account is updated automatically to show: (i) that his Key Identity Attributes have been 'verified by University XYZ'; and that (ii) he is formally a 'student'.
- Subsequently: the university communicates with students via their broker accounts; students use their broker account to link to other students, to academics, and to groups organised by year, course, hobby, or other theme; any counterparty can, if given permission, write to and / or read a student's calendar; and the student can prove student status to any counterparty, either within or without the ecosystem. Eventually, the university adds a degree result and transcript to the student's record in its systems, and the student can - using his broker account - also show these to any counterparty.
- As the pilot progresses, other universities see the merit of PIB, and sign-up.

Implementation - phase 2

35 When the majority of universities, and many schools, have joined PIB, it will be time for phase 2. The graphic below shows the revised - and this time much simplified - data flows.



36 At this stage:

- The individual is invited to acquire a broker account at the age of 14 or so, and uses it to maintain his relationship with his secondary school, register with exam-boards, take online exams and aggregate the results into an online personal qualification record.
- To apply to university, the individual sets up a relationship with UCAS, downloads an appropriate 'app' - containing the application protocol - to his broker account, and then applies to his selected universities directly from his broker account. There is no longer need for back-office transfer of data between UCAS and the universities.
- The Learning Records Service has been supplanted by personal learning records held within broker accounts; and is gradually closed down.
- Back-office transfer of attendance - and change of circumstance - data from universities to SLC may continue, or may be replaced by data transferred by the individual from university to SLC via his broker account. Transfer of personalised records by universities to HESA is no longer necessary. Instead universities send HESA anonymised data; and HESA, and/ or other research agencies, obtain personalised data - if required - directly from an individual's broker account, having asked for and been granted permission. A more thorough discussion of the possible effects of user-control on HESA is given in Annex E.
- The individual uses his broker account for interacting with many other entities, outside the HE sector, including merchants and central government.

Effects on UCAS, HESA, SLC, JANET, & UKAMF

37 In the text above, we have stated - almost in passing - that the implementation of PIB requires cooperation from organisations that already serve the entire HE sector, i.e. UCAS, SLC and HESA. Mention could also have been made of JANET and the UK Access Management Federation (UKAMF).

38 We recognise that the PIB proposal presents these organisations with a dilemma. On one hand, they are anxious to continue delivering reliable services to their customers, both universities and students, and so prefer incremental improvements rather than step-changes. But, on the other, they all exist to serve the HE sector and should - surely - cooperate with proposals to develop new infrastructure that will benefit their customers. The solution is to ensure that risk is properly assigned and managed.

39 To summarise the proposed changes for each organisation:

- UCAS would, in first phase of implementation, require applicants to choose a broker as a 'front-end' to their existing systems, to be used for authentication and as a store of the master copy of personal information held by UCAS and SLC. In a second phase, UCAS would cede its data-switching role to the brokers, but would retain its responsibility for: (i) defining the application protocol (and providing it as a downloadable 'app' to an individual's broker account; (ii) providing a help/ advice service to applicants; and (iii) maintaining an online course directory. UCAS would continue to receive fees, from both applicant and university, but at a reduced level; and would not pay any fees to the broker ecosystem.
- The Student Loan Company would, in the first phase of implementation, require applicants to choose a broker as a 'front-end' to their existing systems, to be used for authentication and as a store of the master of copy of personal information held by UCAS and SLC. In later phases, SLC might decide to integrate more deeply with PIB, using the system for proof of Key Identity Attributes, and - possibly - to gain sight of validated income data from parents. Fees paid by SLC would be commensurate to the benefit it gains from the service, i.e. little or nothing initially, and possibly rising later on.
- HESA would be unaffected by the first phase of PIB implementation. Later on, it may decide to offer individuals, via their broker accounts, access to the personal information that it holds. Further, it may find that it can obtain better data for statistical research direct from individuals, via their broker accounts, rather than by requiring transfer of personal records direct from the universities. A more thorough discussion of the possible effect of user-control on HESA is given in Annex E.
- JANET could become the in-house Service Provider Acquirer for the HE sector, purchasing broker services on behalf of all universities, much as it purchases bandwidth at present. If so, it would retain a portion of the fees paid by the universities to cover its costs.
- UKAMF would continue to act as the original trust framework for the education sector, serving universities and resource providers who choose not to implement PIB. Eventually, if all universities and resource providers upgrade, UKAMF would have served its purpose as a first-generation trust framework, and could be gently retired.

PIB complements relevant Government initiatives

40 As a stand-alone initiative, PIB could be seen as a step too far. But, in fact, the proposal fits well with a number of other initiatives being pursued by central government, so that - taken together - each part reinforces the rest. Specifically:

Identity Assurance Programme

41 In late 2012, and as a major milestone towards implementation of the Cabinet Office Identity Assurance Programme[4] (IdAP), the Department of Work and Pensions (DWP) announced that eight organisations had succeeded in their efforts to be appointed as Framework suppliers for the provision of Identity Provider (IdP) services. Late in 2013, individuals wishing to apply to DWP for the new Universal Credit will be asked to choose an IdP from this emerging market;

[4] See http://digital.cabinetoffice.gov.uk/category/id-assurance/

the IdP will then check certain Key Identity Attributes, and vouch for these attributes - and the individual's authentication state - whenever they wish to transact with DWP. Other government departments, such as HMRC, are expected to follow suit. PIB offers the HE sector (and education more generally) an opportunity to adapt IdAP to meet its own needs. A discussion re the compatibility of the two is given in Annex D.

Midata

42 Under the Midata[5] programme, BIS is encouraging commercial sector companies to release personal data back to individuals in electronic form. Legislation to enable ministers to require such release is now being considered by Parliament. These are big steps forward. But the programme lacks any measures to provide individuals with tools to make use of this data effectively, to delegate access to it to others, or to convey attributes to others together with proof that values have not been altered. PIB provides individuals with such tools, and - if scaled to critical mass in HE - should be taken up by the private sector.

Open Data

43 Under the Open Data[6] programme, led by the Cabinet Office with assistance from Sir Tim Berners-Lee and Professor Nigel Shadbolt, government departments are being encouraged to give everyone access to data held by government. A new portal, data.gov.uk, has been launched recently for the purpose. However, the project is primarily concerned with data that it is either not personal at all, such as mapping information, or data that has been anonymised prior to release. Giving individuals access to their own personal data seems to a lesser priority, and is barely addressed in - for example - the Department for Education's 'Open Data Strategy'[7]. PIB promises to address this issue, and will bridge the gap between the Open Data and Midata programmes, complementing both.

Emerging industrial strategy

44 Finally, the Secretary of State for Business, Innovation and Skills, Vince Cable, is developing[8] a new industrial strategy that emphasises the importance of university-industry links, and of building on current strengths, to create products and services for export. Given the Government's current work to develop an innovative, distributed approach to identity assurance, and the strength of the UK's HE sector, adapting the first to suit the second would seem to be an obvious step, and may well create export opportunities.

Other applications for PIB, outside HE

45 Although this proposal focuses on applications of PIB within the HE sector, which is the most likely initial adopter, there are several other potential application areas for the infrastructure, each capable of generating traffic and revenue as scale is achieved. Many of these areas have already been touched upon, but we give a full listing here for the sake of completeness.

- Secondary education. If PIB succeeds in HE, it will spread quickly to secondary schools, perhaps being offered to pupils as they begin Key Stage 4 (typically at the age of 14).
- Proof-of-age for age-restricted purchases and safer online activity. Assuming PIB does spread down to secondary education, the new infrastructure will provide a good solution to two perennial problems: (i) enabling retailers to prove the age of customers who wish to buy

[5] See http://www.bis.gov.uk/policies/consumer-issues/consumer-empowerment/personal-data

[6] See http://data.gov.uk/

[7] See http://www.data.gov.uk/library/dfe-open-data-strategy

[8] See http://www.bis.gov.uk/news/speeches/vince-cable-industrial-strategy-september-2012

restricted goods (such as alcohol, knives, glue . . .); and (ii) enabling online service providers to prove the age of entrants to 'safe' on-line services, e.g. chat rooms and social networks targeted at kids.

