enisa
European Network
and Information
Security Agency

Managing multiple electronic identities

enisa

European Network
and Information
Security Agency

The European Network and Information Security Agency (ENISA) is an EU agency created as a response to security issues of the European Union. The Agency's mission is essential to achieving a high and effective level of network and information security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of network and information security for the benefit of citizens, consumers, business and public sector organisations in the European Union. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between European institutions, the Member States and industry players.

Contact details

For enquiries about this study, please use the following contact details:
European Network and Information Security Agency
Technical Competence Department
Email: sta@enisa.europa.eu
Internet: http://www.enisa.europa.eu/act/it/eid

Supervisor of the study: Sławomir Górniak – ENISA
Authors: John Elliott, Margaret Ford, Dave Birch – Consult Hyperion
ENISA staff involved in the project: Demosthenes Ikonomou, Rodica Tirtea

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies, unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA, nor any person acting on its behalf, is responsible for the use that might be made of the information contained in this publication.

Table of contents

TABLES

Executive summary

Though the field of digital identity is still developing, some key principles have emerged. Many of these have their origins in the following:

- OECD Privacy Guidelines (1980) [OECD PRIV];
- EC ‘Data Protection’ Directive 95-46 (1995) [EC DPD];
- Kim Cameron, The Laws of Identity (2005) [KC LAWS ID].

Nowadays each person has the opportunity of living multiple lives in parallel, in the real as well as in the virtual world. A trend observed over the last years, first in the research community, but now also in commercial offerings is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet.

An area of particular interest is the management of multiple identities, where “identity” is being considered in a broad sense. Issues related with this area include anonymity, pseudonymity, unlinkability and unobservability. The increasingly digital nature of relationships between people is central to dealing with those issues. It is not a question simply of hardware or software, but more importantly of enabling people to enjoy and benefit from their online experiences, while dealing with potential issues. The problems might include a lack of knowledge or training, difficult personal circumstances or simply irritation at the diversity and unpredictability of online privacy and identity mechanisms. It is therefore vital that we should have strong, reliable mechanisms, which can be easily understood and relied upon across the course of a lifetime.

This paper is divided into two parts. In the first one, section 2 introduces the key concepts of electronic identity, while section 3 presents available methods of managing multiple identities.

The second part (Section 4) gives the guidelines and recommendations with regard to multiple identities. The addressed issues are grouped in three categories (users, technical communities, policy makers) although in many cases there are significant areas of overlap.

The main challenges identified with relation to end users consist of the whole life approach to the management of identities, reputation of individuals, their online behaviour and use of technical protection. In this respect, the following recommendations for the communities of end users are the most important:

- Education targeted at the general public should be simple, practical and broad in scope
- There is a value in exploring means of ‘forgiving’, which could take a form of ‘reputation bankruptcy’
- Keeping safe online involves awareness of one’s own behaviour, which should be based on the kind of common sense
- It is important to keep in mind that technical protection is not a panacea for all potential risks.

Technical communities – developers of software, architects of IT systems etc. – are faced to numerous problems related to infrastructural anonymity, renewals and revocation of credentials (also biometrical), unlinkability of identities, minimal disclosure issues and attacks against identities. This study provides guidelines for them, where the most relevant are:

- There are strong social reasons to provide credible anonymity in digital environment, but not leading to a form of anarchy

- Privacy-enhancing technologies have a role to play in promoting effective mechanisms to support true or conditional anonymity

- Greater emphasis should be placed on the desirability of maintaining unlinkability between digital identities

- It is important that policies relating to multiple identities are considered at the design stage of system planning and implementation. Systems should have the ability to limit the risk of attacks while maintaining a reasonable degree of separation of identity

The biggest number of recommendations included in this paper is addressed to the policy makers – legislators, regulators and government services. Identified issues in this group relate to effective regulation, role of public sector, best practice incentives, enforcement and regular review of legislation. The main recommendations are:

- It is essential that individuals feel empowered to protect their own identity data. In the global market place it has to be handled by taking a global approach.

- By nature of their operations, public sector bodies have the greatest incentive to act as an example to the business world

- There is a significant need for greater recognition and adoption of best practice around identity management.

- Policy measures promoting open source initiatives should be used to contribute to a more flexible, reliable ecosystem

- Substantial measures are required to monitor and curb excessive surveillance of individuals by third parties

- As it is expected that the online environment will continue to change rapidly over coming years, relevant legislation must be adapted as necessary.

1. INTRODUCTION

1.1 Background

For approximately ten years, European Member States and EEA countries have been implementing electronic identity management (eIDM) systems based on their national requirements, which included improving administrative efficiency, improving accessibility and user-friendliness, and reducing costs. 'As an authentication token and personal data source, an eID card is a gateway to personal information.' [ENISA PRIV]

These requirements can be improved at the European level by improving the interoperability of electronic identification/authentication systems currently operated at national level.

Each person has the opportunity of having multiple identities in the real world, as well as in the virtual world, examples including: national identification number, local library identity, leisure club identity, bank account number, eBay user ID, social networking identity and others. A trend observed over the last few years, first in the research community, but now also in commercial offerings, is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet.

An area of particular interest is the management of multiple digital identities. In this context, "identity" is being considered in a broad sense (i.e. eID, federated identity, RFID, avatars, etc.). Specifically, this study aims to investigate the ways in which an individual may choose to use different electronic identities, either separately or in combination, to achieve a range of goals online. In investigating these options, due attention is paid to the associated issues and benefits.

This study will identify and describe the ways of:

- Managing multiple identities
- Providing best practices and guidelines in this area

1.2 Scope of this document

The scope of this report is as follows. It:

- Identifies and describes a broad set of types of digital identities
- Identifies and describes general techniques of managing multiple identities
- Identifies good practices and develops key guidelines for three communities:
    - Technical – software developers, standards development organisations
    - Policy – policy makers
    - End users – organisations leading awareness raising campaigns

1.3 Report structure

The report is structured as follows:

1. ***Introduction (this section):*** Provides an overview of this study and its scope, the structure of the report and the intended audience for whom the report is written.

2. ***Electronic identity key concepts:*** The key concepts relating to electronic identity are briefly explained for the reader unfamiliar with the field.

3. ***Methods of management of multiple electronic identities:*** Consideration is given to systems that have failed in the past and what lessons can be learned. Current and emerging systems are considered in as much as they address the management of multiple electronic identities belonging to the same entity.

4. ***Guidelines and best practice:*** In the light of the analysis in the previous sections, guidelines are presented for three user groups wishing to facilitate the management of multiple electronic identities: End user; Technical; Policy.

2. ELECTRONIC IDENTITY KEY CONCEPTS

Electronic identity is in different stages of development in various countries. In this chapter we introduce some existing models of electronic identity and take key elements of what they propose as the basis for the model to be used in this report.

In the process, we define key terms that the reader unfamiliar with the field will need to understand and also some that do not (yet) have an agreed definition, so that all readers will know what is meant by them. Where possible, we avoid introducing new definitions for terms that are already used in this field.

2.1 Current electronic identity landscape

Digital-age society relies increasingly on access to information and services online. At the same time, we have seen an increase in the levels of threat to personal or sensitive information and transactions, meaning that the probability of loss is increasing all the time.

Most identity systems to date have been monolithic, created and used for a single specific purpose only, operating within their own separate domain and not addressing the problem of multiple electronic identities that is the subject of this report. This has resulted in users having a multitude of (incompatible) electronic identities in order to access the services that they require, i.e. each identity can only be used in a particular context and mutual recognition of authentication tokens between contexts is still far from standard practice. Today's criminals often exploit weak authentication solutions for individuals, web sites and email,. For example, phishing attacks seek to capture active usernames and passwords. As Kim Cameron puts it:

We are headed towards a deep crisis: the ad hoc nature of Internet identity cannot withstand the growing assault of professionalised attackers. [KC LAWS ID]

As a result, the trust necessary for thriving online services has not been established. How does an e-commerce site know it can trust credentials from an identity provider without knowing if that provider's security, privacy, and operational policies are strong enough to protect the site's interests? This is not a technology problem; it is a business, legal and social problem that must be solved with policy-based solutions. The current lack of user-centricity means that solutions are often dictated to the user, who is left to manage a multiplicity of electronic identities.

2.1.1 Definition of key terms

One of the key problems in the field of digital identity has been the lack of agreed terminology. The problem is being addressed at the time of writing under the ISO 24760 Identity Management Framework, in co-operation with PrimeLife [POLICIES], and is not available at the time of writing. Therefore, we briefly summarise the key terms that are used in this report, citing respectable sources where possible:

- ***Individual:*** A person engaged in an online transaction. [NSTIC]
- ***Non-person entity (NPE):*** Organisations, hardware, software or services engaged in an online transaction. [NSTIC]
- ***Identity:*** An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as "the identity", but several of them. [TERM]
- ***Identifier:*** A name or another bit string. E.g., nicknames chosen by a user may contain information on heroes he admires; a sequence number may contain information on the time the pseudonym was issued; an e-mail address or phone number contains information on how to reach the user. [TERM]. Used to identify a subject within a domain

- ***Digital identity:*** A digital identity, which is a set of attributes, represents an individual in a transaction [NSTIC]. Note that Kim Cameron's definition, a set of claims made by one digital subject about itself or another digital subject [KC LAWS ID] is very similar where claims and attributes are the same in this context

- ***Attribute:*** Named quality or characteristic ascribed to an individual or NPE. Attributes might be values (e.g. date of birth) or claims (e.g. is over 21). Definition derived from both [NSTIC] and [TERM]

- ***Credential:*** Attributes including their authentication by third parties [TERM]

- ***Device:*** Object that can be used for storing identifiers, attributes and credentials related to a subject. Examples include a smart card, an NFC mobile phone secure element, a USB dongle and a security chip inside a PC

- ***Identification:*** Establishing unique digital identities [NSTIC]

- ***Authentication:*** Associating an individual with a unique identity [NSTIC]. Providing evidence for the association is essential to this.

- ***Authorisation:*** Enforcing what services/resources the subject is entitled to access

- ***Identity Provider (IDP):*** Responsible for the processes associated with enrolling a subject, establishing and maintaining the electronic identity. [NSTIC] An IDP is usually also an AP for a particular set of attributes of its subjects

- ***Attribute Provider (AP):*** Responsible for the processes associated with establishing and maintaining identity attributes. [NSTIC]

- ***Relying Party (RP):*** Requires trusted assertions about subjects. [SWIMF] Makes transaction decisions based upon its receipt, validation and acceptance of a subject's authenticated attributes. [NSTIC]

- ***Subject (of transaction):*** either an Individual or an Non-Person Entity (see below). [NSTIC]

- ***Discovery Service Provider (DSP):*** Finds and authenticates the subject's IDP on behalf of any RP. The assumption is that there may be many IDPs and so each RP does not generally know where to go to validate assertions from unknown subjects. [Liberty DSF]

- ***Anonymity:*** An anonymous person is 'a person whose name is not given, or is unknown' [OED]. Here is a simple example: I am my own identity provider, so I create the identity Lewis Carroll and sign it myself. There is no third party who knows that Lewis Carroll is me. Such self-asserted identities are unlikely to have much commercial value in the online future, but they are nevertheless an important element of the identity portfolio

- ***Pseudonymity:*** 'A pseudonym is an identifier of a subject other than one of the subject's real names' [TERM]. Here is a simple example. Imagine walking into a shop to buy something with your debit card. The card has a computer chip on it and when you punch in your PIN at the checkout, the chip tells the merchant's till that the PIN is correct. Therefore, the merchant's till is able to accept the bank card, you take your goods and walk out. The shopkeeper has no need to know your name, only that you are authorised to complete the transaction

- ***Absonymity:*** The final case, the absonymous identity, is where the real world identity is transparent to the relying party (although they may still wish to verify with a third party; the relying party may not, for example, be able to determine for themselves whether a passport is real). It can be very inconvenient to the individual to have to use this form if identification in the absence of anything better (e.g. the UK driving licence reveals name and address on the front of the card).

Various EU-funded projects have addressed some of the issues described in Section 2.1 (e.g. MODINIS, PRIME, PrimeLife [POLICIES], STORK, FIDIS), but only industry and international standards will change the way online identity is carried out. There is standardisation work underway (ISO/IEC CD 24760[1]) to try to produce a framework for identity management. However, the work is not yet public and is not expected to be completed until April 2013.

The US draft National Strategy for Trusted Identities in Cyberspace [NSTIC] presents the Identity Ecosystem as a layered model that provides interoperability of electronic identities and services and we will use these layers in our study in the remainder of this report:

- An ***execution layer***, where the online transactions that use virtual identities take place according to agreed rules of the Identity Ecosystem
- A ***management layer***, where the rules for participants in the Identity Ecosystem are enforced
- Above that, a ***governance layer*** where the rules required to function in the Identity Ecosystem are established and maintained.

It is interesting to note that NSTIC and the Open Identity Exchange[2] [OIX] Open Identity Trust Framework (OITF) propose similar layers, but with slightly different naming conventions. For this report, we will use the layers proposed in NSTIC, since it is well-structured and already receiving widespread attention.

2.2 Layers of the Identity Ecosystem

Having defined the key terms we wish to use, we next describe the main operations that occur within the layers of the Identity Ecosystem.

2.2.1 Execution layer

The execution layer is the level at which subjects interact in the form of transactions that follow established rules. Relying parties offer online resource or services to subjects (individuals or NPEs). All parties need to be able to trust the capabilities of the system in order to transact with confidence.

Subjects can obtain digital identities that contain appropriate attributes from IDPs. These attributes can be presented by the subject as ***assertions*** to be verified by the RP before ***authorising*** access by the subject to the resource or service.

2.2.2 Management layer

The management layer is where digital identities are created, maintained and revoked. Subjects affiliate with at least one Identity Provider (IDP). IDPs validate the identity of subjects (during an ***enrolment*** process) and ensure that the digital identity accurately reflects the real-world identity of the subject, as appropriate to the level of identity proofing being used. This may range from a high level of proof to none at all, e.g. self-asserted identities where the subject is the IDP.

Attribute Providers (AP) can confirm, bind and assert attribute information about a subject [NSTIC]. This provides flexibility, allowing the subject to obtain a digital identity from an IDP without having to prove attributes that are already known by an AP. The attributes can then be bound to their identity.

IDPs associate validated attributes (credentials) to a digital identity. The digital identity also includes an ***identifier***, which might be some sort of name (e.g. a nickname or an email address), or simply a unique number (e.g. a mobile phone number or an identity card number).

[1] http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306

[2] The Open Identity Exchange (OIX) is a non-profit corporation serving as an independent, neutral provider of certification trust frameworks for open identity technologies.

When an identity becomes obsolete, either at the request of the subject, or as a result of the provider deciding to remove it from the system, the associated credentials are revoked. Although in principle a simple step, revocation is commonly overlooked, as it is a disabling rather than an enabling process.

2.2.3 Governance layer

The purpose of the Governance layer is to allow unaffiliated entities to trust each other. NSTIC defines the following:

- ***Governance Authority (GA):*** Governs using an agreed Identity Ecosystem framework, which establishes overarching standards and laws that apply to trust frameworks. Defines the criteria for assessing and certifying other bodies in the Identity Ecosystem (Accreditation Authorities, Service Providers). There may be more than one GA. For example, in a payments environment, both Visa and Mastercard might be regarded as GAs

- ***Service Providers:*** IDPs, APs and RPs

- ***Accreditation Authority (AA):*** Assess and certify Service Providers

The trustframework mentioned above under the GA identifies the specific requirements associated with a particular set of participants and transactions within the Identity Ecosystem. For example, one might imagine the established *IdenTrust*[3] scheme having a trust framework covering its member banks for *IdenTrust* transactions within a larger Identity Ecosystem.

2.3 Research and development, projects

We are now in a period of intense R&D and collaboration over how to solve the issues of managing digital identities. There are a number of key projects – primarily funded by the European Commission – that are exploring and establishing pan-European standards in electronic identity.

2.3.1 FIDIS

The Future of Identity in the Information Society (FIDIS)[4] is a large EU FP6 Network of Excellence targeting various aspects of digital identity and privacy. The partners of the project are universities and companies working in areas related to digital identity. FIDIS areas of interest include new forms of ID cards, usage of identifiers in information systems, technologies used for citizen's identification and profiling. The activities cover:

- 'Identity of identity' (definitions of key terms in the domain)

- Profiling

- Interoperability of IDs and ID management systems

- Forensic implications

- Privacy and the legal-social content of identity

- High-tech ID

- Mobility and identity

[3] http://www.identrust.com/
[4] http://www.fidis.net

FIDIS has provided a number of publications on the changing nature of ‘natural’ to ‘digital’ identity, and predictive publications on possible scenarios for the future of ID. This includes substantial work on the nature of 'partial identities' or personae. FIDIS started in 2004, and whilst it has technically finished, the project continues to provide deliverables.