- VRM-type applications. The Vendor Relationship Management[9] project, led by Doc Searls at the Berkman Center for Internet & Society at Harvard University, aims to provide individuals with software tools that offer both independence from vendors and better means for engaging with vendors. These same tools can also apply to individuals' relations with other institutions and organizations. Named for the inverse of Customer Relationship Management, VRM is designed to replace the CRM mindset - typified by words such as 'target', 'capture', 'acquire', 'lock in', 'direct', 'own' - with an approach in which customers are involved as participants, rather than as subjects.
- Central and local government. As already stated, a broker can act as an Identity Provider within the Cabinet Office Identity Assurance Programme, as being implemented by DWP and, potentially, other central government departments. It is not yet clear whether local authorities will implement IdAP as it stands, or wait on developments, such as PIB.
- The phrase 'Internet of Things (IoT)' is often used to describe a future in which the internet is used to connect huge numbers of electronic devices, ranging from sensors to door locks, and from smart phones to beer barrels. IoT applications are of two different kinds: those concerned with impersonal data, such as the weather or beer-barrel location; and those concerned with personal data, such as health or location, originating from - respectively - health sensors and mobile phones. The routing of such personal data from sensor to end-user requires something very like a PIB ecosystem.
- Health. The idea of a truly personal heath record, to which an individual (or their carer) can give a doctor access, has been mooted for some time, and has some advantages, principally privacy and avoidance of lock-in to a single care provider. But there are also problems, such as creating barriers to population-scale epidemiological studies. Quite how far the shift from records controlled by organisations to records owned by individuals will go is uncertain, but there is certainly scope for progress. Giving individuals proper online control of prescriptions would be a good first step.
- Disclosure & Barring Service. Organisations who have responsibility for children and vulnerable adults must ensure that all who come into regular contact with their charges are fit to do so, i.e. that they have no record of unsuitable behaviour that would render them unsuitable. For this purpose, candidates' details are checked by the Disclosure and Barring Service. In time, PIB could enable individuals to include the results of their DBS check within a trustworthy CV submitted as part of their application to work with vulnerable groups. The scheme could be designed so that either (i) organisations could request a refresh of the DBS result whenever required; or (ii) organisations would be informed automatically should new information, relevant to the DBS result, arise. But this is for the future: an application of this kind would only be feasible once a broker ecosystem has been proven elsewhere, and - in any case - would probably require legislative change.

46 Note that it is for an individual to decide whether to use a single broker account to manage all relationships, or to use different accounts for different areas of life - say education, health, and commerce. The trade off, between greater convenience and a minor increase in risk, is similar to that made when an individual decides to place all his money in a single bank, or spread it between banks.

[9] See http://cyber.law.harvard.edu/projectvrm/Main_Page

Developing consensus and moving forward

47 PIB has been the developed by a tiny company, a joint-venture between the HE and private sectors, for the past 14 months. So far we have produced a detailed functional specification, some initial mock-ups of the new user-interface, a technical design for the software components, and the basis of an accurate costing for the necessary software development and subsequent pilot.

48 To make progress with user-control, we believe the first necessary step is for the HE sector - as a whole - to admit the possibility of change, and invite the emerging personal data industry to assemble and submit a formal proposal for a pilot. This task would require that PIB-d and partners engage in preliminary discussions with:

- Government departments: (i) Cabinet Office, to confirm acceptability of PIB as an extension of the Identity Assurance Programme; (ii) BIS, in its capacity as leader of the Midata project; (iii) Cabinet Office (again), this time in its capacity as leader of the Open Data project; and (iv) BIS, in its twin roles of developing the UK's industrial strategy and overseeing the HE sector.
- UCAS, and the Student Loan Company: to ensure that the proposal is acceptable in principle, and to develop outline specifications for the necessary interfaces.
- Further universities: to confirm that our initial findings at UH are correct
- Potential brokers: to confirm their interest in the proposal.
- Software suppliers: to confirm their interest in supplying software to the ecosystem, and double check our initial estimates for software development cost.
- Financiers: to gauge their willingness to finance ecosystem development, and whether they will require any part of the capital cost to be met by the HE sector. Potential brokers may choose to provide part of the up-front capital, so becoming part owners of PIB-d Ltd; and
- Subject experts: to confirm that PIB-d's initial design work conforms with relevant security standards, privacy principles, and data-protection legislation, and that there are no insurmountable hurdles in the procurement regulations.

49 Once these discussions are complete, PIB-d would submit a formal proposal to HEFCE and the wider HE sector, comprising (i) firm plans for the subsequent steps; and (ii) review of options for financing. In terms of timing, we expect that the further discussions, described above will take about 4-5 months. If the decision to go ahead is taken, we would hope to launch the broker ecosystem in good time for the application cycle for university entry in 2015.

50 Note that we recognise that the HE sector is comprised of multiple independent institutions, and that it is thus not possible for any one body to take a decision that is binding on all. Given this situation, the PIB project is only viable if one (or more) universities agrees to host an initial pilot and the pilot receives support and cooperation from the national service providers, i.e. UCAS, SLC, and HESA. Even though each university is autonomous, there is then a reasonable chance that all would see the benefits of PIB and implement within a reasonable period.

Annex A The challenges - and opportunities - of online learning

A1 In 2012 Bill Gates commented[10] that information technology had barely changed the traditional model of university education. He was partly right. Change is happening, gradually within established universities, and more quickly in new-start universities that have embraced a fully-online model. Also there are early signs of more radical change, with the creation of 'Massive Open Online Courses (MOOCS)'.

Students needs and expectations are changing

A2 In 'Collaborate to Compete[11]', a report on online learning published by HEFCE in January 2011, Dame Lynne Bradley and colleagues point out that students now wish - and need - to 'consume' higher education in different environments. While many still choose a traditional university setting for their first degree, many others - particularly post-graduates and mature students - choose to study part-time, and from wherever is most convenient. Some study from home, some are allowed time to study in their workplace, and either location can be in the UK or in some other country around the world. Further, most students are - even before starting a course - already familiar with the use of high quality-online tools, such as encyclopaedias (Wikipedia), search engines (Google) and collaboration tools (Google docs; Office365).

A3 Thus students need - and expect – that: (i) Higher Education will offer them a range of options for study, both face-to-face and online; and that (ii) the software tools offered to them for online learning will be of a standard equivalent to, if not better than, those they already use for free.

Universities are updating their products

A4 When the nature of demand changes, suppliers must either update their products or risk losing their customers. And so universities are changing. In a survey[12] of online learning, conducted for HEFCE in 2010, it was found that:

- Over 400 predominantly online courses were offered by over 100 HE and FE institutions in the UK. A further 175 online courses were offered by HE and FE institutions in partnership with commercial providers.
- The vast majority of online courses offered by HEIs were at post-graduate level. Courses offered in partnership with commercial providers were more evenly spread across the HE academic levels.

A5 In the USA Eduventures, a research and consulting firm, estimates[13] that - in the autumn of 2009 - 8% of US undergraduates were enrolled on fully online programmes; and that the equivalent figure for enrolment in fully-online masters programmes was 24%. At about the same time, the Sloan Consortium - a grouping of US HEIs interested in the development of online learning - estimated that approximately 16% of all US undergraduates were enrolled in programmes that require at least some modules to be taken online.

A6 The speed at which HEIs adopt online learning generally depends on their background and circumstances. Established universities, who have invested heavily in the facilities required for conventional face-to-face teaching, tend to be conservative. Newer universities, particularly those that are privately funded and have few capital assets, have been quicker to adopt the online approach. Notable examples include: (i) the UK's Open University, founded 40 years ago

[10] See http://chronicle.com/article/A-Conversation-With-Bill-Gates/132591/

[11] See http://www.hefce.ac.uk/pubs/year/2011/201101/

[12] See http://www.hefce.ac.uk/pubs/rereports/year/2010/ukonlinelearning/

[13] 'Reinventing Higher Education: the promise of innovation', edited by Ben Wildavsky et al. Page 207. Harvard Education Press. ISBN 978-1-934742-87-7

as a specialist, non-profit, provider of distance learning courses; and (ii) the University of Phoenix, a very large, very commercial, and sometimes controversial university founded in 1976 in Arizona.