2.3.2 STORK

STORK[5] is a large-scale pilot operated by a consortium of European public administrations and private partners and 50% co-funded by the EU. It aims to implement an EU-wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. It will also pilot trans-border eGovernment identity services and learn from experience how to roll out such services, and to understand the benefits and challenges an EU-wide interoperability system for recognition of eID will bring.

The STORK interoperable solution for electronic identity (eID) is based on a distributed architecture that will pave the way towards full integration of EU e-services, while taking into account specifications and infrastructures currently existing in EU Member States. Its goal is to simplify administrative formalities by providing secure online access to public services across EU borders. The solution provided is intended to be robust, transparent, safe to use and scalable, and should be implemented in such a way that it is sustainable beyond the life of the pilot.

The project aims at:

- Developing common rules and specifications to assist mutual recognition of eIDs across national borders
- Testing, in real life environments, secure and easy-to-use eID solutions for citizens and businesses
- Interacting with other EU initiatives to maximize the usefulness of eID services

STORK takes diverse implementations and reduces them to a simple set of architectural options, which simplifies interoperability of the Member States’ ID systems. Pilots, including private sector identity service providers, are expected to go live in 2011.

2.3.3 PRIME

PRIME[6], an EU FP6 project, concluded in June 2008. PRIME aimed to develop a working prototype of a privacy-enhancing identity management system, and included formative work on PETs (Privacy Enhancing Technologies) and their potential contribution to a trusted information society.

To foster market adoption, novel solutions for managing identities had been demonstrated in challenging real-world scenarios, e.g., from Internet communication, airline passenger processes, location-based services and collaborative e-learning.

PRIME was essentially a research project. The work on prototype development was a means to validate its new scientific and research results. PRIME's work is now continued by PrimeLife, PRIME's follow-up project.

[5] http://www.eid-stork.eu/
[6] https://www.prime-project.eu/

2.3.4 PRIMELife

The successor to PRIME, PRIMElife[7] is an FP7-funded project researching core privacy and trust issues. The programme's objective is to facilitate anonymity in life-long personal data trails, without compromising on system functionality. To achieve this, PRIMELife will focus on areas of human computer interfaces, configurable policy languages, web service federations, infrastructures and privacy-enhancing cryptography. Open source communities and standardisation bodies will be encouraged to adopt privacy technologies.

The project has produced some exceptionally high quality deliverables. These include a comprehensive overview of the strengths and weaknesses of existing approaches to identity, with a particular focus on the complex issue of protecting privacy across a lifetime [PL OSI]. While mainly looking into open source initiatives, it also takes appropriate account of other very influential offerings, such as Microsoft CardSpace. Another significant contribution is the discussion of the nature and role of trust when using web protocols [PL TRUSTED]. This looks in detail at the structures that may be used to underpin trusted content and the issues still to be resolved in this area.

PrimeLife reviews the experiences of individuals across the different EU Member States in relation to government identity, education, health, employment and social interaction. In doing so, it describes the changes which affect identity throughout life. Some of the proposed responses to the issues uncovered in exploring these changes include a privacy-enhanced backup and synchronisation demonstrator and further development of policy languages.

2.3.5 PICOS

PICOS[8] is an EU FP7 project running from 2007-10. Its objective is to provide privacy-enhanced identity features within complex, community-supporting services that are built on Next generation networks. It will provide a GUI tool for managing multiple partial identities and creating communities of users. There is a concept of private rooms, a place to store personal data and share these with communities by defining personal privacy policies. This could be like a privacy-enhanced version of Facebook.

PICOS has worked with user groups, including anglers, taxi drivers and online gamers, to develop a detailed privacy and identity framework to support their mobile and Internet communications needs. In many cases these involve both sharing information and maintaining a competitive advantage. In the case of online gamers, the exploration of relationships is particularly interesting. While identifying the standard interactions between online gamers and the privacy protection required to support these, it also highlights the fact that individuals involved in an online gaming environment may already know each other in an entirely different social setting, such as a place of work, or school. Whether they choose to interact with one another within the game or not, these external relationships can still have important privacy implications.

PICOS has the concept of 'blurring', which allows mobile users to hide their exact location to within a previously defined radius. It also has a useful 'Privacy Advisor', which aims to create awareness of online privacy risks. It does this by notifying the user when they are about to disclose personal information, such as their telephone number or postcode.

2.3.6 TAS3

The TAS3[9] Integrated Project (Trusted Architecture for Securely Shared Services) is a 4-year EU FP7 project running from 2008 -11. It aims to have a European- wide impact on services based upon personal information, which is typically generated over a human lifetime and therefore is collected and stored at distributed locations and used in a multitude of business processes.

[7] http://www.primelife.eu/
[8] http://www.picos-project.eu/Home.75.0.html
[9] http://www.tas3.eu/

Key features of this project include:

- Attribute aggregation from different locations;
- Multiple 'sticky policy' evaluation; (see Section 3.2.2.2)
- Privacy-protecting work flows.

2.3.7 SERAMIS[10]

SEMIRAMIS defines a Pilot infrastructure which provides e-services in line with the required underlying secure authentication and management approach and tests it on the basis of two scenarios representing a large number of options related to ID Management and Secure Data Transfer.

SEMIRAMIS will provide an easy-to-implement and easy-to-use solution for single sign-on and secure access to services on which novel offerings can be easily deployed.

2.4 Academic federation/inter-federation

2.4.1 Kantara

The Kantara[11] initiative was established in 2008 to create a robust focal point for collaboration within the identity community. The programme aims to bring together work on key issues, including interoperability and compliance testing, identity assurance, policy, privacy and software development. Members of the initiative (who contribute towards its funding) include the DataPortability Project[12], the Concordia Project[13], Liberty Alliance[14], the Internet Society (ISOC)[15], the Information Card Foundation (ICF)[16], OpenLiberty.org and XDI.org.

Kantara is unique in being the first time that so many other initiatives have collaborated on a common goal of improving adoption of interoperability within identity.

2.4.2 TERENA (EU)

Terena[17] provides a forum to collaborate, innovate and share knowledge in order to foster the development of Internet technology, infrastructure and services to be used by the research and education community. In the context of electronic identity, Terena looks at interoperability between existing federations. Established US federation programmes with Terena liaison include Internet/2[18] and InCommon[19]. Terena is engaged in ground-breaking work in attribute-level authentication, and technical and policy-level interoperability of Levels of Assurance (LoAs).

2.5 Multiple identities

We have established above that a number of different identities may be associated with an individual, not all of which will present the same credentials, or have the same identity provider. In different circumstances, a person may wish to transact with another person as an individual, as a pseudonymous individual, as an agent of a company and so on. One can envisage people having a number of different electronic identities (just as they have a number of different credit cards) and one can further envision an electronic identity being shared between a number of people (e.g. corporate officers). One could certainly imagine niche identity providers springing up across both horizontal and vertical sectors (the government, from this perspective, becomes a special case of a niche identity issuer) where economics or other pressures dictate.

[10] http://www.semiramis-cip.eu/
[11] http://kantarainitiative.org/
[12] http://www.dataportability.org/
[13] http://projectconcordia.org/
[14] http://www.projectliberty.org/
[15] http://www.isoc.org/
[16] http://informationcard.net/
[17] http://www.terena.org/
[18] http://www.internet2.edu/
[19] http://www.incommonfederation.org/

2.6 Classification of electronic identities

When considering the potential uses of an electronic identity, we need to consider the following significant factors:

- ***Level of Assurance (LoA):*** This determines the level of confidence we have in virtual identities and their claimed attributes. We have used the levels suggested by Kantara [KANTARA], which are both well defined and comprehensive, ranging from Low (no confidence) to Very High (e.g. positively vetted).

- ***Strength of Authentication:*** Quality of the association between an entity and the associated ID. See Section 2.1.1

There are guidelines matching appropriate strength of authentication to levels of assurance, such as that from NIST [NIST AUTH]. Using these two factors as axes, we can produce a two-by-two matrix to distribute the electronic identities as shown in Figure 2 1. In general, as LoA increases, so should strength of authentication and so we see a scattered distribution, but with a trend line from top left to bottom right.

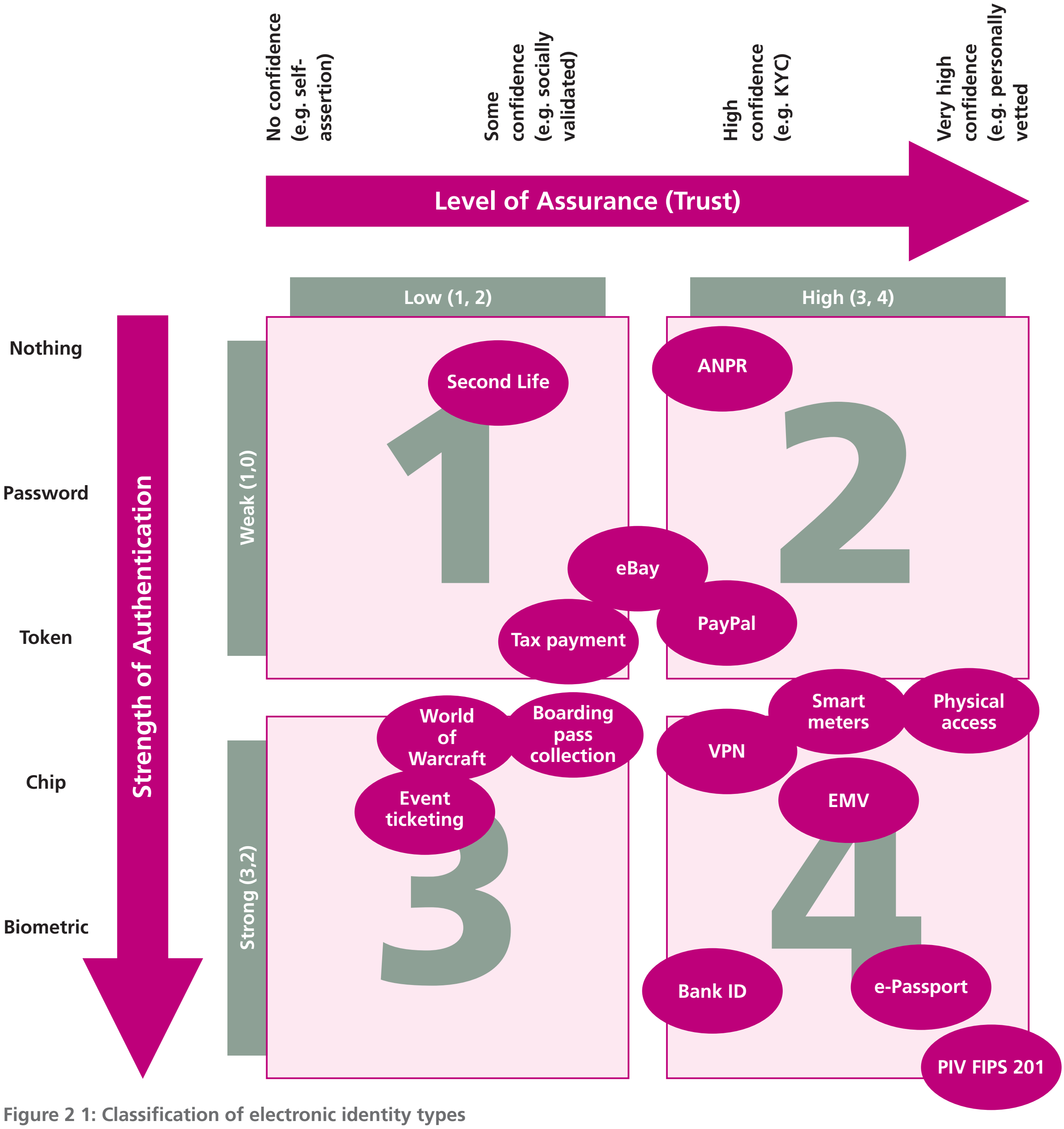

Figure 2 1: Classification of electronic identity types

The first quadrant contains a low level of assurance (e.g. self asserted identities) and low authentication (nothing or username and password). The digital identities are not very useful for performing transactions, since they provide low levels of security and are easily phished. However, they represent the majority of identities that we use today.

The second quadrant represents identities used for online payments (such as PayPal) and online auctions (e.g. eBay). The level of confidence in the identity is higher (typically through linking with bank accounts), but the presence of the identity owner is not well authenticated, due to the overwhelming use of username and password.

Applications cross from the first quadrant into the third where the strength of authentication is increased, e.g. through the use of a second channel.

In the fourth quadrant, there is a high level of assurance and strong authentication. It is these kinds of trusted digital identities that might be used in transactions (for e-business, e-finance, e-government and so on).

Apart from the confidence afforded by the level of assurance and strength of authentication, a certain degree of social validation is inherent to the situations in which particular identities are used. For example, if I am playing an online game with someone who knows me well, they will most likely be able to tell by the pattern of my actions and communications if another person has taken over control of my character in that game. Social clues would offer the possibility to expose an impostor.

2.7 Types of electronic identity

Table 2 1: Examples of electronic identities

In Table 2 1 we consider the various types of electronic identity that are available and being used today. To recap, we have defined an electronic identity as an identifier and attributes stored in a device. The term 'Internet computer' is used here to denote a computer with Internet access.

Application	Identifier	Authentication strength	Device	Assurance (LoA)	Comment
Twitter, Facebook, etc. Online gaming (e.g. Second Life)	Username	Weak: Password	Internet computer, mobile etc	Low may be socially validated	Low level of authentication since passwords are easily phished.
Online gaming (e.g. World of Warcraft)	Username	Strong: 2FA, PIN + OTP generated on mobile phone	Mobile phone	High - PIN	Recent events have shown the high real-world value of virtual gains, such as skill points and weapons. Therefore, there is demand for better protection than username and password. Using a second channel (such as OTP) provides stronger authentication.
Automatic Number Plate Recognition (ANPR)	Vehicle number plate	Weak (possession of ticket)	Magnetic strip ticket	Low: the holder of the ticket could be anyone	Traditionally used for policing purposes, in some airport car parks, vehicle number plate recognition is used to advise you where your car is parked on your return. You present your ticket and the zone your car is parked in is displayed. The information is based on the last ANPR camera to log the car before it parked.
Online Auction (e.g. e-Bay) PayPal	Username	Weak: Password	Internet computer	Socially validated and credit card registration Bank account details if accepting payments on PayPal.	PayPal is requiring stronger assurance of identity on registration. Once an account has received over a certain amount, further checks are required, using bank account payments and codes to keep the account running.
Tax payment	Username	Weak: Password	Internet computer	UK Government Gateway requires PIN to be sent to your address.	Most governments do not care who pays your tax, so strong authentication seems not considered important for this application.

Table 2 1: Examples of electronic identities

Application	Identifier	Authentication strength	Device	Assurance (LoA)	Comment
Airport boarding pass collection	Frequent flyer a/c no or payment card a/c no on card magnetic strip	Weak: Something you have (the card)	The magnetic-strip card	High if credit card used	Someone could easily collect your boarding pass using your card. The security at airports relies on checking other ID documents you travel with, such as passports.
Event ticket collection	Payment card number and name	Weak: Visual inspection only of something you have (the card)	Plastic payment cardface	Low since the card could be easily forged	This is not electronic identity since only visual inspection of the card is made on collection of the tickets.
Transit smart card (e.g. Oyster, London)	Card number. Can be anonymous or registered and linked to bank account for top up	Weak: Something you have (the card)	Contactless chip card	Low unless registered, but not intended as an identity.	The transit card can simply be an anonymous ticket, or it could be a valuable season pass owned by an individual.
Bank ID (PKI-based identity issued by ten banks in Sweden)	Private key	Strong: 2FA, smart card or phone SIM containing a private key and requiring PIN entry.	Smart card or mobile phone SIM	High: bank customer background checks	More than 2 million people use BankID in over 400 private and public services. According to Swedish law, and within the European Union, BankID is an advanced signature and a signature with BankID is legally binding. The customer's identification is guaranteed by the bank issuing the BankID. RPs must check the validity of the customer's identity and signature, using software developed by certified specialist companies. BankID is available on smart card, soft certificate and on mobile phones.
VPN	Staff number	Strong: 2FA	Smart token	High	We are assuming that this is a corporate VPN that requires 2FA and that tokens are only issued to verified staff, but background checks are not typically made.

Table 2 1: Examples of electronic identities

Application	Identifier	Authentication strength	Device	Assurance (LoA)	Comment
EMV (chip and PIN)	Bank a/c no	Strong: PIN verified by chip card you have	Smart chip card	High	Banks are regulated by Know Your Customer (KYC). It is becoming harder to open bank accounts without significant background checks.
Smart meters	Meter number	Should be strong	Smart chip needed in meter	Should be high	Smart meters are only now emerging. The idea is to develop a smart-grid for machine-to-machine communications to rival the Internet. Smart meters will monitor consumption and relay this over a WAN to suppliers. Smart metering was encouraged by the EU Energy Services Directive in 2006. As a result, the UK, for example, plans to have them in all homes by 2020. [IET S_METER]
Physical Access Control System (PACS)	Staff number	Weak (no PIN typically)	Contactless smart card	High	Access to some areas might also require PIN entry, as well as contactless card. But the PIN might not be verified by the contactless card chip, so all terminals have to be online and PINs held centrally.
ICAO biometric e-Passport [ICAO MRTD]	Passport number	Very high. Photo for visual inspection and possible biometric verification (face and fingerprint)	Passport book with contactless smart chip	Very high (extensive background checks)	No PIN. Relies on visual inspection and finger biometric match for authentication. Government response to terrorism. Not designed for generic user-friendly transactions.
Federal smart ID (e.g. the US FIPS 201 Personal Identity Verification card) [NIST PIV]	Staff (card) number	Very high. PIN and fingerprint biometric	Smart chip card	Very high (extensive background checks)	Government response to terrorism. Not designed for generic user-friendly transactions.

3. Methods of management of multiple electronic identities

This chapter briefly describes the various efforts made to date to manage multiple electronic identities. Then the emerging issues are discussed and a small number of case studies are provided to illustrate the key issues.

3.1 A brief history of federation

A clear need for identification within online services has been recognised for some time. Furthermore, the desirability of using one form of electronic identity to access multiple services (RPs) is also clear. Federated Identity Management lets computer systems distribute identity information and tasks across security domains. It is the means by which users can be offered cross-domain single sign on (SSO), meaning that they can authenticate once and then gain access to protected resources in a variety of places, without being asked to re-authenticate.

This user convenience comes at a cost and identity systems need to provide appropriate protection against security concerns, such as:

- Can identity transactions be recorded and used on replay attacks?
- Is the level of user authentication (e.g. username and password) strong enough for all the services being accessed?
- Does the convenience of SSO create a single point of failure that is more easily exploited by attackers in order to access all of a user's resources?

Early attempts at providing identity services have tried to provide a single IDP acting as a *trusted third party* that could be used with all online services. Examples of this include Microsoft (MS) Passport in the private sector and Athens in the UK education and health sectors.

Reasons that MS Passport was not successful include:

- It provided a central repository for identity and all participating services were required to trust MS to hold the identity of and authenticate the users. This fails the 3rd Law: *Justifiable Parties*. [KC LAWS ID]
- The 1st Law: *User Control and Consent* was also not met since the control was not fine grained enough
- The underlying protocols were not all standards-based, leading to possible mistrust of the technical security

MS has now replaced Passport with Windows Live ID, which aims to be an identity meta-system [KC LAWS ID], providing support for Passport, CardSpace and OpenID.

Athens was the *de facto* standard for secure access management to online services for the UK education and health sectors. Originally, it was invented by a team at the University of Bath. Now it is owned, developed and operated by EduServ[20]. It essentially provides a database of user IDs and passwords and authorisation data (which services users can access). Each participating institution administers its own part of the identity database.

[20] www.eduserv.org.uk

Although Athens was successful in certain sectors in the UK, its success was limited for the following reasons:

- Its use of proprietary protocols made it unattractive for adoption by other countries
- The software is not open source
- Web sites cannot leverage Athens to set up their own federations of services

For these reasons, many countries are now moving to adopt Shibboleth/SAMLv2[21],which provides similar functionality while being standards based and using open source software.

Shibboleth[22] is a project run by a consortium in the USA, with over 350 academic and commercial partners called Internet2. Privacy protection is a key feature. User identifiers remain private to the IDP; users are identified using a transient identifier, which changes with each transaction. Authorisation is based upon identity attributes, rather than identifiers. An attribution release policy set by the user determines the release of attributes to RPs.

Over the past decade, it has become clear that hoping to provide a single digital ID panacea is not a sensible aim, due to the multitude of contexts within which such a system would need to work [KC LAWS ID]. Instead, the goal these days has become to provide a 'loosely coupled' digital identity that can work with whatever systems emerge over time, in the same way that the invention of device drivers allowed personal computers to work regardless of the latest display technology that they happened to have.

Liberty Alliance[23] and WS-Federation[24] are examples of specifications aimed at providing interoperable SSO. The expectation is that in general, each user will choose his/her IDP (or several IDPs) and therefore there is a multitude of decentralised IDPs that have to be handled and some discovery services are needed to cope with this.

More recently still, user-centric identity focusing on privacy issues has become a key feature of Federated ID Management [HOGBEN]. A number of identity frameworks are emerging that attempt to address those requirements of user-centric identity that were not fully addressed by the previous generation of frameworks.

It would not be appropriate in this study to examine each framework in detail. They are briefly described below:

- ***CardSpace (Info Cards):*** CardSpace is Microsoft's response to Cameron's Laws of Identity [KC LAWS ID]. It provides a user abstraction of assertion sets and assertion requests in the form of "information cards" and integrates this user interface with other existing identity management frameworks and components, such as WS-Federation, Liberty Alliance and OpenID.

  Microsoft's acquisition of Credentica[25] and its U-Prove electronic identity technology is significant when considering developments in electronic identity. U-Prove allows asserting parties to verify personal information with relying parties, without actually revealing information. Where information is revealed, it cannot be used for onward purposes without the asserting party's consent. Even where relying parties collude, there is no mechanism for them to undermine the asserting party's privacy.

  Microsoft is now integrating U-Prove into Windows and CardSpace, and as it becomes increasingly available on the desktop, it is likely that providers will exploit the toolkit and build commercial implementations

- ***OpenID:*** OpenID is primarily a single sign-on system for web site logins, providing only limited possibilities for the management of identity data. It is probably the most successful self-asserted cross-provider electronic identity scheme in use today. Created and managed by the open source community, the scheme provides a federated electronic identity for use across multiple relying parties, which trust assertions from OpenID, rather than requiring a relationship with the end user. This in turn allows users to access new participating services without having to register, or provide additional personal information each time they wish to do so. The precise information revealed to a new provider remains under the user's control

[21] SAML is an industry standard specified by OASIS that allows assertions about authentication, attributes and authorisation to be encoded in XML.

[22] http://shibboleth.internet2.edu/

[23] Liberty Alliance is a specification set aimed at providing interoperable online single sign on (SSO) and single logout, through a federated identity architecture. http://www.projectliberty.org/

[24] WS-Federation is another Identity Federation specification, developed by BEA Systems, BMC Software, CA, Inc., IBM, Layer 7 Technologies, Microsoft, Novell, and VeriSign. http://en.wikipedia.org/wiki/WS-Federation

[25] http://www.credentica.com/

OpenID claims to have over 1bn enabled user accounts and over 50,000 participating websites, and already has a substantial commitment from key Internet companies, including Google, Yahoo, Blogger, myspace, Wordpress, Flickr, Orange and AOL.

Government has yet to make widespread use of self-asserted ID. It is a concept that flies in the face of the traditional model of government being the 'most trusted' issuer of credentials. This may be about to change, as the US government is proposing to use OpenID as a citizen credential in 'low assurance,' low-trust scenarios (the evolution path to using IDs in a higher-trust scenario is as yet unclear). Plans are at a very early stage, and are being debated mainly between government security architects and technologists, but if they turn into an implementation, this will clearly have implications for the EU electronic identity landscape.

- ***Higgins:*** Higgins is an open source identity management framework co-ordinated by the Eclipse foundation[26]. It is designed to integrate identity, profile and social relationship information across multiple sites, applications and devices, and is designed to work with all popular protocols [PL OSI] including:

  - WS-Federation
  - WS-Trust
  - SAML
  - LDAP
  - MS CardSpace

Higgins is organised into three main areas:

- Higgins Selector, which focuses on a user's management of multiple digital identities
- Identity Services, providing tools, syntax and protocols for RP's and IdPs
- Higgins Identity Data Service which provides for interoperability and accessibility between different types of identity data

3.2 Discussion of issues

The increasingly digital nature of relationships between people is central to dealing with the issues of managing multiple identities. It is not a question simply of hardware or software, but more importantly of enabling people to enjoy and benefit from their online experiences, while dealing with potential issues. These issues might include a lack of knowledge or training, difficult personal circumstances or simply irritation at the diversity and unpredictability of online privacy and identity mechanisms. It is therefore vital that we should have strong, reliable mechanisms, which can be easily understood and relied upon across the course of a lifetime.

This is a very ambitious aim, but one that is potentially well supported by the range of technologies developing in this area. Privacy enhancing technologies have a major role to play. Equally, simple good sense, such as using appropriate strength of authentication and not keeping credentials beyond their useful lifespan, are important considerations. The adoption of open standards, with the flexibility this implies, also has a significant part to play.

There is considerable scope for policy to assist by supporting and protecting people in their online experience. Problematic activities such as spam, data mining and other identity-related attacks deserve close scrutiny. There are still questions to be resolved around the legal implications of ownership and also revocation of identities online. In such a fast-moving and interconnected area, it is likely that these and other issues will require the ongoing attention of policy makers in the coming years.

[26] http://www.eclipse.org/higgins/

The issues in this section have been divided into three categories, although in many cases there are significant areas of overlap:

- User - those most applicable at the user level
- Technical - those most applicable at the technical level
- Policy - those most applicable at the policy level

This categorisation has been chosen in order to form the basis for guidelines that will be developed in Chapter 5. It also has clear parallels with the layers described by frameworks such as NSTIC, which is based upon execution, management and governance layers, as described in Section 2.2.

3.2.1 User

3.2.1.1 User-centricity, privacy, inclusion

Digital identity management is an inescapably human discipline. Whether we are dealing with taxes or virtual worlds, the individual must always be at the heart of any process. When failures occur, it is commonplace for technologists to blame the user, leading to a cycle known as 'blame and train' [SAFEWARE]. Education is both admirable and important, but it cannot replace good design.

As digital communications mediate increasingly large areas of our lives, user-centricity is a principle that must be respected and cherished: 'The digital web of meaning has value to businesses only because it is about more than business. We are creating it not just as employees and customers, but as citizens, parents, lovers, artists… all of what we are.' [MISC]

A vital principle in achieving a successful system is to pay appropriate attention to privacy and consent. Any successful system must be based on high quality standards, which underpin predictable, standard 'ceremonies' [KC LAWS ID]. This at least provides a framework within which an individual can make informed choices regarding the disclosure of personally identifiable information.

The public is becoming increasingly better informed about the nature of the risks it runs when participating in online activities. This is supported by the efforts of information commissioners across the EU, as well as targeted education campaigns, often focused on financial fraud and child safety. While these are very important steps, it is still hard to predict the long-term implications of the current mass publication of personal data online. 'Human nature is such that we do not fear threats that we do not perceive.' [PERF] This is complicated still further by the much-publicised 'privacy paradox', whereby the level of concern professed by individuals for their own privacy is often not reflected in their actual behaviour patterns.

Whilst many are embracing the opportunities of the online world, others are rejecting it, leading to issues of inclusion: 'Dropouts are significant because their significance suggests that Internet diffusion may not reach full saturation levels due to certain inherent barriers that make it different from television, radio, and other household technologies.' [POL] It is unclear whether this rejection of online interaction is due to discomfort with the risks involved, financial reasons or other factors. Governments, both local and national, are increasingly pushing to deliver their services more cheaply online. This process would appear to have been hastened by the current economic crisis. With many of the recipients of these services being least well equipped, both educationally and in terms of their access to technology, to navigate the online world, this will present many challenges.

3.2.1.2 Proliferation of identities

In the early days of computing, we might have had access to a single standalone system. This had the advantage that the system was very much less vulnerable to attack than the highly networked systems that are now widespread. In those days, each of us probably only had to remember a single username and password.

In an increasingly networked world, most individuals hold a number of unconnected digital identities for a variety of purposes. In describing the 'patchwork of identity one-offs' which represents the online experience of many Internet users, Cameron details the shortcomings of the current arrangement:

'Hundreds of millions of people have been trained to accept anything any site wants to throw at them as being the "normal way" to conduct business online. They have been taught to type their names, secret passwords and personal identifying information into almost any input form that appears on their screen. There is no consistent and comprehensible framework allowing them to evaluate the authenticity of the sites they visit, and they don't have a reliable way of knowing when they are disclosing private information to illegitimate parties. At the same time, they lack a framework for controlling or even remembering the many different aspects of their digital existence.' [KC LAWS ID]

The ubiquity of weak authentication, recording passwords insecurely and using a single password across multiple accounts make this situation still more serious.

Federation, enabling a single ID to be used across multiple federated systems, is widely promoted as a way of limiting the total quantity of identity data that an individual is required to handle. This holds significant promise, so long as the surveillance risks of 'super-federation', where data is shared freely beyond the subject's control, are guarded against. Apart from convenience and security, effective identity policies can offer significant cost savings. Resetting passwords and enforcing policy requirements place substantial demands on helpdesk staff, at considerable expense. An important development in relation to user-centric identity is the widespread use of avatars in online worlds and gaming environments. In terms of privacy, they are very similar to other forms of digital identity. They do, however, present a number of unique issues, especially as they may give the owner a false sense of security in hiding behind an assumed persona, which may make them more likely to inadvertently 'leak' information. This vulnerability is already being targeted, with behavioural marketing, based on information gleaned from avatars becoming an increasingly prominent activity. [ENISA VW]

3.2.1.3 Lifecycle of a person

Our identity-related needs change throughout life. Our first and most formal engagement with the identity process is at birth, when we are registered and allocated a birth certificate. From then onwards, we will be subject to many different kinds of identification: medical, educational and later work-related records. We will also normally be associated with a number of social groups, which may require some kind of registration process.

All of these processes assume a certain level of capacity and consent from the person carrying out the registration. There will be times in our lives when we lack this capacity and the identity transactions will have to be delegated to a competent person. For children, this will be a parent or legal guardian. In adult life, there may at times be a similar need to delegate authority, such as when we find ourselves in poor health. [LIFELONG] The question of proxy identity management is an extremely complex and sensitive area in relation to digital inclusion, requiring that a person's abilities and wishes are respected at all times and individual tasks are delegated only when absolutely necessary.

Throughout our lives, increasing quantities of personal data about us accumulate in the public sphere and may still be accessed and used even after we die. It is therefore important for both individuals and authorities to be aware of the protection required to limit potential harm from over-exposure: 'Although we may initially be willing, over time we might seek to exercise greater control over the information that resides in databases. It is socially useful to have control over what others can know about us, because publicly available information may be inaccurate, partial, or decontextualised.' [POL]

3.2.1.4 Digital identity awareness

Beyond the issues of trust, privacy and consent discussed in 3.2.1.1, there are some basic concepts of which individuals should be aware in their handling of digital identity. An increasing move to empower the individual has led to initiatives such as VRM (Vendor Relationship Management [VRM]). This is in contrast to the traditional concept of CRM (Customer Relationship Management), with service providers of various kinds at its core. With VRM, an individual may maintain a repository of their own personal data, or have this maintained by a third party. The individual concerned may then choose with whom they share this data, on what basis and for what time period. Effectively, the vendor subscribes to the individual's data for as long as the individual wishes to maintain a relationship with that vendor. When the relationship is terminated, the vendor no longer has any rights to access the data.