A7 One recent innovation is the development of Massive Open Online Courses, or MOOCs, a term first coined when a Stanford University professor offered a free artificial-intelligence course online. When 160,000 students from 190 countries signed up within a few weeks, the professor quit his day job, and founded Udacity, aiming to 'democratise education' by offering free, bite-sized courses. Udacity joins other US university start-ups: edX, a joint-venture between Harvard, MIT and Berkeley; and Coursera, which - like Udacity - originated at Stanford. Sceptics point out, correctly, that these new ventures have yet to sort out a business model, offer far less support than a traditional university, and cannot yet give students a recognised qualification.

A8 Despite these shortcomings, at least two UK universities - Edinburgh and the University of London - have joined Coursera, apparently seeing the platform as an interesting experiment and as a free 'taster' for students who may later sign-up for conventional, paid, online courses. Also, and more importantly, the Open University launched – in late 2012 – FutureLearn as the first UK-led, multi-university MOOC platform. As of March 2013, seventeen UK universities have joined FutureLearn as partners, as have the British Library and the British Council.

A9 Given the pace of change, no-one knows what the ultimate balance between online and face-to-face learning will be. But it seems certain that the current shift towards online programmes is only the beginning. One expert, Eduventures, estimates that, by 2014, 20% of all US students (i.e. undergraduates and masters) will be enrolled on fully-online courses. No one has yet guessed a figure for 2020. Prof Martin Bean, vice-chancellor of the Open University, describes[14] this as the 'Napster moment for higher education'. There are certainly many new online providers, all setting out their wares, and - as in many industries - they may well have common requirements for new tools and services.

Need for common tool set

A10 To date neither the new entrants, nor any of the established organisations, in the online learning field have figured out how to address certain common problems: (i) how to reliably identify students with whom they never have face-to-face contact (ii) how to authenticate such students during assessments in order to prevent impersonation; and (iii) how to give successful students a trustworthy electronic certificate that can be combined with others to form a validated CV, and shown to any counterparty of their choice. Also, none of these online providers will be interested in developing their own version of common web services - such as those for communication, payment, and calendar - and will, presumably, be happy to outsource the requirement to a specialist.

A11 What is suggested - in the PIB proposal - is a variant of an old story: in a gold-rush, the best way to make money is not to go prospecting, but rather to sell shovels. Similarly, in the rush to online learning, the best way to make money is to build on the strengths off the UK's HE systems to create a tool-set that works for both offline and online learning, and can be exported around the world.

----

[14] See http://www.guardian.co.uk/education/2012/dec/03/massive-online-open-courses-universities

Annex B The emerging personal data industry

B1 All but one of the ingredients for fast innovation in the personal data sector, beginning with education, are now present. The analysts say it is about to happen; the start-ups are keen to make it happen, and have learned that an ecosystem, rather than stand-alone business, is required; large corporates are biding their time, waiting for a sizeable opportunity to emerge; and investors are showing interest. There is just one ingredient missing.

The analysts

B2 The development of any new industry tends to be accompanied by the emergence of analysts and commentators who opine and advise in return for per-diem fees. Personal data is no exception:

- Ctrl-Shift, the industry's first specialised consultancy, is UK-based, and makes some useful information available on its website[15]. Back in 2010, Ctrl-Shift was commissioned by NESTA to report on the feasibility of creating a system of portable 'Personal Education Records'. They concluded[16] that PERs could provide both educational benefit, and efficiency savings, and recommended facilitation of market development. But NESTA reorganised, and chose not to act upon the recommendation.
- KuppingerCole, a German firm of IT analysts, focuses principally on identity management, but also works in the (related) field of personal data. They predict[17] that (what they call) 'Life Management Platforms . . . . will be the one technology that has the strongest influence on our everyday life (and, on the other side, on enterprise infrastructures and the Internet architecture) for the next 10 years'
- The World Economic Forum is attempting to lead from on high, and has launched the 'Rethinking Personal Data' initiative[18]. Its objective is 'to bring together the many stakeholders and deepen the collective understanding of how a principled, collaborative, and balanced personal data ecosystem can evolve'.

Market entrants, existing and future.

B3 Initiatives to give individuals better control of their personal data have been gathering momentum for the past several years, with clear clusters of activity on both sides of the Atlantic. In the UK:

- Allfiled[19] Ltd made some progress as a standalone broker, but then realised that the market could only prosper if multiple interoperable brokers emerged, and so has refocused on becoming a software supplier to brokers.
- Like Allfiled, PAOGA[20] launched a broker service some years ago, and is continuing to experiment with new technology. The company has not made any public announcements about its long-term intentions.
- Mydex[21] was set-up as a community-interest company, and has conducted some trials in collaboration with local authorities. The company has just succeeded in its bid to become a

[15] See http://ctrl-shift.co.uk/

[16] NESTA chose not to publish the report, but PIB-d can supply copies - obtained under FOI - on request.

[17] See the KuppingerCole advisory note 'Life Management Platforms: Control and privacy for personal data', available free of charge, but after registration, at www.kuppingercole.com

[18] See www.weforum.org/issues/rethinking-personal-data

[19] See https://www.allfiled.com/

[20] See http://www.paoga.com/

Framework supplier of IdP services in the DWP /Cabinet Office's Identity Assurance programme (IdAP).

B4 Mydex's decision to become an IdP in the Cabinet Office's IdAP scheme shows how the personal data market in the UK may now develop. Large corporates, including certain mobile network operators and representatives of the banks, are watching IdAP closely, and are expressing interest in joining a successor scheme that will deliver, in addition to the basic IdAP functionality, a wider range of applications, to include attribute exchange, payment, and various other personal web services.

B5 In the USA, there are numerous start-ups, of which the most notable is Personal.com, a company backed by ample venture funding. Recently Personal.com announced[22] the launch of 'Personal for Education' in an event at the White House.

Emerging ecosystems

B6 Without exception, all potential brokers subscribe to the view that the new market cannot be 'winner takes all'. Instead, there is a need to give individuals a choice of broker, and to arrange for interoperability, and account portability, between brokers. Put otherwise, there's recognition of a need to create a new ecosystem, or industry, and there are the beginnings of progress in this direction.

B7 Many start-ups have now joined the Personal Data Ecosystem Consortium[23], a loose industry body which has a membership of about 40, of which about 1/3rd are based in Europe and 6 or 7 in the UK. But PDEC is mainly a facilitator of discussion; there are just three concrete proposals to create ecosystems.

- The Respect Network[24], a commercial company based in the USA, has chosen to create an individual-individual reputation network (Connect.me) as the first step, and may soon introduce merchants for various VRM type applications. RN is working closely with a Innotribe, the innovation arm of the Swift interbank payment network.
- Qiy[25], a Dutch charitable foundation, got started by giving employees - of commercial companies - control over their payslip data, and is now working on various pilots in collaboration with the Netherlands government.
- PIB-d, the instigator of this proposal, was set-up in the UK in 2011 to determine the practicality of creating a user-control ecosystem in partnership with the HE sector, adopting a collaborative approach to application development and ecosystem governance.

B8 Although all three of the ecosystem proposals have dreamt, at one time or another, of world domination, their initiators are all pragmatic and recognise that cooperation will serve everyone's interests. As soon as two or more of the proposals begin to make headway, there will be talks about interoperability - at both technical and business levels.

The missing ingredient, or 'There's no party like a relying party'

B9 The big question, then, is 'When will the ecosystems proposals begin to make headway ?' The answer is very simple: as soon as one of the proposals can persuade a *suitable group* of organisations to cooperate. Note the emphasis above on the words 'group' and 'suitable'. A single organisation, no matter how large, is less than ideal as development partner because its

[21] See http://mydex.org/

[22] See https://www.personal.com/personal-launches-personal-for-education

[23] See http://pde.cc/

[24] See http://respectnetwork.com/

[25] See http://www.qiy.com/

main requirement will likely be proof of the identity by which it already knows its existing customers. This fact explains the attempt by the UK Government to issue a national identity card in the early years of this decade, and - when that attempt failed - their subsequent decision to create a market of Identity Providers, whose only job is to prove Key Identity Attributes.