ProjectVRM, launched by the Berkman Center for Internet and Society at Harvard University, explains the aims of VRM as follows: 'The primary theory behind ProjectVRM is that many market problems (including the widespread belief that customer lock-in is a "best practice") can only be solved from the customer side; by making the customer a fully-empowered actor in the marketplace, rather than one whose power in many cases is dependent on exclusive relationships with vendors, by coerced agreement provided entirely by those vendors.'[VRM]

The transition towards the VRM model may require some adjustment in people who have habitually been directed by service providers in the transaction process. In particular, it is a major departure from the traditional image of a wide-ranging government-issued eID. There would appear to be a tension between a utopian vision of a single universal source of identity for all purposes and the current collection of haphazard identities. In fact, it seems likely that, as in the real world, we will probably each hold a range of non-interchangeable identities for different purposes, such as a passport, car key, work log-in.

3.2.1.5 Anonymous transactions

Anonymity (see Section 2.1.1) has an important role to play in digital transactions. It can be used to support transactions where protection of the individual is essential (for example, a whistleblower). 'There are common and legitimate purposes for which casual anonymity is not sufficient. Investigators of many kinds, from academics, to reporters, to police, try to hide the patterns of their inquiries, even when they are consulting open sources. Many individuals value their privacy. For example, they wish to learn how to handle their illnesses without revealing their conditions to medical marketers or colleagues.' [PRIV]

When considering anonymity it is important to keep in mind that it is context dependent – according to the size of the group involved and the behaviours of each member of the group. Also, it is inevitable that relative anonymity will at best remain the same and at worst, decrease over time. [ANONYMITY]

Pseudonymity is also a valuable tool in providing increased protection in managing an online presence. Efforts to raise awareness around this option could significantly enhance the degree of privacy afforded to individuals. Such an approach may be discouraged by service providers wishing to have full visibility of customer details. It can, however, foster an increased level of security and atmosphere of trust in reputation-based systems.

3.2.2 Technology

3.2.2.1 Lifecycle of an identity

Some forms of identity records, such as birth certificates and medical records, are effectively retained for a lifetime. Others, such as access to school systems or a child's bus pass, have a clearly defined period of use; once a particular age or stage is attained, they are no longer applicable. Beyond these reasons for an identity becoming defunct, there are also practical reasons to limit the lifespan of many identities. These may relate as much to the nature of the identity as to the circumstances of the holder.

Each of us changes over time. Any identity that includes a record of our physical characteristics will need to be updated periodically. Photo IDs, such as passports, are a clear example of this. Similarly, over the course of a lifetime, biometric measurements will vary to some degree. It may be necessary to update records periodically in order to ensure effective matching. [BIO US]

Even identities that do not depend on temporary circumstances or physical characteristics still have a limited lifespan. 'A key has a cryptographic lifetime. It also has a theft lifetime, as a function of the vulnerability of the subsystem storing it, the rate of physical and network exposure, attractiveness of the key to an attacker, etc. From these, one can compute the probability of loss of key as a function of time and usage.'[PKI]

It is to be expected that throughout the course of a person's life they will hold multiple identities, each with a different purpose and a different renewal schedule. There may be reason to combine elements from one or more, for example when purchasing car insurance, to prove qualification, age and the number of years since a claim was last made. In the same way, digital identities are likely to be complementary, running in parallel, with each being renewed to a schedule appropriate to its purpose and composition.

Although it is impossible to guarantee absolute life-long security for elements of a person's identity, it is essential that the greatest possible care is taken in putting appropriate protection in place. The longer the lifespan of the identity concerned, the greater the challenges involved: 'In the United States, census data, income tax returns, medical records, and other personal information are supposed to be kept secret for a lifetime.'[PRIV]

3.2.2.2 Open standards, Open interfaces

As systems become increasingly complex, effective processing of both data and metadata are ever more important. While the handling of data is a reasonably mature discipline, best practice for handling metadata is less widely implemented. For reasons of efficiency as well as privacy, metadata is a key consideration. In a standalone system, the management of metadata is relatively simple. However, in federated systems, considerable complexity surrounds both the technical and semantic handling of metadata.

High quality interoperability between systems is an essential requirement for successful federated identity management. It is required in order to ensure that one system can interact with another and effectively verify identity claims. Open standards such as those promoted by the Liberty Alliance, provide a means for organisations to implement such federated systems with reasonable confidence that they will be able to work effectively with other such systems.

Although this is the initial aim of the federation, in order to protect user privacy it is also necessary to ensure that policies agreed with the initial identity provider are respected by subsequent recipients of any identity data. This requirement may be underpinned by both technical and governance measures: 'In the data handling preferences associated to a piece of PII, the data subject specifies its requirements on how it expects her data to be treated by the data controller. The data controller, before receiving the PII, describes his intentions on how he will treat the PII in his data handling policy. When an agreement is reached, the agreed-upon policy that the data controller has to adhere to is referred to as the sticky policy.'[POLICIES]

Syntactical interoperability at the level of metadata is still somewhat problematic and until this situation is resolved, the level of privacy protection afforded by federated systems may be unpredictable. If the initial agreement between the user and the original system is not effectively understood by subsequent systems, then it is unlikely that the associated obligations will be respected by those secondary systems. It is for this reason that standard processes around the expectations embodied in the metadata are so important.[PL OSI]

The need for interoperability between systems is paralleled by the need for flexibility within systems. The OSI seven layer network model demonstrates this very well. By breaking a system down into layers that need only interact with the open interfaces above or below them in the stack, a modular approach can be achieved. This circumvents the dangers of monolithic, closed systems thatimpede progress. A key benefit of the modular approach including open interfaces is that it can enable progressive and even experimental approaches to be taken to specific parts of the system, without undermining the integrity of the system as a whole. Commercially it is also a valuable addition to the landscape through its fostering of competition in provision of services.

3.2.2.3 Devices, portability, security of credentials

Digital identities cannot simply exist in the ether. For an identity transaction to take place, the subject (whether a person or non-person entity (NPE)) requires some kind of platform from which to initiate the transaction. This may be a smart card, a mobile phone, PC, fingerprint reader or some other kind of device. Even in widely federated web-based systems, the initiation of an identity transaction will normally be triggered as the result of the action of an individual on a device, which is attached to the web. This may be something as simple as entering a username and password into a PC to log into a webmail account.

The US National Strategy for Trusted Identities in Cyberspace draft document [NSTIC] places strong emphasis on the use of secure protocols, including BGPSEC, DNSSEC and IPSEC to support the integrity of the identity infrastructure. These protocols are only meaningful if implemented on an appropriately secure platform. Trusted Computing has been widely promoted as a means of building security into a system. Although it may not have achieved the widespread popularity that was originally envisaged, it is clear that any systems supporting identity transactions must include sufficient security measures to afford the identity data reasonable protection. The end-to-end authentication that secure protocols can provide on appropriate hardware is a key contributor towards securing the identity infrastructure.

In order to offer a high level of choice, flexibility and convenience, portability of digital identities is also an important priority. I may choose to hold particular credentials on my mobile phone, with others held on a smart card. To support a user-centric view of identity, it is essential that the user can choose both the ways in which they present themselves and the type of device on which their data is held.

The increasing prevalence of phishing and pharming serve to underline the need to ensure that credentials are stored on devices capable of securing them and are handled appropriately on those devices. The current scandal surrounding eavesdropping on public figures by the News of the World newspaper in the UK provides a powerful example of the risks, both financial and reputational, of inadequately securing personal communications.

3.2.2.4 Unlinkability

Unlinkability is one of the key requirements of truly privacy-enhancing identity systems. Traditionally, systems have involved a single identifier with a wide range of associated identity data. Repeated use of this identifier with associated credentials can gradually enable both the identity provider and relying parties to build up an increasingly detailed picture of the individual's activities.

This situation leaves the individual more vulnerable to disclosure of their private information, as well as potential compromise of their credentials. Cryptographically, it is possible to separate out transactions so that the credentials used by a particular person in dealings with one relying party can not be recognised as belonging to the same individual as those used in their dealings with another relying party. For example, I have no desire for my bank to know anything about my medical data. Equally, I can see no good reason for the local hospital to have access to my financial data. By using a system that supports unlinkability, such as the IBM Zurich IdeMix, I can be confident that although I control both areas of my identity, there is no means for the relying parties to make associations between the two.

In matters where the data is held and controlled within a particular system, the mechanisms are available to control the linkability of data. However, geographic data presents a still greater challenge. 'Location-based services are becoming ubiquitous, fuelled by the proliferation of mobile devices, notably smart phones…Despite the popularity of these services, privacy issues such as the undesired leakage of users' location information to location-based service operators, or to external eavesdroppers is a major concern.' [FRAME LOC]

Although the Directive 2002/58/EC makes specific legal provision for location data in order to protect the privacy of the device holder, this is by no means universally respected: 'Recent studies have analyzed the human behaviour and daily routines using real-life data collected with mobile phones. This analysis shows that wireless communication can be easily used to track people and create patterns of human behaviour regarding their physical location or their social activities.'[MOBILE IDM]

This is another area in which a combination of user awareness, appropriate technological intervention and legal regulation are essential to deal with the complex social and commercial issues involved.

3.2.2.5 Dynamic management of partial identities

It appears desirable to use partial identities [FIDIS, PICOS], in order to protect privacy by respecting the principle of minimal disclosure. The most flexible approach to this, which is promoted by Higgins, would be to be able to select attributes from a subject's full collection of identities. They could then be combined according to the requirements of a particular situation. For example, a bar tender needs to know whether the person they are serving is both old enough to buy a drink and also has the means to pay for it. By combining these two attributes from two different identities, it is possible to complete the transaction conveniently and still retain a high level of privacy.

Although MS CardSpace gives the individual the capability to select from their Identity Selector which InfoCard (identity) they wish to use for a particular transaction, it does not yet offer the means to dynamically combine attributes from multiple identities, as described above. [CHADWICK]

Some very interesting work has been done by the PrimeLife project, looking into the requirements for partial profiles in the social networking environment. For example, a subject may wish to display a professional profile to one group, while maintaining anonymity, or displaying details of their hobbies, friends and family to another group. They describe a number of different scenarios in depth and suggest practical means for achieving them. [PLIFE SNS]

3.2.2.6 Inflexibility of systems

A number of important capabilities are not yet readily available in the existing frameworks described in Section 3.1. For instance, the resource description framework (RDF) language, commonly used across the semantic web, includes a concept known as a 'blank node', which can be useful for complex, nested relationships, such as if a subject is related to a child, who has some kind of domestic pet. This may be inferred from the subject being a parent of a person aged nine, who has a rabbit. Unfortunately, this type of inference and semantic matching are not currently well handled in identity systems, leading to limitations in their effectiveness, both from the inability to reach more complex conclusions and to recognise the risks of such conclusions being reached inappropriately from inferences drawn by linking various data items. [HOGBEN]

A similar area of inflexibility relates to the quality of assertions. The existing frameworks effectively lack the flexibility to express arbitrary assertions beyond simple binary relationships such as 'first name = Adam'. The ability to use richer assertions describing more complex attributes would significantly enhance such systems.

There are also considerable risks and operational overheads associated with tying the identity layer too closely to the data layer. This greatly decreases the flexibility possible in managing identity and increases the intervention required in the data layer to enable the identity processes to work effectively. An essential element in achieving a really successful identity implementation is to include the capability for anonymous bindings. These simply link data and metadata without specifying details of the data that the metadata describes. For example, if I know that metadata x,y,z refers to field 12, this provides a much greater degree of privacy than knowing that metadata x,y,z refers to named field 'regular blood tests'. [HOGBEN]

3.2.2.7 Spam

Certain kinds of anti-social behaviour, such as spam (the indiscriminate sending of large amounts of unsolicited e-mail) rely on the use of multiple identities. If I receive an unacceptable message, I can block the address from which it was sent. The sender then creates any number of new addresses (a rapid and easily automated process) from which to send further unwanted mail. Equally, they may use address spoofing (impersonating a legitimate user) to give the impression that their mail is coming from a respectable source.

An interesting development of the traditional spam model, is the increasing number of bots (scripted avatars) present in online worlds. These may be used to push unsolicited marketing, as well as offering services or products that are banned by the service provider. [ENISA VW]

3.2.2.8 Data mining

Individuals can also be vulnerable as a result of the proliferation of identities discussed in Section 3.2.1.2. Any organisation that holds identity data may potentially subject it to data mining. This wholesale processing of data can compromise an individual's privacy in significant and unexpected ways. This may occur when a company holding our data is purchased by another company, which may not respect our original agreement. Indeed, a company's mailing list is often considered to be its most valuable asset and therefore vulnerable to this type of activity.

3.2.3 Policy

3.2.3.1 Ownership

With an increasing emphasis on user-centricity, rather than a person's identity data being held in excessive quantities, in fragmented data stores, across multiple systems, initiatives such as VRM [VRM] aim to return control of the data to the subject (see Section 3.2.1.4). The subject can then choose which elements of their data to share, for what purpose and which associated terms and conditions they are prepared to accept. This is an important contribution because, although in principle many of an individual's rights are already protected, in practice enforcement is not easily achieved across multiple distributed systems.

Another initiative, which aims to return power to the subject in the identity transaction, is the Internet of Subjects organisation. In recent years there has been widespread discussion of an Internet of Objects, where sensors and appliances make up a widely connected network of non-human participants. Some have expressed concern over the privacy and surveillance implications of such a scenario. The Internet of Subjects highlights the importance of people in the future of the Internet and has produced a manifesto aimed at enabling individuals to control their own data: 'Our goal is to create the conditions for the emergence and sustainability of a person-centric Internet, an Internet of Subjects, where individuals in full control over the storage, transport and exploitation of their personal data, can monitor their use by other individuals, networks, communities, businesses and authorities. Our aim is to enforce privacy and trust, while enabling business and innovation.'[IOS]

The vision of the Internet of Subjects Foundation depends on each subject maintaining a personal data store (PDS). This may be something that they manage themselves, or contract out to a third party provider. The purpose of maintaining the PDS is to control the amount of data that is shared and the terms associated with that sharing.

An extension of this question of control and ownership relates to the use of avatars in Massively-Multiplayer Online Games (MMO) and virtual worlds (VW): 'Ownership of avatar names and identities is also problematic, giving rise to issues of trade marks, misleading and deceptive conduct, as well as issues of publicity rights. In Second Life (and other civic or social worlds) the choice of avatar name may be restricted, either due to guild or social status or because of a finite list of names. It is not clear if the creator owns the rights in their avatar name, particularly if they want to exploit that name outside the originating MMO/VW.'[ENISA VW]

If a truly user-centric identity ecosystem is to be achieved, greater attention will need to be paid to these issues of ownership. A first step would be wider education of the user population, so that they can fully understand their rights and options. Equally, regulation and clearer paths to enforcement may have a part to play.

3.2.3.2 Trust

Trust is a central issue in all identity transactions, as described in Section 2. The subject must be confident that their personal information will be handled appropriately, in order to take part in the transaction. Equally, the relying party must be confident that the subject's obligations under the transaction (such as payment) will be honoured. In order for the relying party to have this confidence, they will need the means to assess the trustworthiness of the assertion being provided in that particular context. Metadata relating to that assertion would be helpful in assessing its quality. However, at present there is no reliable mechanism underlying this process. [HOGBEN]

Clearly this is much more than simply a technical issue. Trust is a complex and multi-faceted part of a relationship, which varies from one context to another and changes rapidly over time. Although a relying party may have little reason to trust the assertion provided by the subject, they will have significantly more reason to trust an identity provider. This will be enhanced if the relying party already has a relationship with the identity provider and has the assurance of knowing their quality processes. [CHADWICK]

Another crucial element of trust is having confidence that any anomalies will be recognised and dealt with effectively. 'The framework should provide data structures which facilitate efficient audit and enforcement of data processing events'. [HOGBEN] This apparently simple requirement, without which the integrity of the system is severely compromised, is unfortunately not sufficiently widely implemented across current frameworks.

3.2.3.3 Revocation

The usual lifecycle of an identity will involve enrolment, active use, and at the end of the identity's useful life, revocation. The aim of the system is undermined if enrolment or active use fail. However, if revocation fails, the system can still continue processing identity transactions perfectly effectively. For this reason, it is rarely a priority for those managing such systems.

In terms of data handling, having a system littered with defunct identity data, which may even be duplicated several times over, can become problematic. It may be unclear which record relates to a particular subject and their current data. Indeed, the quantity of excess data may even lead to an increase in transaction processing times. Failure of revocation also increases the potential for systems to be compromised. Just because a person ceased to use their access credentials many years ago does not mean that those credentials ceased to be viable. Without specific intervention, they will continue to allow access to the associated resources.

Due to the proliferation of identities described in Section 3.2.1.2, a person may be associated with a considerable number of identities that are no longer required or active, but may not have been revoked. Apart from the threat to the associated systems, this can also imply a substantial privacy risk. Personal data may still be held by these parties, without our being able to carry out effective checks.