B10 The ideal partner for the development of an ecosystem of brokers is not a single organisation, however large, but rather a *group* of organisations, each of which supports the principle that individual should be empowered - whenever possible - to control the use of their own data. Further desirable characteristics are:

- A high turnover of customers, thus making it possible to trial the new systems on new customers, rather than having to persuade existing customers to migrate.
- A need to give individuals personal information - such as a qualification - that is intended to be shown to others.
- The ability to collaborate, both to save cost through ‘shared services’, and to develop the necessary common infrastructure required for such sharing.

B11 As will be obvious already, the HE sector in England comes close to the ideal as a development partner. Few, if any, other groups of organisations match the criteria so exactly, or stand to benefit so much should the ecosystem prove successful.

Annex C Integration with the National Careers & Learning Records Services

C1 In this annex, we start by describing the National Careers Service and the associated Learning Records Service, then offer a critique of these services as they currently stand, and finally propose a way forward that combines the best of what has been achieved to date with the potential of a PIB-style ecosystem.

C2 Note that the comments below are PIB-d's own views, and have not yet been discussed with any of the named organisations.

Background

C3 The Skills Funding Agency[26] (SFA) operates the National Careers Service[27] (NCS) on behalf of the Department of Business, Innovation and Skills (BIS). The service is targeted mainly at those who choose to pursue vocational careers rather than follow a more academic/ professional route. But there is, of course, significant overlap between the two groups.

C4 The NCS website invites individuals to create a 'Learning Record'. Qualification data can either be entered by the individual or is provided by NCS, based on records held by the Learning Records Service[28] (LRS), a further service run by SFA on behalf – this time – of both BIS and the Department for Education.

C5 According to its website, LRS is '*designed to support learners at all levels to access, manage, and use their own achievement information - such as qualifications, awards, or training received as they progress through education, training and lifelong learning*'. LRS also delivers certain ancillary services, such as the maintenance of a register of learning providers, and the registration of learners. A Unique Learner Number (ULN) is issued to each learner at the time of registration.

C6 LRS was launched in 2006 under its original name of 'Managing Information Across Partners'. At the time, it was assumed that individuals would be active participants in the scheme, and would use their ULN – and associated password – to access and maintain their own learner record. But experience has shown this not to be case. Most learners are registered for LRS, and given a ULN, when they are 14 years old. At that age, the task of planning a career and applying for a job still seems a long way ahead, and so the ULN is often forgotten.

C7 Later on, when careers and job become important, an individual may well seek advice from NCS, and use its website to create a learning record. At this point, NCS needs a way to match the individual to his existing LRS record, and finds the problem difficult because key attributes – such as name and address – may well have changed. Two solutions have, or are, being tried:

- Initially NCS required that an individual's identity be verified by a new learning provider, say an FE college, who – in the course of a face-to-face interview – could determine the individual's previous addresses/ names, and search manually for the matching LRS record (or records, if duplicates have been created). But it seems that this approach was found unsatisfactory, perhaps either because many job seekers have no contact with a learning provider, or because learning providers lack training in identity verification.
- Instead, NCS has now sub-contracted the task to Experian, a credit reference company, who will verify a learner's identity online against its existing database, and will – at least in theory – then provide NCS with the information necessary to match an online user of its service against their LRS record(s). This scheme has similarities to IdAP (as described in

[26] See http://skillsfundingagency.bis.gov.uk/

[27] See https://nationalcareersservice.direct.gov.uk/Pages/Home.aspx

[28] See http://www.learningrecordsservice.org.uk/

Annex D), save that: (i) there is only IdP, rather than a managed market; and (ii) the Service Provider – in this case NCS – provides the authentication service, not the IdP.

C8 Despite its ambition to become a comprehensive national qualification database, LRS has never managed to persuade the HE sector to contribute their records. Instead, universities either validate qualifications manually, in response to requests from their graduates' potential employers, or have - in some cases - begun to install DARE, as described in Annex J.

Critique

C9 The Skills Funding Agency, as the operator of both NCS and LRS, must be aware that its approach to learner records is less than perfect. In the old paper-based world, individuals were given tamper-proof paper certificates by awarding bodies, and could show a selection of these, whenever necessary, to new learning providers or potential employers. But, in the LRS scheme, as currently configured:

- *Qualification records are not complete.* At present, LRS only covers state-funded secondary schools (post 14), and Further Education colleges, in England and Wales, together with some independent learning providers. State-funded schools and FE colleges in Scotland and Northern Ireland do not make use of the service; nor do many schools in the private sector; nor do any of the UK universities. Thus one clear goal for LRS must be to improve coverage.
- *Individuals feel little sense of ownership or control.* A simple definition of the word 'personal' might just convey the idea of idea of 'relevant to' a particular individual, and - in this respect - the 'personal learning record' provided by LRS is indeed personal. But other, richer definitions[29] of the word pull in ideas of ownership by, and the presence or action of, the individual. The fact that NCS has to employ a credit-reference-bureau as an identity provider, in order to match customers to their LRS records, would suggest that individuals do not generally regard their LRS record a being personal possession, i.e. something of value which they wish to control, and that there is scope for improvement.
- *LRS records are not used as much as could be desired.* At the moment LRS is not used as part of the university admissions process, or as part of the process by which most individuals seek jobs, whether directly after leaving school of after university or college. Thus a third goal for LRS must be to ensure that its services are used more frequently.

A possible way forward

C10 PIB-d believes that these three goals will be difficult, if not impossible, to achieve if LRS continues to rely exclusively on back-office transfer of qualification data from awarding bodies to its central database. Take, for example, the goal of completeness:

- No matter how hard LRS staff work, there will always be relevant awarding bodies who decline to provide data. Consider a pupil from a school in England who studies at a Scottish university. Since Scotland does not make use of LRS at all, not even at the secondary level, it seems unlikely that its universities will ever contribute data, even if the English universities are eventually persuaded. What is true for universities in Scotland is doubly so for universities fully outside the UK, both those offering traditional courses and those experimenting with new online methods (as discussed in Annex A).
- Similarly, it seems unlikely that the professional bodies - whether in England or elsewhere - will ever contribute data to LRS. Such bodies have a close relationship with their members, and neither side would see any logic in exporting data to a distant third party.

[29] The first three definitions of the word 'personal' in the Concise Oxford English Dictionary are (i) of, affecting, or belonging to a particular person; (ii) involving the presence or action of a particular individual; and (iii) of, or concerning, a person's private rather than professional life

C11 This view - that a personal learning record can never be complete, or properly personal, if assembled using only back-office data transfer - is almost unarguable. Once accepted, the question becomes 'How can we build on the achievements of LRS to develop a better scheme?' The answer is a hybrid approach, allowing an individual to combine qualifications assembled by LRS with others, provided by awarding bodies who do not participate in the scheme. Put otherwise, LRS needs to recognise that it is a source of qualification data contributed by some of the awarding bodies in a particular geographic area, i.e. England and Wales. An individual can, if he wishes, draw data from this source, and - using a broker-type account - combine it with data from other sources, to create a true personal learning record. But LRS can never be a personal learning record in its own right: it is a source of data, not the whole.

C12 This said, individuals do vary. A proportion of the population may not wish to use a broker account to interact with learning providers, and so will be content with the current version of the LRS service, at least for the time being. But, just as the banks have gradually persuaded their clients to use plastic cards rather than paper cheques, so it may be that the use of brokers will – eventually – become ubiquitous throughout the education sector, and individuals will have little choice but to follow the crowd.

C13 Once it is accepted that LRS is a source of data, rather than a truly personal learning record, then it becomes straightforward to map out a path for convergence with PIB:

- Instead of issuing students (typically at the age of 14), with a Unique Learner Number, schools and colleges in England and Wales would invite each student to select a broker from the managed market, and issue a relationship request from their broker account to LRS.
- Acting on behalf of LRS, the school / college would then accept the relationship request, and make a note - *for its own internal purposes* - of the ULN issued by LRS in return. The individual would not be expected to remember his own ULN number.
- Then, as at present, schools would cite the student's ULN on all registrations with examination boards; the assessment bodies would include the ULN in submissions to LRS; and LRS would aggregate the submissions to create a qualification record against a particular broker relationship.
- Subsequently, the learner can use: (i) his broker account to apply to - and interact with - other learning providers, such as the universities, who do not participate in the LRS scheme; and (ii) can 'suck' qualification attributes direct from such learning providers into his broker account, for aggregation with existing attributes - including those obtained from LRS.
- Finally, as and when PIB becomes ubiquitous, some of the learning providers and assessment bodies who participate in the current LRS scheme could choose to become PIB service providers in their own right, set up broker-enabled relationships directly with their learners, and hand back qualification attributes directly. At this point, LRS would become simply the back-office record system for the rump of learning providers and awarding bodies who – perhaps because of their small size – choose not to become PIB service providers in their own right, preferring instead to interact with the ecosystem as a group.

C14 Note that this PIB approach to qualification records can only work if individuals come to regard their broker account as truly personal, i.e. something they use as a means of interaction with many counterparties, not just as an authentication service for a single learning provider. This explains why: (i) PIB has to be implemented as an infrastructural project, intended for use by the entire education sector; and why (ii) the development of a rich set of person-person applications will be a priority.

C15 Note further that implementation of PIB will change, but not necessarily eliminate, the role of 'identity providers', such as the credit reference bureau working under contract to the National Careers Service. Instead of the IdP being the sole source of trustworthy identity attributes, the individual will – using his broker account – be able to aggregate evidence of his identity, as recorded, and possibly verified, by multiple different service providers, e.g. a school, then a university or college, and then an employer. If this aggregated evidence proves insufficient for a new service provider (such as, say, DWP) then the individual may need to set up a relationship with an ‘IdP’ to obtain a ‘top-up’. This IdP relationship will be identical to that with any other service provider in the PIB ecosystem, save that the IdP may be paid for the relationship rather than make payment for it.

C16 For NCS itself, the advent of PIB would mean paying an individual’s broker for access to the individual’s qualification record, rather than paying a credit-reference bureau to match a customer against the individual’s (partial) qualification record as held in LRS. PIB would also break the close link between NCS and LRS, allowing an individual to obtain careers advice – based on a trustworthy qualification record – from any appropriate counterparty.

Annex D PIB complements, and takes forward, IdAP

D1 In this annex, we outline the Cabinet Office's Identity Assurance Programme (IdAP), position the programme along the multi-step transition from paper-based to digital-approaches to identity and personal information management, and argue that PIB (i) represents the next step in the transition; and (ii) is backwardly compatible.

D2 The Cabinet Office team leading IdAP is aware of the PIB proposal and has expressed interest, but – so far – has stopped short of offering unequivocal support.

The nature of IdAP

D3 Under the IdAP programme, by way of quick summary, individuals will choose a 'identity provider (IdP)' from a managed market; the IdP will then verify certain Key Identity Attributes[30], and - whenever the individual wishes to transact with a central government department - will vouch for these attributes and the individual's authentication state. The department then uses a computerised service to attempt to match the Key Identity Attributes against a particular record on its database. If a match can be found, the service returns the record identifier by which the department knows the individual and the transaction can then proceed.

D4 DWP will be the first department to implement the scheme: in late 2013 individuals will be required to choose an IdP as part of the process of applying to its new Universal Credit programme. In this case, the identifier returned to DWP by its matching service will be - presumably - an individual's National Insurance Number. It is not yet clear how the scheme will deal with new claimants (who have no DWP record), or with existing claimants who have a relationship with DWP but may not be able to prove their Key Identity Attributes to an IdP.

D5 If DWP is successful, HMRC may follow its lead, and implement IdAP for some services commencing 2014/2015. Its matching service would return the identifier by which an individual is known to HMRC, presumably the Unique Taxpayer Reference.

D6 The design for IdAP is pragmatic, being the direct result of the previous Government's failure to create a system of National Identity Cards. One objection to the ID card was that the consequent common identifier could be used by different organisations to link their records, and would lead to an abuse of privacy. IdAP relies instead on the set of Key Identity Attributes to uniquely identify the individual, and so permit linking of records held by an IdP with those held by a department. Since the departments will be able to use the same set of attributes to link their records directly, as has long been the case, IdAP can be said to preserve the status quo: it neither harms, nor helps, the cause of privacy.

Uses cases for which IdAP not designed

D7 As well as being pragmatic, the design for IdAP is also specific and modest: it seeks to solve the proof-of-identity problem for a large Government department, DWP, which already has records for, and rarely has face-to-face contact with, most if its customers. Because of this modest ambition, there are a number of areas where desirable functionality has been sacrificed, and some potential use-cases that cannot be easily delivered:

- Use of face-to-face relationship with Service Providers. Because DWP rarely meets its customers face-to-face, IdAP relies entirely on the commercial IdPs to check Key Identity Attributes, and so link the individual to DWP's existing record. In other sectors, such as health and education, face-to-face contact between customers and delivery organisations is the norm and can be used either for (i) validating Key-Identity Attributes by checking paper proof, or (ii) linking an individual's broker account to a pseudonymous online record; or (iii)

[30] See footnote #3 on page 9.

both of the foregoing. For example, a school could easily confirm the link between a pupil and an online record, such as the Learning Records Service, leaving the third party - as commissioned by the individual - to provide simply a common authentication service, rather than the combined 'proof of key-identity-attributes and authentication' service required of IdAP style IdPs.

- Management of multiple identities In the UK individuals can, and do, use different identities for different purposes, e.g. (i) a professional woman may retain her maiden name at work, but take her husband's name in private life; and (ii) individuals may have more than one home address, perhaps living in a city in the working week and in the country at weekends, or - if in the military - splitting their time between a military base and home. Online, as an extension of the same idea, many people use multiple identities - or pseudonyms - to protect their privacy, only releasing their 'real' identity attributes when trust has been established. IdAP does not cater well for the use of either pseudonyms or different 'real' identities. While this does not matter much in a scheme that seeks only to prove an individual's identity for a single counterparty (i.e. DWP, and by extension, HMRC), it becomes problematic as soon as attempts are made to extend the use of the scheme to multiple counterparties, both within and outside the public sector (e.g. local authorities, schools, universities, healthcare providers, commerce, etc).
- Secure communication. At present, individuals have no facility to receive secure communications over the internet; instead they are sent e-mails or SMS texts to notify them that a secure message is waiting for them in a mail-box on a counterparty's website. Authenticating to multiple websites to collect secure mail rapidly becomes tedious. IdAP does not offer a solution. Because individuals can choose to authenticate to an IdAP service provider using any IdP, and can switch IdPs from one transaction to the next, a service provider - such as DWP - will never know which IdP an individual will choose, and so cannot send secure messages to the individual 'at' an IdP.
- Attribute exchange. In relationships between individuals and organisations, either party may offer the other validated information. Airlines are required, by government, to obtain proof of identity from the individual; and they issue tickets in return; train companies don't require proof of identity, but still supply tickets; universities do require proof of identity, and give qualifications in return; and so on. DWP does require proof of identity, but offers consumers money in return, rather than validated information, and so did not design IdAP in a way that would allow individuals to receive attributes from a counterparty, and then disclose them to another counterparty. But this functionality - termed 'attribute exchange' - is vital to the development of a mature, privacy-enhancing, identity infrastructure.

D8 Taking this last point further, one sign of a future-proof design for online identity assurance is that it can lead - eventually - to the elimination of physical identity tokens (e.g. passport, birth certificate). IdAP, as it currently stands, does not meet this criterion, since many IdPs will need to inspect such tokens, or rely upon electronic records created by other organisations who have done so. PIB is - we believe - closer to being future proof, since it provides for Central Government, when it is finally ready, to issue electronic identity tokens to the individual who can then show them, using their broker account, to others.

PIB takes IdAP forward, and is backward compatible.