The issues surrounding revocation have been looked at in detail by the EnCoRe privacy research project. Their findings would seem to imply that there are legal issues, as well as the more obvious administrative and technical ones, surrounding revocation:

'The E-Privacy Directive addresses particular concerns brought about by the surge in the use of electronic communications to deal with personal data; however it alone does not provide an adequate 'revocation solution', conferring as it does only limited rights on individuals to prevent types of processing by withdrawing consent to such processing. The apparent danger that the legislation may deny data subjects a right to self-control over their personal data is concerning…we believe that individuals should be better informed, facilitated by technology if possible, as to the expectations of how their data should, and should not, be used in different contexts, coupled with more robust methods to take action when the processing of data is not acceptable to them. Currently, individuals are not provided with workable rights to take such action.' [ENCORE]

Where the identity data involves the use of highly personal and irreplaceable, if public, features, such as biometrics, some kind of revocability is essential. It is commonly stated, and clearly true, that a person cannot request a new set of fingerprints. However, by the use of abstractions such as templates, biometrics may still be used with sufficient revocability. The EU-funded TURBINE[27] project is doing work in this area, looking at unlinkability and revocation of biometrics, strongly supported by advanced cryptography.

3.2.3.4 Attacks – whitewashing, sybil attack, DDOS

There are a number of attacks that are only possible through the use of multiple identities. Regulation of the ways in which identities are issued and rules for their subsequent use may make a substantial contribution to the management of these attacks. Two that we will explore initially relate to manipulation of ratings in reputation-based systems: Whitewashing describes a situation where a user creates a new identity in order to achieve a clean slate after previously having earned a poor reputation in a particular environment. Regulation of such practices needs to balance the desirability of welcoming new users to the environment, with the need to maintain integrity within the system. Although in principle tracking of external factors may provide indicators of whitewashing, this level of surveillance may also be undesirable. In some ways, whitewashing may be compared to the concept of 'reputation bankruptcy' that is gaining currency. An important distinction is that reputation bankruptcy is an open recognition of reputational difficulties, with a clear and overt mechanism for dealing with them. Whitewashing, on the other hand, is intended to subvert the system when an existing reputation falls below a tolerable level.

[27] http://www.turbine-project.eu/

The sybil attack, also referred to as 'pseudospoofing' involves the creation of multiple identities (sybils) in order to distort ratings within a reputation-based system. This can be used to achieve a high star rating across a large number of very low value transactions, where those transactions have in fact taken place between two identities owned by the same individual. For the protection of other users and for the credibility of reputation-based systems, appropriate regulations to highlight and control this type of behaviour are essential.

The use of avatars gives rise to another form of attack, which depends on possession of multiple identities. Because avatars take up a certain amount of 'space' in virtual worlds, there is potential for them to take apparently 'physical' action: 'In Second life it is possible to push another character and prevent them from performing actions in the world. For example, avatar A might push avatar B off the stage during a public performance.' [ENISA VW] If multiple avatars choose to block a space, or create objects to block a space, this can produce the equivalent of a distributed denial of service attack (DDOS). Historically, access control for virtual worlds has tended to be centralised and weakly authenticated. With the growing emergence of ever more sophisticated attacks, and the large amounts of money involved in online gaming, the level of regulation and also authentication is beginning to improve.

3.3 Case studies

3.3.1 Introduction

This section includes three case studies, developed to illustrate the issues described in Chapter 4 of this report. Collectively, the case studies make reference to all of the issues identified. The following table relates specific issues to their coverage in each individual case study. It also shows which of the 7 Laws of Identity [KC LAWS ID] apply to each of the issues.

The case studies each take a day-in-the-life approach to illustrating the issues and some known approaches to dealing with the problems encountered. The table below shows, for each of the three case studies, which issues are touched upon.

Section	Issue	Laws [KC LAWS ID]	Social networking	Travel	Recovery
3.2.1.1	User-centricity, privacy, inclusion	1, 2, 3, 6	x	x	x
3.2.1.2	Proliferation of identities	2, 7	x	x	
3.2.1.3	Lifecycle of a person	1, 2, 3, 6			x
3.2.1.4	Digital identity awareness	1, 4, 5, 6	x	x	x
3.2.1.5	Anonymity	1, 2, 3, 4	x	x	
3.2.2.1	Lifecycle of an identity	2, 3, 4	x		x
3.2.2.2	Open standards, pen interfaces	5, 7	x	x	
3.2.2.3	Devices, portability, security of credentials	1, 2, 3, 5, 6, 7	x	x	
3.2.2.4	Unlinkability	1, 2, 3, 4	x	x	
3.2.2.5	Dynamic management of partial identities	1, 2, 3, 4	x		
3.2.2.6	Inflexibility of systems	1, 4	x		x
3.2.2.7	Spam	2, 3	x		
3.2.2.8	Data mining	1, 2, 3	x		
3.2.3.1	Ownership	1, 2, 3, 5, 6, 7	x		x
3.2.3.2	Trust	1, 2, 3			x
3.2.3.3	Revocation	1, 2, 3, 5		x	x
3.2.3.4	Attacks – whitewashing, sybil attack, DDOS	1, 2, 3	x		

Table 3 1: Summary of case studies

3.3.2 Social networking sites

Sarah is a journalist who likes to use social media in both her work and her personal life. In her early days online, she felt apprehensive about the large number of different services available on the Internet. Initially, she struggled to manage all her different accounts, using sticky notes and subsequently a notebook to store her details. She found this unwieldy and inconvenient. Consequently, she now uses a single password aggregation tool created specifically for this purpose, protected with strong cryptography and a complex pass phrase. She feels reassured that this is both more convenient and more secure.

Having been online for several years now, she has settled into a pattern of using particular services with which she feels comfortable. She has become familiar with the features of each, both positive and negative, and uses them in combination to support her lifestyle. She makes every effort to protect herself, by reading user agreements and privacy policies before downloading files from the Internet or disclosing any personal information online. She also looks for opportunities to express her personal preferences, such as check boxes to accept/refuse further contact with an organisation or its affiliates. From a technical perspective, Sarah has standard, sensible measures in place: she only accepts cookies from sites that she has permitted; she regularly clears her browser history and deletes temporary internet files and cookies. She also regularly checks for spyware on her computer and has current anti-virus and firewall protection. While she has a spam filter on her e-mail, she is also careful not to open suspicious looking mails. She knows that technical protection is helpful but awareness is also essential to staying safe online.

Sarah is aware that it may be possible to use a single ID, such as her Facebook ID, for accessing other services. She would like the convenience of using one of her existing IDs for accessing a range of different services, but remains unconvinced. She will want to have reassurance that the identities are truly interoperable and respect the policies contained in her original privacy settings. These 'sticky policies' should be transferable in full force from one system to another. She would also like the power to control and maintain her own identity, rather than ceding ownership to a third party, without clear means of restitution if it is abused. This is some distance from the capabilities of current implementations, but it is essential for her to maintain the separation between her very public work life and the privacy of her home life. She does not want to share her family photographs with the general public, or her more obscure projects with her friends. Recently, she has received notifications from friends, who have chosen to link their IDs online. Some have subsequently sent apologies for the associated mass mailings, but in several cases it was a useful update.

Sarah has long been a subscriber to Linkedin, to support her professional networking. Having received a number of commissions for freelance work via business contacts, she soon became aware of the value of an extensive and high quality network. Still, she would never go as far as her editor; he maintains a network of 10,000 people, most of whom he has never even met. For a link to be worth anything to her, it must be a "real" link. She does not want to be bombarded with speculative e-mails from virtual strangers. With this in mind, she is sparing in her use of unsolicited introductions in making contact with others on the network. Where Sarah's use of Linkedin is clear-cut and purely for professional purposes, her use of Facebook is much more complex. She has discovered a wealth of groups relating to a huge range of different interests, such as music, cooking, activism and health. She even found that there was a group for the Parent Teacher Association at her son's school. As a result, she has been able to get more involved in fund-raising activities, despite the irregular hours that her work sometimes requires. Beyond a greater sense of social connection, a further benefit from spending time on Facebook is that it has become the first port of call for journalists researching human interest stories of all kinds.

Sarah is aware that there have been privacy issues on Facebook in the past and she is meticulous about managing her own security settings. She is intent on controlling exactly who has access to her information. She uses an ID that is known only to her family and friends and is not easily connected with the IDs which she uses elsewhere online. She also makes sure that she uses long, complex, unpredictable passwords, which are different for each ID she has and changes them regularly. However, when researching stories, she has noticed that many people appear to show no regard for their own privacy. They expose not only their own details, but also photographs and comments relating to their friends and family. Once this information is in the public domain, it is irretrievable. Even within the SNS it is very hard to have the relevant information permanently removed, especially if it has been copied in several different locations. At its most devastating, this has resulted in grieving relatives seeing intimate family details published in the national press, with no respect for their personal tragedy.

For professional reasons, Sarah is also active on Twitter. She is required to update her Twitter feed on a regular basis in order to publicise her column in a national newspaper. This enhances her visibility and also gives her the opportunity to develop a closer relationship with her readers. She is also subscribed to a number of twitter feeds, in order to keep up with areas of both professional and personal interest. She likes the easy accessibility and brief format of the messages, which enable her to keep informed without too much exertion. Her ID is simply an aggregation of her name and the newspaper name, so this is a purely professional ID, which gives away very little on a personal level.

Sarah is aware that additional services are available via social networking sites, such as multiplayer games and geographical services. Although she is not particularly drawn to the games, the geographical services could be very convenient in getting together with friends and colleagues. She also rather likes the idea of knowing where her son is if he's out with friends, or late home from school. Realistically, she knows that this kind of tracking would be a breach of trust, so she does not intend to pursue it. For herself, as a woman who often travels alone and sometimes covers controversial stories, she is concerned that enabling geographical services could make her more vulnerable to unwanted attention.

Sarah is still interested in investigating the options for using her online identities to sign into different sites across the web. She has found information showing that Facebook is the most frequently used ID for accessing sites, especially those which offer entertainment, where they make up 52% of the social network IDs used to gain access [GIGYA]. For news sites, Twitter is dominant, although across online access MySpace, Yahoo, Google, AOL and Linkedin also play a part. Apart from concerns about links being forged between her identities, there are also circumstances under which Sarah wishes to maintain a reasonable degree of anonymity. Particularly when carrying out research, it is important for the integrity of her story that she should not actively divulge her identity. At present, Sarah is not confident that the convenience provided by linking online identities merits the current risks associated with it. When she does decide to take a further step in this direction, she will probably still want to maintain a number of different IDs for a range of purposes (such as blogging, banking, government transactions), but fewer than she has now. Until the responsibilities of the major providers are enforced by something stronger than negative publicity, Sarah would prefer not to put all her eggs in one basket.

3.3.3 Recovery following compromise of identity data

Every news programme on the television today has urged Maria to 'get online'. The programme launches with a report on the grave dangers of cyber crime, covers a few general interest stories and ends with exhortations to join the digital revolution. The government-sponsored campaign encourages her to buy her shopping, pay her taxes and check train times online, as well as keeping up with friends and family. Unconvinced, she is having second thoughts about the whole online experience.

Late last year, Maria's home was broken into and her laptop computer stolen. Maria had been very shaken and immediately reported the crime to the police. She was given a crime reference number for insurance purposes and advised that the police did not have the capability to locate the burglar by IP address or ISP. Under normal circumstances, this would have been the end of the investigation. All the rather prescriptive advice she had received regarding staying safe online gave no pointers as to how to handle a situation such as this. It appeared that once things had gone wrong, she was effectively left to recover alone, as best she could.

Although the laptop was password protected, the password was weak and so easily guessed. The browser had all her usernames and passwords saved so that when the thief connected to MyFace[28], it logged in automatically in her name. He then took the opportunity to make several public posts to MyFace, boasting about his thefts, but under her name. Maria was unable to access her account and contacted MyFace with a view to reinstating her own access. Their response was that the account was blocked due to a breach of security.

[28] MyFace is fictional and represents a generic social networking site in this case study.

Fortunately, although access details for several other accounts were stored in the browser (Twitter, LinkedIn, Gmail, Banking), Maria had managed to change the related passwords in time to prevent the thief from using those accounts. This may indicate that he is a MyFace user himself but was unaware of the existence of her other accounts. In order to regain access, she was required to send MyFace an e-mail from a registered e-mail address. She sent a mail from her usual e-mail address, but was still refused access. Because her e-mail address with Popularmail[29] had been switched over to Pmail (which both actually work synonymously) without her knowledge, the MyFace systems would not recognise it and she continued to be refused access. It was not until several months later that she understood how this misunderstanding between systems had arisen.

Eventually, she decided not to persevere with MyFace and simply gave up using it. After a few months, she started to receive frequent e-mails from MyFace, noting that she hadn't visited recently. One contained a link to click in order to log in. She clicked the link and was logged in immediately. It appeared that they had set up a new account for her without asking her permission and had deleted all the posts about the burglary. All her connections to her friends were lost but all the older posts were still present. By this time her trust in MyFace and their processes was severely eroded: they had failed to grant her access when she had reasonably requested it after she had been robbed. Now that she had been out of contact for some time, they seemed to be lowering their barriers in order to entice her back in.

Meanwhile, Maria's husband had discovered both her handbag and the gloves that the burglar had been wearing, discarded in a hedge. This enabled the police to identify the criminal, via an existing entry in the national DNA database and recover Maria's laptop. Although this was a positive step, it was a further year until the police were prepared to release the laptop, on the basis that it was hard to remove the results of the burglar's activities.

When the case finally came to trial, Maria had the opportunity to make a statement regarding the level of distress caused to her, so that it could be used to impact the level of sentencing. However, Maria chose not to make a statement for fear of recriminations against herself or her family. Finally, the police mentioned the names of the criminals concerned to Maria's husband, who subsequently looked them up on MyFace, only to discover that he had passed them in the street.

Maria has recently been in contact with her nephew, David, who has himself experienced a very different kind of online security breach. He is an enthusiastic player of the Massively Multiplayer Online Role-Playing Game (MMORPG), World of Warcraft (WoW). This is a very compulsive game, providing a succession of challenges with the opportunity to achieve incremental rewards. It is internationally popular, with a large user population. David has one main character in the game, who is a member of a guild (an organisation that enables characters to work together to accumulate wealth and achieve their aims), as well as several lesser characters. Within the game, value is measured in gold and assets can be sold at auction in order to accumulate more gold. Assets may include ore, which has been mined, or craft items produced by members of the guild. Raiding and fighting are also intrinsic parts of the game.

Because the game is so popular, WoW gold has real value beyond the game and can be purchased by credit and debit card via external gold-buying websites. Indeed, some individuals are paid to accumulate goods on WoW, sell them at the WoW auction house and then sell the WoW dollars on for real-world currency. Unfortunately, this real-world value for WoW dollars has led to widespread hacking. David experienced this himself when a hacker guessed his password. When he logged on, his characters had disappeared. In their place, someone had created low level characters on every single realm, in major cities, promoting an external gold-buying website. Not only had they taken all his goods and sold them on, they had also used his credentials to hack the guild bank. This was a source of considerable embarrassment to David, who, after apologising to his guild master, set about resolving the situation. Luckily the hackers had not changed his password, so Blizzard, who manage the game, were happy to restore David's account and the goods associated with both his account and the guild. Their privacy policy means that they are unable to search individuals' accounts, so they were unable to trace the goods, but everything was restored.

[29] Popularmail is fictional and represents a generic free email service commonly used across the globe.

In response to this kind of hacking, which involves repeated guessing of an individual's password until access is gained (brute force attack), WoW has now introduced two-factor authentication. This requires that, rather than simply entering a username and password, a user has to enter their username followed by a password and then a code from their authenticator. This authenticator is a small application, which can run on a mobile phone and produces unpredictable codes that change at regular intervals. This greatly increases the difficulty of hacking an account of this kind. As a result, David is very pleased with his authenticator, confident that his gold (and that of his guild) is safe and feels that his trust in WoW is justified.

3.3.4 ID implications of travel

Thomas is a bright, well-connected young man with an enthusiasm for technology. He is registered disabled and therefore benefits from a free bus pass, as well as a disabled person's railcard. He has recently seen a film on television, entitled 'Erasing David', which highlights the increasing levels of surveillance in his country. He is planning to travel from his home in the north to visit friends in the south-west. While planning his journey, he has decided to experiment by aiming to limit the information he discloses about himself as much as possible, while taking into account the cost and convenience of different modes of transport.

He would like to be able to cover the entire distance on foot without any need at all for identification, as his favourite celebrity has recently done. Sadly, due to limitations of stamina and time, this is not practical. He has read a book about pensioners travelling the length of the country using their free bus passes. His bus pass is a simple flash card, so although it identifies him in a limited way to the bus driver, it would not result in any information being stored about his journey. Nevertheless, using local buses would make the journey very long and unpredictable. He is also aware that his local council is in the process of trialling contactless technologies, including smart cards and mobile phones using NFC (Near Field Communications), on local bus routes. Soon his flash card will be replaced with a smart card, which will enable him to have his credentials (rather than his identity, since there will be no cardholder authentication) authenticated electronically and open up the possibility of tracking his travel patterns more closely. He likes the idea of a card that can offer a range of interoperable services, but he is concerned that the resulting records may be linked to produce a detailed picture of his lifestyle. In any case, the bus is not convenient for the journey he is currently planning.

Due to his disability, Thomas needs to be sure that he will have a seat on the train and must therefore book in advance. This requires him to book either online, or by telephone, as it is not practical for him to travel to the station simply to buy tickets. Both online and telephone bookings automatically provide a means of tracing the source of his transaction, either by his IP address via his ISP, or by the contact telephone number that the call centre requests from him. When he comes to pay for his ticket, he is required to provide credit or debit card details. Although in principle these are pseudonymous, in practice they are likely to provide further clues to his identity. It is common for the service provider to want to check the address at which the card is registered, prior to completing a remote transaction of this kind.

If he is to receive a discounted ticket, Thomas must also declare that he has a disabled person's railcard. This does not assist in identifying him, but does highlight his personal circumstances. Once he has completed the transaction to purchase his ticket, he may choose to collect the ticket from a self-service machine at the station prior to departure (for which his payment card is required along with a transaction reference number provided at the time of booking to prove that he has the right to receive the ticket). Otherwise, he may choose to have the tickets sent to him by post, which will of course entail confirming his name and address.

Alternatively, Thomas might choose to hire a car in order to drive to his friends' house. The car-hire company will require him to present his driver's licence as photo ID. The hire firm requires that he should be at least 23 years old, so proof of age is a further requirement. Although he may make payment using cash or a debit card, he is required to present a credit card, in order to cover the cost of any unforeseen extra charges he may incur.

Thomas is alarmed at the high quality (validated) identity documentation that is required to hire a car. This effectively provides the hire company with a large amount of information that is irrelevant to the business of hiring the car. In practice, they only really need to know that he has a valid licence, is of sufficient age and has the means to pay. Unfortunately, the current state of identity documentation leaves them with few other options than to request the kind of formal documentation that provides this assurance. In time, it would be desirable to find a way of providing the same kind of assurance, while disclosing much less personal information.

Beyond the information that the car hire firm collects, Thomas would be traceable while driving via the number plate on his car. This is used to manage penalty notices for driving offences, as well as providing a means of tracing vehicles that are subject to congestion charging in specific urban areas. It may also be subject to automatic number plate recognition (ANPR) in areas where police checks are undertaken. Modern road cameras can measure the speed of a vehicle, record the number plate, the driver and passengers in the vehicle and whether they are wearing seat belts.

In principle, it would be possible for Thomas to take an internal flight from an airport close to his home, to the city where his friends live. However, the identity requirements for this are also onerous in that passengers must provide photographic ID. He has heard that once his local council starts to issue smart cards, these too will be acceptable as photographic identity for domestic flights. This is due largely to comprehensive auditing of the issuance process, which verifies that the person requesting the card is genuinely the person named and pictured on the card.

Having considered all his options, Thomas decides that he would prefer to travel by train. He books online, choosing to collect his ticket at the station on departure. When he reaches the city where his friends live, he will be able to use a local contactless travel card on the underground network and buses. His friends are always encouraging him to register his card by providing his name and contact details, so that if he loses it he can reclaim the balance of money remaining on the card. It would also provide him with the convenience of being able to top up the balance on his card, without having to physically take the card to a kiosk. He has considered it, but he visits infrequently and rarely has more than a few Euros on the card, so he does not really see the point. In any case, he likes a little anonymity.

4. Guidelines and best practice

This section provides guidelines and best practice in the management of multiple eIDs aimed at three different target audiences:

1. End user.
2. Technical, such as system designers and implementers.
3. Policy makers, such as the EC and governments.

These guidelines were developed by considering each of the issues described in Chapter 4 in relation to the potential for each group of stakeholders, listed above, to contribute to achieving a resolution. In many cases, a single issue has resulted in multiple guidelines, each with a specific aim. The guidelines have been grouped according to potential for User (U), Technical (T), or Policy (P) intervention, on the understanding that these categories will naturally overlap.

The table below summarises the guidelines and shows how they relate to each issue raised in Chapter 4. The guidelines and best practices are then expanded and discussed in the remainder of this chapter, labelled as 'GL' and 'BP' respectively.

The guidelines in parts 4.2-4.4 have been prioritized according to their importance for specific user group.

Table 4-1: Guidelines and best practice summary

Section	Issue	Guideline	User/ Tech/ Policy
3.2.1.1	User-centricity, privacy, inclusion	1. It is essential that individuals should feel empowered to protect their own identity data. This should be underpinned by effective regulation, promoted through user education and enabled through a range of high quality technical options. Issue 3.2.1.1, guideline 21. 2. Public authorities should act as an example to the business world, by placing user-centricity at the heart of their processes, in co-operation with the local information commissioner. Issue 3.2.1.1, guideline 23. 3. Incentives should be put in place to encourage organisations to adopt best practice around user-centricity and privacy. Issue 3.2.1.1, guideline 24.	P (TU)
3.2.1.2	Proliferation of identities	4. Greater attention to standard, predictable 'ceremonies' for handling identity transactions should be promoted, in order to improve the user experience. Issue 3.2.1.2, guideline 25.	P
3.2.1.3	Lifecycle of a person	5. Mechanisms are required to manage identity throughout life, including periods of incapacity such as childhood and illness. Wherever possible, these mechanisms should be controlled by the subject. Issue 3.2.1.3, guideline 1. 6. Current actions influence future reputation. To alleviate the life-long impact of earlier misdemeanours, there is value in exploring means of 'forgiving', even if 'forgetting' is not practicable. Issue 3.2.1.3, guideline 2.	U

Section	Issue	Guideline	User/ Tech/ Policy
3.2.1.4	Digital identity awareness	7. Keeping safe online involves awareness of your own behaviour, who you mix with, where you go and potential means of defence. It should be based on the kind of common sense that discourages people from picking fights with strangers, walking down dark alleys alone at night, picking up unidentified objects and leaving their mobile phone at home. Issue 3.2.1.4, guideline 3. 8. The subject should use appropriate technical protection, while keeping in mind that, like a seat belt, it is not a panacea for all potential risks. Issue 3.2.1.4, guidelines 4-5.	U
3.2.1.5	Anonymity	9. There are strong social reasons to provide credible anonymity in the digital environment. At present the majority of online transactions can be traced via information available through the networking infrastructure, such as IP addresses. More effective and widespread mechanisms to support anonymity are required. User awareness of the varying degrees of disclosure is also important in this area. Issue 3.2.1.5, guidelines 6-10.	T (U)
3.2.2.1	Lifecycle of an identity	10. Different IDs may need to be renewed/replaced several times throughout a person's lifetime. For reasons of currency and security, it is essential that effective expiry dates are identified and respected. Issue 3.2.2.1, guideline 11.	T (U)
3.2.2.2	Open standards, Open interfaces	11. Policy measures promoting open source initiatives have the potential to contribute to a more flexible, reliable ecosystem. Issue 3.2.2.2, guideline 28.	P (T)
3.2.2.3	Devices, portability, security of credentials	12. Choice and variety are essential to a healthy identity infrastructure. With the proliferation of novel devices, the portability of digital identities between devices, while maintaining the security of credentials, will be a key requirement. Issue 3.2.2.3, guideline 12.	T
3.2.2.4	Unlinkability	13. Greater emphasis should be placed on the desirability of maintaining unlinkability between digital identities. This is matter for policy, user awareness and further development of the available technology. Issue 3.2.2.4, guideline 13.	T (PU)

Section	Issue	Guideline	User/ Tech/ Policy
3.2.2.5	Dynamic management of partial identities	14. The subject should be in a position to achieve a reasonable degree of separation of identity, without undue management overheads. The standard systems administration model, which allows for multiple roles (e.g. user + administrator + director) to be allocated to a single individual, may provide useful insights in this respect. Issue 3.2.2.5, guideline 15.	T
3.2.2.6	Inflexibility of systems	15. The online environment is extremely fast moving. The moment a rule is written, some inventive individual will find a way to subvert it for personal advantage. It is essential that systems are sufficiently flexible to deal with the changing nature of the digital landscape. Issue 3.2.2.6, guideline 16.	T
3.2.2.7	Spam	16. Greater focus is required on the business model of spam. Its prosperity depends on the prospect of some kind of reward, with minimal overheads or risks. The overheads are likely to remain minimal, while the reward can be decreased through effective user education. However, there is scope to look more closely at increasing the penalties and therefore the risk to the spammer. Issue 3.2.2.7, guideline 29.	P
3.2.2.8	Data mining	17. Substantial measures are required to monitor and curb excessive surveillance of individuals by third parties. Linking of various elements of personal data is of particular concern in this respect. Issue 3.2.2.8, guideline 31.	P
3.2.3.1	Ownership	18. Greater clarification is required regarding the ownership of online identity data. This may be particularly complex in relation to virtual worlds, where characters and their goods can have substantial real-world value. Issue 3.2.3.1, guideline 32.	P
3.2.3.2	Trust	19. An essential requirement in supporting trust in the online environment is that existing laws should be enforced effectively, with penalties that provide adequate deterrence. Issue 3.2.3.2, guidelines 33-34. 20. The online environment changes very rapidly, so it is essential that existing legislation is reviewed on a regular basis to ensure that it is still adequate to encompass any emerging issues. Issue 3.2.3.2, guideline 35.	P

Section	Issue	Guideline	User/ Tech/ Policy
3.2.3.3	Revocation	21. Clarification of the legal position regarding revocation is required. Individuals should have the means to ensure that their data is not unreasonably retained on systems, once they have requested its removal. Issue 3.2.3.3, guideline 36.	P
		22. Further research is required into the revocation of biometrics. The Turbine project would seem to provide an excellent model for this. Issue 3.2.3.3, best practice 11.	T
3.2.3.4	Attacks – whitewashing, sybil attack, DDOS	23. Insofar as possible, security mechanisms should be built into systems to limit the opportunity for those systems to be subverted by attacks involving the abuse of multiple identities. Issue 3.2.3.4, guidelines 18-20.	T

4.1 End user

4.1.1 Whole life approach - Issue 3.2.1.3

Mechanisms are required to manage identity throughout life, including periods when full capacity is lacking, such as childhood and illness. Wherever possible, these mechanisms should be controlled by the subject. Where it is necessary for a proxy to be appointed to assist the subject in dealing with these mechanisms, it should be on a case-by-case basis. For example, a person who is unable to deal with complex legal and financial affairs due to mild cognitive impairment is highly likely to have sufficient capacity to make valid decisions regarding their housing and daily care. A proxy may be appointed to handle the subject's financial affairs. Should their health deteriorate further, an entirely separate proxy, such as a family member, might take responsibility for decisions regarding their housing and daily care [DEMENTIA].

In the case of a child, the proxy would normally be the child's parents or legal guardian, until such time as they reach adulthood. It is vital that children are provided with appropriate education and protection from the earliest age. There are a number of software packages produced with the aim of enabling children to use the Internet safely. Although these may contain valuable features, appropriate supervision of children while they are online is still essential. For parents or guardians to be able to supervise children effectively, they too will require an appropriate level of knowledge.

BP 1
Education targeted at the general public should be simple, practical and broad in scope, such as that produced by the UK Office of the Information Commissioner [ICO]. Too narrow a focus on financial fraud or 'stranger danger' may cause the practical essentials to be overlooked in favour of an inappropriately alarmist response.

GL 1
For adults who lack the capacity to manage their own affairs, the proxy should as far as possible be a responsible person of their own choosing. Clearly, circumstances may occur which require intervention by the relevant authorities. In every case, the guiding principle should be that individuals retain as much control as possible within their range of capabilities [DEMENTIA].

Attention paid to proxy mechanisms within the digital arena could contribute substantially to this often problematic area. At present, the non-digital interventions can tend towards an all-or-nothing approach: an individual who is unable to manage a particular area of their life may be deemed 'incapable' in a more general sense and unnecessarily deprived of day-to-day autonomy. Issues around banking and incapacity have historically been hard to manage successfully. Many transactions have required the individual to be present at a branch of the bank. Arrangements for those physically unable to attend in person, even if mentally competent, have tended to be obscure, complex and lengthy [OMBUDSMAN]. Indeed, they have often involved handing over an unnecessary level of control to a third party.

BP 2
With a networked world in which remote transactions are increasingly becoming the norm, processes to support people in managing their own affairs from any location are becoming increasingly widespread and helpful in this area[30].

4.1.2 Enduring reputation - Issue 3.2.1.3

Current actions influence future reputation. Personal details posted online, whether by you or a third party, are effectively public across the world. These details may be in the form of text, photographs or video. Under certain jurisdictions, it may be possible to take steps to have the original defamatory material removed, but this is not an easy process and, in the interim, any number of people may have downloaded the material and, in the case of text and photographs, printed it out. One may be able to retrieve the original, but the multiple copies will continue to exist and may be published again at any point.

The risk is greatest to children, who may not have the maturity and life skills to understand the ways in which current activities could jeopardise their future wellbeing and prosperity. They are also likely to see much greater social and technological changes across their lifetimes than other generations.

BP 3
This point is highlighted in a recent European Commission publication 'A comprehensive approach on personal data protection in the European Union' [EU PD]. The document underlines the extent to which the online environment has changed in the fifteen years since the introduction of the 1995 Data Protection Directive. Specifically, the risks to personal information have increased substantially with the advent of cloud computing and the popularity of social networking. At the same time, methods of collecting information have become increasingly sophisticated and subtle. The principles underpinning the Directive are still applicable, but there is a need to review the measures required to support those principles.

The right to data protection is now enshrined as fundamental under the 'EU Charter of Fundamental Rights' arising from the Lisbon Treaty. Recent moves would place greater emphasis on transparency and mandatory data breach notification. Four key areas identified for further scrutiny include data minimisation, improved processes for individuals to control the way in which their information is managed (relating to access, speed of response and removing associated charges), the 'right to be forgotten', i.e. removal of data and data portability.

GL 2
To alleviate the life-long impact of earlier misdemeanours, there is value in exploring means of 'forgiving', which could take a number of forms. Reputation bankruptcy (see Section 3.2.3.4), which in principle permits an individual to start afresh following substantial damage to their reputation, might provide one option, even if 'forgetting' in a complete sense may not be practicable.

[30] http://www.personal.barclays.co.uk/BRC1/jsp/brccontrol?task=articlesocial&site=pfs&value=2655&menu=2634

4.1.3 Online behaviour - Issue 3.2.1.4

BP 4

Keeping safe online involves awareness of your own behaviour, the people you mix with, where you go and potential means of defence. It should be based on the kind of common sense that discourages people from picking fights with strangers, walking down dark alleys alone at night, picking up unidentified objects and leaving their mobile phone at home[31].

Behaviour which is unacceptable in everyday life is likely to be similarly unacceptable online. For example, verbally attacking an individual online can have very serious consequences. It may result in harm to your reputation, being banned from particular communities and even remote attacks on your equipment. Arguments started online may result in litigation, or in exceptional circumstances may spill over into physical violence. It is therefore dangerous to regard the online world as somehow separate from everyday life. The increasing prevalence of cyber bullying shows that being online is simply another means of communication, with features that can be used in negative as well as positive ways.

The company you keep is another important consideration online. Visiting the wrong kind of website may leave your system infected and your data compromised. Engaging in a transaction with a previously unknown retailer may result in substantial financial loss. It is always wise to mitigate these risks by aiming to deal with well-known organisations, preferably those that have a physical presence or a good reputation, which they will want to protect. The most conservative may choose to deal only with high street names.