D9 By focusing, initially, on a relatively specialised segment of the population, i.e. students, PIB is able to offer the functionality, and address the general use cases, that could not be included within the original DWP design for IdAP. Thus PIB can be seen as the next phase of IdAP, making the scheme suitable not only for the relationship between the individual and central government, but also for relationships with schools, universities, merchants, healthcare providers etc. To highlight the advances:

- Use of face-to-face validation by Service Providers. PIB caters for Service Providers - such as schools, and universities - to contribute to validation of Key Identity Attributes: they will act, in PIB-terminology, as Proxy Attribute Authorities, so competing with one of the two roles allocated to IdPs within the IdAP scheme. (But note that there is no risk of Service Providers competing directly with IdPs: they are not positioned correctly to fulfil the IdPs' other role, that of providing a common authentication service, nor can they act as brokers - which offer attribute switching as well as authentication).

- Attribute generation and exchange. PIB is designed in the expectation that service providers will generate, as well as consume attributes. Thus, using a broker account, an individual can either (i) 'reflect' an attribute, generated by a service provider, back to the same service provider, so simply proving that he is the individual that registered - perhaps pseudonymously - with that service provider in the first place; or (ii) the individual can show an attribute, generated by one service provider (A), to another (B), so proving to B some fact that A has already recorded, perhaps the individual's identity as known to A, or student status, or qualifications, etc. This practice, of taking an attribute generated by one service provider and showing it to another, is known as 'attribute exchange;
- Communication. PIB provides for appropriately secure communication between multiple counterparties and the individual, as represented by his broker account.

D10 In order to ensure compatibility between PIB and IdAP, the brokers would need to be members of both trust frameworks, i.e. the XCOT for PIB, and whatever the trust framework designed for IdAP is eventually called. Then, when an individual with a broker account wishes to interact with central government, his broker could function as an IdP for IdAP purposes.

Annex E Possible effects of user-control on HESA

E1 When designing a new ecosystem for user control of data, starting in the HE sector, it is difficult to ignore the significant flows of data from universities to Higher Education Statistics Agency.

E2 HESA is a private limited company, which has formal agreements with government departments to provide the data that they require, and is funded by subscription from all of UK universities and higher education colleges. Its mission is 'To support the advancement of UK higher education by collecting, analysing and disseminating accurate and comprehensive statistical information in response to the needs of all those with an interest in its characteristics and a stake in its future.'

E3 In this annex, we describe what HESA does, suggest some comparators from other sectors, and discuss a number of possible drivers of change. Finally, we describe some scenarios for the future shape of HESA's services in a world where individuals control their own data. But note that these scenarios are the work of PIB-d Ltd, and have not yet been shaped by input either from: (i) HESA, to whom we hope to speak in a later phase of this project; or (ii) the University of Hertfordshire, which observes merely that HESA's appetite for data tends ever upwards.

What does HESA do ?

E4 The range of data collected by HESA is broad. Some of the required returns from institutions comprise data about things, such as: institutional profile, estates management data, finance statistics, and course descriptions. But other required returns comprise data about people, specifically: staff, student, and initial teacher training.

E5 If the functions of HESA were limited - as its name suggests - to the production of statistics, then one would expect that these people-focused returns would be anonymised at the institutional level. But this is not the case. HESA also performs certain 'administrative functions', specifically[31]: (i) maintenance of individual qualification records, for use within the HE sector to determine the eligibility of an applicant for funding to study for a further degree; and (ii) provision of data about non-EU domiciled students to the UK Borders' Agency (UKBA), as it may require in order to carry out its statutory functions. To satisfy these functions, HESA requires each institution to submit a personalised record about every enrolled student, to include name, date-of-birth, term-time address, and many other fields.

Comparators from other sectors

E6 Thus HESA is more than a statistics agency. It actually maintains a single database of information about every student that has passed through the UK HE system, dating back – presumably – to the year of HESA's creation in 1993. The functions of this database can usefully be compared to that of other databases in other sectors:

- Credit reference. In one sense, the HESA database is similar in function to the credit reference databases that serve the financial sector. Both provide a means of aggregating customer records, produced by service providers in each sector, to guard against the possibility that applicants to a further service provider will not be entirely frank when disclosing past history. HESA also shares with the credit reference agencies the problem of how to deal with (at least some) individuals who will expect to be able see, and query, their records online. More on this later.
- Learning Records Service. HESA can also be compared to the Learning Records Service, in that both store personal qualification records. But there are two significant differences: (i) LRS stores, as yet, mainly qualification data from the secondary and FE sectors, whereas

[31] See: http://www.hesa.ac.uk/index.php?option=com_content&task=view&id=141&Itemid=171

HESA stores data from the HE sector; and (ii) the LRS record exists for the benefit of the individual, who can – by design, if rarely in practice – show excerpts from their record to others, whereas the HESA record exists for the benefit of the HE sector, and there is no apparent desire to give the individual access to, or control over, it.

- National Pupil Database. NPD fulfils a similar function to HESA, but for the primary and secondary education sectors, rather than HE. As is the case for HESA, the database exists for the benefit of the sector as a whole, and there is no apparent desire to give individual access to, or control over, it.

Drivers of change

E7 The HESA database, and its various comparators, were designed prior to the advent of ubiquitous broadband, and the consequent possibility of user access to, and control over, personal data. Thus there is a question as to whether these changes will have a knock-on effect on the way HESA fulfils its function, or whether they can be safely ignored. The following factors are relevant:

- Government policy. As described in paragraphs 42 and 43 of the main paper, the Government now advocates giving individuals access to their data online, and has launched the Open Data and Midata programmes to achieve just that. The Government is now legislating to acquire powers to require that organisations comply. Although the initial focus is on commercial sectors, there is a clear intention to widen the remit as time passes.
- Better ways of obtaining data. HESA requires that institutions facilitate an annual survey of students leaving HE to find out what they go on to do. The data collected is, inevitably, a snapshot, and cannot show the way in which careers evolve. The advent of a PIB-type ecosystem may address this problem. If the majority of individuals consent to release anonymised data from their broker accounts on a periodic basis, the resulting data would form a rich resource for career path analysis.
- Change in funding patterns. As funding for the HE sector is reformed to more closely follow the student, it may become possible to determine eligibility for further funding – at least at the undergraduate level - using records held by the Student Loan Company, rather than by HESA. This change would reduce the need for HESA to gather personalised data.
- Disintermediation. As web services become ever more sophisticated, it may be possible for end-users to obtain student data direct from individual HEIs, rather than using HESA as an aggregator. As one example, it appears that the UK Borders Agency now obtains attendance data for international students direct from HEIs, and so – presumably – is less dependent on HESA.

Scenarios for HESA

E8 PIB-d can see a number of possible futures for HESA's methods of handling personal information, ranging from minimal change, to radical transformation as the new personal data ecosystem is developed. In more detail:

A. 'Business as usual'. HESA continues to collect personal information from HEIs in the current way. Given that HESA is unique in what it does, and is empowered by Government to produce the statistics required by Government (and others), it is by no means certain that change is inevitable, despite the tide flowing in favour of user access and control.

B. Use of PIB to give students access to their record. If HESA accepts that students should be given access online to their record, then it would make sense for each student to set up a relationship with HESA, from a broker account, at the same time as registering at the start of their university course. In this way, the university would be able to vouch for the student's identity, so saving HESA having to complete the same task remotely at a later date.

C. Use of PIB to obtain anonymised information from students. Provided that individuals give their consent, HESA could use brokers to obtain anonymised information – say about career paths – direct from students, as described above.

D. Use of PIB to obtain personalised information from students. Instead of obtaining student records directly from each university, HESA could – in the long term - request that the student release such information, as obtained from the university, to them via his broker account. Indeed, universities could insist that students release data in this way as a condition of attendance. But this becomes complex, and may be little better than the current approach of back-office data sharing between universities and HESA.

As yet, we don't know which of these scenarios is the more likely, or whether they will all come to pass, one after the other. For the purposes of illustration, we have used scenario C in the schematic of the 'rewired' HE sector given in paragraph 35 of the main paper.

Annex F Risks & mitigation

F1 Any project of the size of PIB faces numerous risks. Here we list those that have occurred to us so far, estimate their probability, and describe the available mitigations. The risks are grouped by phase of implementation, i.e. set-up, then operation.

Ecosystem set-up

F2 *No organisations are interested in the broker role.* This seems unlikely. DWP received 81 expressions of interest in response to their procurement for Identity Providers, and has just announced that 8 companies have been successful with their bids. We expect that most of these IdPs, and other companies in addition, will be keen to become brokers, both because of the real prospect of the scheme reaching critical mass, and because of the opportunity to acquire customers who will, later on, earn them revenues from the IdAP scheme.