In any case, it is important to be aware of your potential liability in any situation and limit risks as far as possible. Choosing your means of payment according to the protection provided by its terms and conditions is an obvious example. As in all situations, a reasonable degree of scepticism is preferable to hard and fast rules. For example, it is common for criminals to create very convincing replicas of popular websites for their own purposes.

GL 3

A degree of suspicion can provide protection in such circumstances where otherwise familiar features are used to lull the individual into a false sense of security. While technical protection is essential, it is not sufficient to guarantee staying safe online.

4.1.4 Use of technical protection - Issue 3.2.1.4

BP 5

There are many excellent means of technical protection that individuals and organisations can use to keep themselves safe online. The enduring principle is one of 'defence in depth', ensuring that a range of complementary mechanisms is in place. Individually, they are only effective in a limited way, but collectively they can provide a reasonable level of protection. Such mechanisms might include the following kinds of software: anti-virus, firewall, anti-spyware, anti-spam.

GL 4

It is important to keep in mind that technical protection is not a panacea for all potential risks. As soon as a countermeasure against an attack is introduced, attackers will seek another means of compromising systems. This is an unending game of cat and mouse. Due to the increasing prevalence of zero day attacks (attacks which are previously unknown and not normally detected by existing security software), it is very important to keep software updated. In that way, the updated software will be able to recognise and protect against recently identified forms of attack as quickly as possible. Unfortunately, this is a very fast-moving area and relying on protection which is not updated is likely to result in the system being compromised. Even fully updated software is no guarantee of invulnerability.

[31] http://www.staysafeonline.org/tools-resources/stop-think-connect

BP 6
Apart from the standard software protection described above, other means of protection such as encryption software and smart cards can improve system security. Simple measures such as the use of strong passwords, which are sufficiently long, use a wide range of characters and are changed regularly, can also make an important contribution.

GL 5
While in principle all these measures should contribute to the security which an individual experiences online, it is important to be aware that there may be a tendency to place too much trust in technical protection. This is reminiscent of the seat belt paradox, whereby providing drivers with greater protection, such as seat belts, can result in their feeling more secure and confident within their vehicle and consequently driving faster. Behaviour may become riskier to compensate for the perceived increase in safety. In this way, the benefit from security interventions may be diminished.

4.2 Technical

4.2.1 Infrastructural anonymity - Issue 3.2.1.5

GL 6
There are strong social reasons to provide credible anonymity in the digital environment. These include support for freedom of speech, which although contested under some circumstances, is broadly regarded as a positive feature of a free society. Similarly, mechanisms are required for whistleblowers to be able to alert the authorities without fear of retribution (see Section 3.2.1.5).

GL 7
By default, transactions should preserve the anonymity of those involved. If information regarding the various parties is to be exchanged or retained, this should be the minimum information necessary to the transaction.

GL 8
A clear justification should be required for any disclosure [KC LAWS ID], as well as the prior agreement of the relevant parties. At present, this is not the case and the majority of online transactions can be traced via information easily available through the networking infrastructure, such as IP addresses and MAC addresses. Although anonymity services, such as those provided by Tor[32], are available, they are not yet widely used.

GL 9
Privacy-enhancing technologies[33] (PETs) have a role to play in promoting more effective and widespread mechanisms to support either true anonymity or conditional anonymity (which allows the participant anonymity, so long as they do not contravene the agreed rules). Although the cryptography behind these technologies can be extremely complex, the varying degrees of disclosure that they can support are quite easily understood [PLIFE SNS].

While the technical community may show considerable enthusiasm for PETs, policymakers and the general public tend to be largely unaware of their potential to provide huge improvements in the user experience. With policy based on outdated concepts, such as privacy being inversely proportional to security[34], the public is deprived of the high quality, user-centric, privacy-enhancing infrastructure that it deserves.

GL 10
There may be scope for an education programme, to assist the public to understand the benefits that PETs can offer. This could play a valuable role in enabling people to make informed choices regarding the management of their identity online. At present, most education programmes are targeted at enabling individuals to participate in the existing online environment. There would be considerable social and commercial benefits from encouraging them to look ahead and strive for a safer, more effective, user-centric environment.

[32] http://www.torproject.org
[33] PETs are commonly understood to include smart cards, biometrics and cryptography
[34] http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html

4.2.2 Renewals - Issue 3.2.2.1

An effective means of managing expiry and renewal is one of the most important features of an identity system. If an electronic ID is compromised, unless there is a central deactivation mechanism, it may be misused until the expiry date. Without an expiry date, the abuse may continue indefinitely. It is therefore essential for reasons of currency and security that effective expiry dates are implemented and enforced.

Different IDs may need to be renewed/replaced several times throughout a person's lifetime. This may be for practical reasons relating to the individual, such as changes in appearance and even biometrics over time. To achieve an acceptable level of false negatives (where a valid user is denied access) and false positives (where an invalid user is refused access), the currency of the data must be treated as a priority. A recent report by the US government [BIO US] has highlighted the significance of the variability of biometric data over time.

A further concern is the technical lifespan of an electronic identity. There are ongoing developments in technology, which see new attacks and new solutions published on a continuous basis. Even without new attacks, any identity depends on underlying mechanisms which are hard to break, but not impossible. The longer an identity is used, the more likely it is to be compromised.

GL 11
It is therefore essential that proper attention be paid to identifying the types of identity mechanisms that are appropriate to different tasks and a reasonable expectation of their lifespan.

4.2.3 Choice of identities - Issue 3.2.2.3

Choice and variety are essential to a healthy identity infrastructure[35]. Historically, we have seen too great a focus on government-issued electronic identity. This can have the effect of polarising debate around the identity infrastructure, between those who would support a large scale government implementation and those who would fight it. With a healthy electronic identity market, it should be possible to rise above this[36]. Ideally, it would be preferable to have a range of identities available from many different kinds of providers. The identities could be used for a number of different purposes, depending on the level of assurance required.

A key question in choosing an identity should be 'who do you trust?' You may trust your central government, local authority, bank, ISP, or a specialist security provider.

BP 7
In some countries, this has traditionally been a central government function, but the success of BankID in Scandinavia shows that this does not have to be the case. BankID enables individuals to access online government services using an identity that is issued by their bank. One of the great benefits of this is that the citizen has a commercial relationship with the identity provider and has the option to switch providers whenever they choose. This gives the providers a major incentive to offer high quality, convenient services, which will engender customer loyalty. Because the service is provided via the banks, with which most people already have a relationship, there is an existing level of trust underpinning the service.

GL 12
With the proliferation of novel devices, the portability of digital identities between devices, while maintaining the security of credentials, will be a key requirement. So not only will we have a choice of identity providers, but we will also have a choice of devices on which to store our credentials. Compatibility between systems and portability of personal data will be a key requirement in this area.

[35] http://msdn.microsoft.com/en-us/library/ms996422.aspx
[36] http://www.computerweekly.com/blogs/editors-blog/2010/05/goodbye-id-cards---is-it-time.html

4.2.4 Unlinkability - Issue 3.2.2.4

GL 13
At present, links are all too easily forged between different identities. This may enable the identity provider or the relying party to build up a very substantial picture of the identity holder by aggregating information from multiple sources. Where such links are necessary, appropriate mechanisms can be put in place, but the default for all systems and services should naturally be unlinkability. [KC LAWS ID]

BP 8
Traditionally, systems have not managed unlinkability well, but more advanced systems [PL OSI] now provide scope for an individual to keep their relationships with individual service providers entirely separate. This is clearly an area in which greater use of privacy-enhancing technologies would be of value. One option is for a user to derive multiple sub-identities from their main identity, without any of the relying parties being able to tell whether or not they are dealing with the same person from the information relating to the sub-identities.

GL 14
Greater emphasis should be placed on the desirability of maintaining unlinkability between digital identities. Although further development of the available technology is important in this area, policy and user awareness also have significant parts to play. If policymakers and users can become more aware of the tremendous power of this kind of technology, it could lead to greater convenience, security and privacy for all involved.

4.2.5 Separation of identity - Issue 3.2.2.5

BP 9
The subject should be in a position to achieve a reasonable degree of separation of identity, without undue management overheads. The Higgins model (see Section 3.1) offers considerable flexibility in this area; the opportunity to select attributes from the full range of identities held by the subject, according to the requirements of a particular situation.

In a social networking environment, the need for multiple partial identities is particularly clear. For example, a person may move in a number of different and sometimes conflicting social circles; student friends, football team mates, colleagues and extended family. It would be desirable to be able to keep communications with these groups separate from one another. In some circumstances it would also be desirable to ensure that particular groups are invisible to one another. For example, where a person is professionally involved in groups working on highly confidential projects, these affiliations should not be visible to their wider social circle.

BP 10
The standard systems administration model, which allows for multiple roles (e.g. user + administrator + director) to be allocated to a single individual, may provide useful insights in this respect. It has long been recognised that security is best served when an individual connects to a system with only the minimum level of authority required to carry out the current task. This may be a simple user login for browsing the web. Equally, it may be a very secure identity for the purposes of initiating large money transfers. To use the high quality identity for simple web browsing is to take unnecessary risks[37].

GL 15
The work of the PrimeLife project (see Section 2.3.4) in this area seems likely to make a significant contribution to future developments.

[37] http://www.sans.edu/resources/securitylab/it_separation_duties.php

4.2.6 Flexibility - Issue 3.2.2.6

The online environment is evolving quickly. The moment a rule is written, some inventive individual will find a way to subvert it for personal advantage. In old-fashioned monolithic systems, this could be catastrophic. Once the system is subverted, that flaw remains in place until a comprehensive rebuild of the system can be achieved. It is essential that systems are sufficiently flexible to deal with the ever-changing nature of the digital landscape.

GL 16
Modular systems based on open standards and open interfaces offer the opportunity to correct any identified faults in the system much more quickly and cheaply and at less risk to the subject. They also enable a greater degree of transparency, in that the system is not just a 'black box' with unknown properties. At the very least, it is a collection of modular parts, which join together in a prescribed and largely predictable way. Where an error occurs, it is much easier to isolate and therefore correct.

GL 17
The traditional intertwining of the data layer with the identity layer has involved an unnecessary degree of inflexibility. Keeping these two layers separate allows much greater nuance to be expressed within the identity layer, without this having any kind of adverse effect on the workings of the data layer. Equally, more flexibility is required within the identity layer itself, so that complex relationships and policies can be expressed more effectively (see Section 3.2.2.6).

4.2.7 Revocation of biometrics - Issue 3.2.3.3

Biometrics functions by measuring personal characteristics, which makes it a particularly sensitive area of identity. It is commonly understood that each person has only one set of physical characteristics (fingerprints, iris). Although these may change over time, this does not provide the kind of scope for renewal or revocation that other kinds of identity mechanism, such as passwords or tokens, can offer. Indeed, it is part of the integrity of many identity mechanisms that they should be renewed on a regular basis.

For these reasons, a level of abstraction has been introduced into the processing of biometrics. Rather than basing processing on a full image of a person's characteristics, a template is used. This holds a much more limited range of data, but still enables the system to ascertain with a reasonable degree of certainty whether the person presenting themselves is indeed the person associated with the template. This way of handling biometrics is known as Biometric Template Protection and is now implemented by a number of major international vendors [BUSCH]. The crucial expectation here is that it is not possible to recreate the original image from the template.

Although a huge improvement on earlier more basic matching processes, this still has the potential to present some issues. In the unlikely event of identical templates being held by different organisations, it might be possible to link information held by different parties about the individual concerned. Another difficulty with biometric measurement is that it has the potential to give away important personal information. For example, changes to the eye are well known to be early warning signs of certain serious health conditions.

BP 11
Further research is required into the revocation of biometrics, which have an important role to play in the world of identity. The EU-funded Turbine project would seem to provide an excellent model for this [BUSCH].

4.2.8 Protection against multi-ID attacks - Issue 3.2.3.4

Insofar as possible, security mechanisms should be built into systems to limit the opportunity for those systems to be subverted by attacks involving the abuse of multiple identities. Assurance and verification lie at the heart an effective identity infrastructure. Without the capacity to spoof e-mail addresses, spam would be much less widespread. Although a number of mechanisms, such as encryption, are already available, they are not necessarily used to full advantage.

GL 18
More common use of secure protocols such as BGPSEC, IPSEC and DNSSEC would contribute significantly to the assurance around transactions. Although these may introduce greater complexity and processing overheads, the commercial and social benefits of more secure transactions should also be taken into account.

GL 19
In order to manage the threats presented by whitewashing and sybil attacks, it is important that policies relating to multiple identities are agreed at the design stage of system implementation. If such situations are envisaged, then appropriate protection can be put in place in advance.

GL 20
It is particularly important that mechanisms for welcoming new users to a system are not repeatedly abused through the whitewashing attack. Any policies to counteract sybil attacks should make it clear under which circumstances (if any) it is acceptable to hold multiple identities on a system. System rules would need to take into account the risks of pseudospoofing under these sybil attacks. A well- designed system should have the ability to limit the risk of sybil attacks, while maintaining a reasonable degree of separation of identity, as described in Section 4.2.5.

4.3 Policy

4.3.1 Effective regulation - Issue 3.2.1.1

GL 21
It is essential that individuals should feel empowered to protect their own identity data. This should be underpinned by effective regulation.

BP 12
Perhaps a useful reference point is the recent Resolution of Madrid [MADRID], agreed by representatives from 80 authorities and 42 countries. With the aim of promoting privacy, as well as supporting international data flows via standardisation, it draws on these existing policy texts:

- OECD Privacy Guidelines
- Council of Europe Convention 108
- UN Guidelines from the General Assembly
- European Union Data Protection Directive
- APEC Privacy Framework
- US DoC Safe Harbor Principles
- RIPD Data Protection Guidelines

GL 22
It is only by taking a global approach of this kind that data protection can effectively be handled in a global market place. Although regulation is vital in this area, user education and a range of high quality technical options are also required to achieve a successful identity ecosystem.

4.3.2 Public sector leadership - Issue 3.2.1.1

Government bodies, whether central or local government, are uniquely well placed to provide an example in the area of identity management. Their systems are likely to be experienced by the majority of citizens within their area of responsibility and so will significantly influence individuals' understanding of the role of identity in a digital world. Many of the technical interventions, such as privacy-enhancing technologies, which have the potential to greatly enhance the online experience, are not being implemented as freely as might be expected. Indeed, there tends to be a certain degree of conservatism in the identity market. As it is such a sensitive area, tried and tested solutions are often preferred by businesses.

If the full benefits of progressive technologies are to be reaped, a reasonable number of high quality implementations are required to prove that they can be successfully deployed on a large scale. Public sector bodies can provide both the scale of implementation and proof that these technologies can work with a wide range of associated services.

GL 23
By the nature of their operations, public sector bodies have the greatest incentive to act as an example to the business world, by placing user-centricity at the heart of their processes, in co-operation with local data protection authorities.

4.3.3 Best practice incentives - Issue 3.2.1.1

GL 24
There is a significant need for greater recognition and adoption of best practice around identity management. For many businesses and public sector bodies, this could lead to improved customer satisfaction and loyalty. However, at present, privacy and identity tend to be consigned to either technical functions (the implementation) or legal functions (in order to meet data protection requirements). In principle, as identity and privacy are likely to underpin the entire customer relationship, they should play a much more prominent role.

There would be considerable value in using incentives, such as industry award schemes or even public grants, to encourage organisations to adopt best practice around user-centricity and privacy. In leading to a more positive online experience, it would encourage individuals to use online services. This would contribute towards inclusion goals, as well as potentially saving money by decreasing the extent of more expensive offline service delivery.

It would also help in allowing individuals to experience the benefits of high quality identity systems, and therefore raise awareness in the population of the capabilities of such systems.

4.3.4 Ceremonies - Issue 3.2.1.2

Many of the risks involved in using the Internet at present result from the unpredictability of interactions. An organisation that warns us never to respond to phishing emails may still send us any number of informational emails each month. In practical terms, we have no real means of telling the difference between a spoofed mail and a genuine one. Even fraudulent websites are now exceptionally well crafted, with the result that they are effectively indistinguishable from the genuine sites of respectable international corporations. Indeed, it is common for fraudsters to use an almost perfect replica of a banking site to lure customers of that bank into divulging their personal details.

Whilst it is important for users to develop an awareness of the risks inherent in the online experience, it is also important to ensure that service providers are doing everything possible to provide users with a secure and predictable service. It is not reasonable to expect users, who are in general not experts, to be able to predict which kinds of interactions are safe and which are not. The diversity of processes involved in online interactions makes this still more problematic.