F3 *Software developers are not interested.* Again this seems unlikely. Developers will flock to wherever they scent a market. PIB-d has already completed a technical design for the required software components, and may well contract with one or more developers to produce open source reference implementations, both as a starting point for others, and as a benchmark for interoperability tests.

F4 *Technology is immature.* This may be a problem. Of the two ways of enabling proper account portability, one is elegant but still unproven, while the second will work best if all brokers use near identical software stacks. There will be a need to make a clear choice between the approaches early in the next phase.

F5 *Market is not ready.* There is always a trade-off between being first to market with new technology, and getting there so early that no-one is ready to implement. PIB-d believes that this risk is modest: the company is a JV between entrepreneurs and potential lead users (the universities) and has the good fortune to be based in a country which, thanks to the Government’s Identity Assurance Programme, is leading the way in the development of distributed ecosystems for identity - and personal information - management.

Ecosystem operation

F6 *Price gouging.* The HE sector may worry that brokers will, once the ecosystem is established, attempt to charge excessive relationship fees. This is unlikely because: (i) the governance body will be a non-profit on which all parties are represented; (ii) the HE sector will - presumably - negotiate en bloc, and thus will be in a position to require reasonable tariffs from the brokers; and (iii) the HE sector may even argue, once the ecosystem is established, that they provide more value - in terms of validated data - to the ecosystem than they receive, and so should be offered a zero or negative tariff.

F7 *Identity theft*. Individuals may be concerned that using a single point to manage multiple relationships will increase the risk of serious ‘identity theft’. There are several factors here, pointing in different directions: an attacker who gains control of an individual’s broker account will certainly be able to cause damage; but the very fact that an individual uses the account for multiple relationships will mean that there is money to pay for better - i.e. both more secure and more usable - methods of authentication, and that the individual will spot intrusion more quickly. But, in the end, the individual faces a trade-off: using a single broker account for all relationships will increase risk slightly, but is more convenient; whereas spreading relationships across many accounts reduces risk, but is far less convenient. His choice may depend on the quality of services offered by the ecosystem to restore a compromised account.

F8 *Complex user interface.* In software development, there is often a trade off between offering rich functionality, and retaining an intuitive user-interface. But there are solutions, including heavy reliance upon defaults. We may even see developers competing on useability.

F9 *Technical failure of brokers.* This is always possible, but - assuming competent software development, and the provision of back-up systems - is probably less likely than a failure in a university's current internal systems.

F10 *Business failure of broker*. Again, this is possible. Or a broker may simply decide to exit the industry. As a solution, the ecosystem will build in measures to sustain a broker as an operational entity in the short-term, and / or transfer user-accounts in bulk to an alternative broker.

F11 *Abuse by broker of personal information.* Safeguards for the individual include: (i) software designed to limit access by broker to information within an individual's account; (ii) strict governance by the ecosystem; and (iii) brokers competing to win trust and thus custom.

F12 *User preference for existing social networks.* The challenge facing PIB is not to compete head on with Facebook and the like (which are discussed in detail in Annex G), but rather to market PIB as superior approach, capable of delivering new services that are beyond the reach of the current social networks. As individuals realise that they really can use a single broker account to keep areas of their life - such as friends and work/ university - separate from each other when necessary, and yet share applications (such as calendar) between them when useful, then the thoughtful may start to migrate and others will follow.

Annex G The social networks as tools for user control of data.

G1 In recent years, and leaving aside the emergence of smart phones, the biggest technology. change for individuals has been the rise of the social networks. The largest, Facebook, launched in 2004, now claims some 32 million UK users, and is clearly a popular way for individuals to socialise, sharing photos, messages, and preference information (the Facebook 'wall') with families and friends. Twitter got started two years later, has somewhere over 10 million UK users, and is the leading micro-blogging service, enabling individuals to subscribe to short messages published by others, often celebrities. Linked-In, which has some 9.5 million UK users, is popular as a means of maintaining links with contacts made at work.

G2 Despite - or perhaps because of - their success, social networks are problematic in a number of ways:

- Privacy. Social networks earn revenue by offering their services free to individuals, and then selling profile data - gleaned from each individual's use of the service - to third-parties, typically advertisers. Although many individuals are content to look at advertising in exchange for otherwise free services, many others are concerned about the consequent privacy issues. These are inherent in the social network business-model, and become more severe as the profiles held by the network becomes richer, so allowing more tailored advertising.
- Lack of supplier choice / account portability. Social networks are - as the name suggests - subject to severe network effects: each becomes more useful as more people use it, and so the largest may grow to a point where it can dictate pricing and neglect innovation. In more mature sectors - such as mobile telecoms and retail banking - regulation is used to maintain competition and ensure that individuals can easily switch suppliers. Such a remedy for the social networks might well be too heavy handed, but it's already apparent that their use as a platform for the development of other, more advanced, services is being held back by the lack of competition.
- Product bundling. Because the main social networks were created from scratch, they had no choice but to bundle two necessary, but distinct, services together. These are: (i) relationship management; and (ii) provision of tools with which an individual can create content for others to look at. Now that the world understands how social networks function, there is a strong case for unbundling these two services, so that individuals can select relationship management tools and content generation tools separately. This would result in greater competition and choice in both areas.
- Security. The social networks provide authentication mechanisms that are just good enough as protection for the kind of data that individuals typically disclose in social contexts. But their business model gives them no incentive to offer better authentication mechanisms, suitable for use to protect more sensitive personal data, such as education records, health records, proof of identity, and so on.

G3 These shortcomings leave society in a strange position: many individuals now use social networks as tools for the sharing of social data, and - by extension - would like to have a similar, if not better, level of control over the sharing of more sensitive, validated data. But, because of the social networks' structure and business model, the organisations - such as schools, healthcare providers, and the like - who generate sensitive / validated data cannot allow this to happen.

G4 And so there is an impasse: individual want to control the sharing of sensitive / personal data; (many of) the organisations who generate such data would like to accommodate them; but the obvious suppliers of the necessary tools do not want to help. There is thus an opportunity, arguably even a responsibility, for such organisations to work with start-ups to satisfy this unmet demand and so promote safe, sustainable, online behaviour.

Annex H Results of a privacy survey

H1 Before going further, it's worth asking whether the premise of this paper - that individuals want, and should be given, control of their data - is actually true. Or might the premise be similar to other popular campaigns, say that to reduce carbon footprints, which are easy for individuals to support in principle, but harder to implement because they require behaviour change? Opinions on this question vary.

H2 In 2010, Eric Schmidt, the chief executive of Google, said[32]:

> 'If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.'

At about the same time, Facebook's Mark Zuckerberg said[33]:

> ' … in the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that's evolved over time.'

H3 These are extreme views, expressed by two individuals who run successful social networks, and so have a business interest in persuading more people to share more data. The truth is more complex. Yes, the social networks do provide a valuable service, enabling individuals to feel connected to a wider group of people, so increasing what is called their 'social capital'. In some circles, a refusal to participate in social networking is even seen as a refusal to participate in civic life.

H4 But it is not true to say that privacy is dead. In a 2011 global survey[34] carried out by advertising agency Mccann Erickson, 70% of people selected '*worries me a great deal'* or '*somewhat worries me'* when asked to what extent they were concerned about the erosion of privacy. The only topic rated as of more concern - to 78% of interviewees - was the possibility of a further global financial crisis.

H5 Although a split of this data by age-group is not available, it seems fair to conclude that many people, of all generations, do care about who gets to see their more sensitive personal information, such as address, credit card statements, medical records, legal and financial documents, business secrets, bad poetry, love letters, and - even - 'the ill-advised videos taken in their hormone-addled youth'.

H6 Looking in more detail, McCann Erickson has identified - for marketing purpose - five groups of consumers based on their attitudes to privacy

- 15% of the global population, Eager Extroverts are defined by their 'love of mobility and sharing through social media. Their constant sharing has its downfalls, though, as they worry that someone might denigrate them online, leading to a sour reputation among friends.'
- At 20% of global consumers, the Sunny Sharers are the second largest group. This optimistic group is 'able to see the positive outcomes associated with sharing data. They are connecting and engaging in order to get the best experience and recommendations possible. They are mindful about sharing information that could damage their finances or reputation, but they won't let this stop them from sharing almost everything else.'
- The largest group, the Savvy Shoppers, 'embodies the data trade-offs necessary in this brave new world of sharing. This group, 37% of the global population, is willing to engage with

[32] See http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people

[33] See http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov

[34] See 'The Truth about Privacy', available for download from http://truthcentral.mccann.com/truth-studies/

businesses, but wants to see safeguards such as security certificates and to receive something in return such as discounts.'

- The smallest group of consumers, 9% globally, is the Cautious Communicators. This group is defined by their 'pronounced dislike of mailings, messages and other forms of frequent contact. While not particularly worried about the erosion of personal privacy, this group is the least likely to sign up for company newsletters and offers and express a strong desire to know exactly how their data will be used.'
- The final group is the most private. 19% of global consumers are Walled Worriers, being the most sensitive to 'perceived invasions of privacy. Although this group harbours a mistrust of businesses, they're not that resistant to receiving news or offers through e-mail. They do, however, require assurances that data collection is minimal and won't be shared with third parties.'

H7 This analysis leads to the question of which groups of individuals are well served by the tools for data sharing that currently dominate the market, i.e. the social networks. The Eager Extroverts and the Sunny Sharers are reasonably content. The Cautious Communicators are not happy, but are principally concerned about a symptom, i.e. unsolicited communications, rather than the erosion of privacy as the root cause. The Savvy Shoppers see the need for improvement to current tools and practices, but they can get by with what exists at the moment, and would only upgrade to a better approach when convenient; while the Walled Worriers would probably switch to a better approach immediately. All told, it seems that about 65% of the population see the need for better approaches to privacy, and would adopt improved tools, either immediately following market launch or at some point thereafter.

Annex I Forthcoming changes to data protection legislation

I1 On 25 January 2012, the European Commission published a proposal for a new general Data Protection Regulation and Directive. The proposal is wide-ranging, and can be seen as a response to the accepted need for an updating of existing legislation.

I2 PIB-d does not claim to be expert on the nuances of data protection law. However, we know there are many instances where the rights of data subjects appear to conflict with the duties - as codified in current statute - of public-sector organisations to collect and process personal information. In some of these cases, such as the processing of criminal records, it is clear that the needs of society must override the rights of the individual. But in other cases, particularly in the education sector, the statutes permitting collection and processing of data seem to be out of date, having been drawn up before individuals could be given online tools to control the use of their data.

I3 Thus we are encouraged by the EC's intention to strengthen the rights of the citizen, and the privacy protection available to him. We hope that the UK's own legislation will soon be updated to ensure that all organisations, both those in the private sector and - wherever possible - those in the public sector, can implement the following principles:

- Consent. Organisations will be required to obtain consent, either explicit or implicit, from an individual before collecting or processing data, rather than relying on the lack of an objection.
- Data protection by design / Data minimisation. Organisations will be required to design their processes so to afford the individual better privacy from the outset, rather than applying privacy-coloured lipstick to large pigs of personal data. One obvious design strategy is to minimise the amount of data collected in the first place.

I4 It is likely to take some time for the Commission to complete work on the new regulation and directive. The results may, perhaps, become effective in English law in 2014 or 2015. Nevertheless, the direction of travel is already clear, and is unlikely to change.

Annex J 'Point' solutions - Dare, Moonshot, and Office365

J1 The HE sector is experimenting with three initiatives that address some – but by no means all – of the issues described in the early part of this report. They are DARE, Moonshot, and Office365.

DARE

J2 To address the proof-of-qualification issue, six universities have cooperated to create a multi-tenant shared service for degree checking, relying upon standards-based software developed by Digitary. In brief: the DARE (Digital Academic Records Exchange) project extracts records from a university's student record systems, arranges for the university to sign them digitally to create electronic certificates, and stores these certificates on a server exposed to the public internet; a student then signs in to the certificate-store using their university username and password, creates a web-page showing the information they wish to disclose to a recruiter; and then sends recruiters - by e-mail or some other means - a web address (known as a 'share') for the page.

J3 DARE has both strengths and weaknesses. For each university, DARE works well, effectively solving the proof-of-qualification problem at modest cost. For individuals, DARE is convenient and privacy-enhancing, but only works for their university qualification: it does not enable them to construct a personal qualification record, or provide proofs of multiple qualifications to a potential employer. Even if DARE became ubiquitous, the individual would - for each qualification - have to remember a (different) username and password for each awarding body, and then create a separate document 'share'.

Moonshot (& eduroam)

J4 JANET, the network provider for the UK's HE sector, has already taken some steps to address the multiple username/ password problem. The eduroam[35] service enables individuals to use their home university log-in to gain access to wireless networks at other participating universities around the world. And the more recent Project Moonshot[36] extends the reach of federated single-sign-on to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures, and other commonly deployed services including mail, file store, remote access and instant messaging.

J5 These tools work well, and make life easier for individuals for as long as they maintain a stable relationship with a single host institution. Thus tenured academics are happy. But the tools do not address the needs of individuals - such as students - who may have a (relatively) short relationship with a university, and then move on to other activities. What they need is a means of authentication that travels with them, ideally from school to university, and then on into subsequent life. For some, the obvious solution is to ask their university to let them login with a username and password that they may already have, provided say by Facebook, Google, Linked-In, or Microsoft. But universities are, very sensibly, not enthusiastic about this suggestion, for the reasons explained in Annex G.

Office365 (& Google Apps.)

J6 Microsoft is now offering an online version of its Office suite of programmes, using the brand Office365. Rather than sell the software outright, they licence it on a per-capita basis, with steep discounts offered to universities and other educational institutions. Similarly Google offers its Google Apps suite of online office applications, again with steep discounts for education.

[35] See www.eduroam.org/

[36] See https://community.ja.net/groups/moonshot

J7 Both O365 and Google Apps help universities address some of the issues above, offering – as well as the office applications - online calendars, and coherent communication tools. Both work well as solutions for a university as a standalone organisation, but are not designed as infrastructure to improve the way in which individuals interact with many different organisations, and give explicit permission for the transmission of personal information between them. They lack key features required for this broader role, such as open-standard code, governance in the public interest, and a business model that shares the costs fairly among the stakeholders.

--

Annex K List of acronyms and abbreviations

This list is provided as a remedy to the alphabet soup of abbreviations that is inevitable in a document of this kind. It does not purport to be a glossary - definitions of terms are generally given in the text when they first arise.

A-level	Public exams taken at the age of 17/18
BIS	Department of Business, Innovation and Skills
ChA	Characterising Authority
CRM	Customer Relationship Management
DARE	Digital Academic Records Exchange
DWP	Department of Work & Pensions
GCSE	Public exams taken at the age of 14/15
HE	Higher Education
HEDD	Higher Education Degree Datacheck
HEFCE	Higher Education Funding Council
HEI	Higher Education Institution
HESA	Higher Education Statistics Authority
HMRC	Her Majesty's Revenue & Customs
IdAP	Identity Assurance Programme
IdP	Identity Provider (within IdAP)
IoT	Internet of Things
IPS	Identity & Passport Service
JANET	Joint Academic Network
JV	Joint Venture
Key Identity Attributes (KIA).	Name, address, previous address, date of birth.
LRS	Learning Records Service
MNO	Mobile Network Operator
MOOC	Massive Open Online Course
NFC	Near Field Communication
NUS	National Union of Students
PIB	Personal Information Brokerage
PIB-d	PIB- development Ltd
SLC	Student Loan Company

SMS	Short Message Service, a.k.a. a ‘text’
SP	Service Provider
SPA	Service Provider Acquirer
UCAS	Universities and Colleges Admissions Service
UH	University of Hertfordshire
UHSU	University of Hertfordshire Student Union
UKAMF	UK Access Management Federation
UKBA	UK Border Agency
ULN	Unique Learner Number
VLE	Virtual Learning Environment
VRM	Vendor Relationship Management
XCOT	eXtensible Circle of Trust