GL 25
A clearer definition of the steps required to complete specific kinds of transaction, such as purchasing online, could contribute significantly in this area. It could form the basis of greater uniformity based on agreement between major organisations. This would result in a much firmer basis for user education, which could focus on what should normally be expected, so that any anomalies are more easily highlighted.

GL 26
At present, it can be hard to deliver user education, as the answer to so many important questions would appear to be 'it depends'. For someone new to the Internet, this can be very frustrating. Greater attention to standard, predictable 'ceremonies' for handling identity transactions should be promoted, in order to improve the user experience.

4.3.5 Open source - Issue 3.2.2.2

In a world where digital identities are increasingly prominent and the federation of identities is becoming more widespread, Open Standards such as those developed by the Liberty Alliance and championed by Higgins (see Section 3.1) have a great deal to offer. Identity federation is a very complex process, which is still in the early stages of development. While a degree of technical interoperability may have been achieved, significant challenges remain around semantic interoperability.

GL 27
Sticky policies have been suggested [POLICIES] as a valuable approach in dealing with this. They may help to ensure that users do not unexpectedly find their data being used on secondary systems in ways that they had not envisaged when they first signed up to a service on another system.

In an era where users are becoming increasingly sophisticated and asking searching questions regarding the basis on which they should trust systems, the transparency offered by open source has considerable appeal. One can be confident that the processes underlying the system have already been subject to considerable scrutiny from the open source community.

GL 28
There are also commercial benefits. Historically, procurement of large-scale proprietary systems has tended to lead to lock-in and greater system costs in the longer term. Where these systems are based on open source, it is much easier to move on from the original supplier, with less disruption and fewer associated costs. In this context, policy measures promoting open source initiatives should be used to contribute to a more flexible, reliable ecosystem.

4.3.6 Spam - Issue 3.2.2.7

Greater focus is required on the business model of spam. Its prosperity depends on the prospect of some kind of reward, with minimal overheads or risks. It relies on the likelihood of one person in many thousands clicking on a link in response to an unsolicited email.

GL 29
The overheads are likely to remain minimal. The reward can be decreased progressively through effective user education and technical measures, in conjunction with the promotion of predictable 'ceremonies' in handling email. However, there is scope to look more closely at increasing the penalties and therefore the risk to the spammer.

GL 30
Where penalties are financial and the spammer is based outside the relevant jurisdiction, it may be difficult to achieve any kind of redress. However, there would be value in looking at all parties involved in the process to see whether a different approach could help to limit the harm done by spam.

4.3.7 Surveillance – Issue 3.2.2.8

Online surveillance has seen a huge rise in recent years. This may not be the kind of traditional surveillance associated with private investigators or government intelligence agencies. Rather, it is often the result of close monitoring of an individual's activities online. These can then be analysed and used to target the person concerned with individualised advertising.

Many online entities, including search engines, commerce sites and webmail providers, are able to glean detailed personal information from the kind of searches a person makes, the kind of sites they visit and the themes which occur within their email. It can be alarming to become aware of the amount of information (and potentially misinformation) that these entities can hold about a person. With data aggregated from multiple sources, the picture can become very much more detailed still.

GL 31
Substantial measures are required to monitor and curb excessive surveillance of individuals by third parties. Linking of various elements of personal data is of particular concern in this respect.

4.3.8 Ownership - Issue 3.2.3.1

Greater clarification is required regarding the ownership of online identity data. It is still common for people to impersonate well-known public figures online, with comparatively little redress. Within Europe, identity data is generally considered to belong to the subject, whereas in other jurisdictions it is considered to belong to the owner of the system on which it is held. With the advent of cloud computing, it is now often very hard to know exactly where data are actually held. Indeed, multiple copies are frequently held in multiple locations.

The question of ownership may be particularly complex in relation to virtual worlds, where characters and their goods can have substantial real-world value. For example, an individual may invest a large amount of time, money and energy into the development of their avatar under an assumed name, within a virtual world. Losing the name and the associated reputation, even if they retain all their associated goods, still leaves them with a substantial loss. With activities within virtual worlds reliant on the goodwill of the organisations that run them, there is no predictable means of restitution.

GL 32
In order to bring greater certainty to online interactions, further investigation should take place into the nature of ownership of digital identities of all kinds.

4.3.9 Enforcement - Issue 3.2.3.2

The data protection and privacy laws in place within the EU aim to provide protection for the personal information of individuals. They certainly provide valuable input regarding the ways in which personal information should be managed. There has, however, been an ongoing issue with the degree of protection afforded, due to a lack of adequate enforcement in some areas[38].

GL 33
This is not the result of unwillingness on the part of the data protection authorities. Rather, where shortcomings have occurred, it has tended to be due to the authorities having insufficient powers to take effective action against those who would contravene data protection laws. Where the risk associated with action by the data protection authorities is less than the cost of putting the correct processes in place, many organisations will cut corners and accept this risk. It is therefore essential that appropriate penalties are in place to ensure that organisations meet their data protection obligations.

GL 34
An essential requirement in supporting trust in the online environment is that existing laws should be enforced effectively, with penalties that provide adequate deterrence.

[38] http://www.scmagazineuk.com/infosecurity-europe-ico-speaks-on-future-of-regulation-three-weeks-after-its-500000-fines-were-introduced/article/168752/

4.3.10 Regular review of legislation - Issue 3.2.3.2

The online environment changes very rapidly, so it is essential that existing legislation is reviewed on a regular basis to ensure that it is still adequate to encompass any emerging issues. A clear example of this is the 1995 Data Protection Act , which was well drafted fifteen years ago. In the interim, however, the use of digital data processing has developed so enormously that it has at times been hard for the legislation to keep pace.

An example of the potential issues may be seen in the handling of anonymised data. In recent years, a process known as de-anonymisation has become widespread, especially in academic circles. This involves data that had previously been anonymised to protect the identity of individuals, being retrieved and pieced back together again to provide a detailed picture of their personal characteristics. A recent paper by Paul Ohm [ANONYM] describes the underlying issues relating to this in some detail. Effectively, it gives us reason to re-evaluate the entire concept of 'personally identifiable information', which is central to effective data protection and privacy laws.

BP 13
The recent move by the European Commission to update the laws surrounding data protection and privacy [EU PD] underlines the need for legislation to be kept under review.

GL 35
It is to be expected that the online environment will continue to change rapidly over coming years and the relevant legislation must be adapted as necessary.

4.3.11 Revocation - Issue 3.2.3.3

Clarification of the legal position regarding revocation is required. Indeed, under UK law there is no clearly defined and absolute right to revocation of an identity [ENCORE]. This is a very serious situation, as a digital identity is not only a partial representation of the subject, but often also a means of accessing particular services. An irresponsible service provider may not be too concerned about who is accessing those services. However, if the services are of a confidential or personal nature, this could cause considerable harm to the individual concerned. This harm could take a number of forms, including reputational and financial damage.

Given that the process for signing up to a service is not normally negotiable, but simply involves agreeing to the terms and conditions and providing the required amount of personal information, it seems unfortunate to make the resulting relationship effectively lifelong and binding. You may choose not to receive their services any longer, but your right to be removed from their systems is much less clear.

GL 36 This is an important area, which deserves further attention. Fundamentally, individuals should have the means to ensure that their data is not unreasonably retained on systems, once they have requested its removal.

4.4 Conclusions

Though the field of digital identity is still developing, some key principles have emerged. Many of these have their origins in the following:

- OECD Privacy Guidelines (1980) [OECD PRIV];
- EC 'Data Protection' Directive 95-46 (1995) [EC DPD];
- Kim Cameron, The Laws of Identity (2005) [KC LAWS ID].

Nowadays each person has the opportunity of living multiple lives in parallel, in the real as well as in the virtual world. A trend observed over the last years, first in the research community, but now also in commercial offerings is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet.

An area of particular interest is the management of multiple identities, where "identity" is being considered in a broad sense. Issues related with this area include anonymity, pseudonymity, unlinkability and unobservability. The increasingly digital nature of relationships between people is central to dealing with those issues. It is not a question simply of hardware or software, but more importantly of enabling people to enjoy and benefit from their online experiences, while dealing with potential issues. The problems might include a lack of knowledge or training, difficult personal circumstances or simply irritation at the diversity and unpredictability of online privacy and identity mechanisms. It is therefore vital that we should have strong, reliable mechanisms, which can be easily understood and relied upon across the course of a lifetime.

This is a very ambitious aim, but one that is potentially well supported by the range of technologies developing in this area. Privacy enhancing technologies have a major role to play. Equally, simple good sense, such as using appropriate strength of authentication and not keeping credentials beyond their useful lifespan, are important considerations. The adoption of open standards, with the flexibility this implies, also has a significant part to play.

There is considerable scope for policy makers (legislators, regulators etc.) to assist by supporting and protecting people in their online experience. Problematic activities such as spam, data mining and other identity-related attacks deserve close scrutiny and development of a framework to address them. There are still questions to be resolved around the legal implications of ownership and also revocation of identities online. In such a fast-moving and interconnected area, it is likely that these and other issues will require the ongoing attention of policy makers in the coming years.

The issues discussed in this paper have been divided into three categories, although in many cases there are significant areas of overlap:

- User - those most applicable at the level of organisations dealing with awareness raising. Guidelines for this group relate to:
  - User-centricity, privacy, inclusion
  - Lifecycle of a person
  - Digital identity awareness
  - Anonymity
  - Lifecycle of an identity
  - Unlinkability

- Technical - those most applicable at the technical level. Guidelines for this group relate to:
  - User-centricity, privacy, inclusion
  - Anonymity
  - Lifecycle of an identity
  - Open standards, open interfaces
  - Devices, portability, security of credentials
  - Unlinkability
  - Dynamic management of partial identities
  - Inflexibility of systems
  - Revocation of credentials
  - Attacks on security mechanisms

- Policy - those most applicable at the policy level. Guidelines for this group relate to:
  - User-centricity, privacy, inclusion
  - Proliferation of identities
  - Open standards, open interfaces
  - Unlinkability
  - Spam
  - Data mining
  - Ownership
  - Trust
  - Revocation of credentials

Fulfilling the given recommendations by organisations dealing with end-user awareness raising, technical communities (developers of software) and policy makers will lead to a better framework allowing for managing multiple identities and by consequence to protect the privacy of individuals.

References

[ANONYM] Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (August 13, 2009). University of Colorado Law Legal Studies Research Paper No. 09-12. Available from: http://ssrn.com/abstract=1450006

[ANONYMITY] Andreas Pfitzmann and Marit Hansen, *A terminology for talking about privacy by data minimization*, August 2010.

[BIO US] Joseph N. Pato and Lynette I. Millett, Editors, *Biometric Recognition: Challenges and Opportunities*, National Academy of Sciences, US, 2010.

[BRANDS] Brands, S. Rethinking *Public Key Infrastructures and Digital Certificates: Building in Privacy*. (MIT Press: 2000).

[BUSCH] Christoph Busch, *Biometrics and Security*, oral presentation at NISNet conference, Finse (Norway), 27 April, 2010. Available from: http://www.nisnet.no/filer/Finse10/Biometrics_and_Security_Busch.pdf

[CHADWICK] David Chadwick, *Federated Identity Management Technologies*, State of the Art Digital Identity workshop, presented at Royal Holloway University, June 2010.

[DEMENTIA] Astell A., *Technology and personhood in dementia care; Quality in Ageing; 7(1):15-25*; 2006.

[DIG SIG] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,* December 1999.

[EC DPD] http://ec.europa.eu/justice/policies/privacy/index_en.htm

[ENCORE] Liam Curren and Jane Kaye, *Revoking consent: A ‘blind spot’ in data protection law?’*, Computer Law & Security Review 26 (2010).

[ENISA PRIV] Ingo Naumann and Giles Hogben, *Privacy Features of European eID Card Specifications,* European Network and Information Security Agency 2009. Available from: http://www.enisa.europa.eu/act/it/eid/eid-cards-en

[ENISA VW] Editor Giles Hogben, *Virtual Worlds, Real Money*, European Network and Information Security Agency 2008. Available from: http://www.enisa.europa.eu/act/it/oar/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming

[EU PD] *A comprehensive approach on personal data protection in the European Union*, European Commission, 4 November 2010. Available from: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[FIDIS] Sandra Steinbrecher, FIDIS Deliverable D4.1, Structured account of approaches on interoperability ch.6, TU Dresden 2005

[FRAME LOC] Reza Shokri, Julien Freudiger and Jean-Pierre Hubaux, *A Unified Framework for Location Privacy*, EPFL-REPORT-148708 June 2010

[GIGYA] *Multiple Identities: What online IDs are people using the most to sign in around the web?* Available from: http://www.gigya.com

[HOGBEN] G. Hogben, *A privacy enhancing identity management framework using the semantic web*, Doctoral Dissertation, Gdańsk University of Technology, Faculty of Electronics, Telecommunications and Informatics, 2009. Available from http://iag.pg.gda.pl/iag/download/Giles_Hogben_PhD_Thesis_SWIM_Framework.pdf

[ICAO MRTD] http://www2.icao.int/en/mrtd/Pages/default.aspx

[ICO] *Data Protection Act Documentation*, UK Information Commissioner's Office, available from: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

[IET S_METER] Kris Sangani, *You're being Monitored, Engineering and Technology*, vol 5, issue 10, IET, July 2010.

[IOS] *Internet of Subjects Charter, 2010*. Available from: http://www.iosf.org

[KANTARA] http://kantarainitiative.org/confluence/display/GI/Identity +Assurance+Framework+v2.0

[KC LAWS ID] Kim Cameron, *The Laws of Identity*, Microsoft Corporation, 11 May 2005. Available from http://www.identityblog.com/stories/2004/12/09/thelaws.html

[KYC] *Discussion Paper 22, Reducing money laundering risk, Know Your Customer and anti-money laundering monitoring*, UK Financial Services Authority, January 2004

[LIBERTY DSF] Liberty Alliance Project, *Liberty ID-WSF Discovery Service Specification*, Version 1.2, 2005.

[LIFELONG] PrimeLife, *Analysis of Privacy and Identity Management throughout Life*, June 2009.

[MADRID] Jose Leandro Nunez Garcia, *Privacy Standards, the Madrid Resolution*, Agencia Espanola de Proteccion de Datos, 2010. Available from: http://isotc.iso.org/livelink/livelink?func=ll&objId=10125101&objAction=browse&viewType=1

[MISC] David Weinberger, *Everything is Miscellaneous*, Times Books 2007.

[MOBILE IDM] Editor Maria Papadopouli, *Mobile Identity Management*, ENISA, April 2010.

[NIST AUTH] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[NIST PIV] http://csrc.nist.gov/groups/SNS/piv/index.html

[NSTIC] www.dhs.gov/xlibrary/assets/ns_tic.pdf

[OECD PRIV] OECD Privacy Guidelines (1980). http://www.oecd.org/document/49/0,3343,en_2649_33703_19216241_1_1_1_1,00.html

[OED] Oxford English Dictionary

[OIX] http://openidentityexchange.org/

[OMBUDSMAN] UK Financial Ombudsman Service, *Ombudsman News, Issue 37, Giving all Customers Equal Access to Banking Services*, May/June 2004. Available from: http://www.financial-ombudsman.org.uk/publications/ombudsman-news/37/banking-equal-access.htm

[ORG] *Internet Password Organizer*, Innovention Lab 2007 - 2009

[PERF] Mark Burnett, Dave Kleiman, *Perfect Passwords – Selection, Protection, Authentication*, Syngress Publishing Inc, 2006

[PKI] Carl Ellison and Bruce Schneier, *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, Computer Security Journal, vol 16, no 1, pp. 1-7, 2000.

[PL OSI] PrimeLife 2nd Report on Standardisation and Interopeability, Overview and Analysis of Open Source Initiatives, H3.3.2/D3.4.2, 28 February 2010.

[PLIFE SNS] PrimeLife Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces, July 2009.

[PL TRUSTED] PrimeLife Analysis of existing web protocols for trusted contents, August 2008.

[POL] Andrew Chadwick, *Internet Politics*, Oxford University Press 2006.

[POLICIES] PrimeLife, *Final requirements and state-of-the-art for next generation policies*, August 2009

[PRIV] Whitfield Diffie and Susan Landau, *Privacy on the Line*, MIT Press 2007.

[REP] Editor Giles Hogben, *Reputation-based Systems: a security analysis*, European Network and Information Security Agency 2007.

[SAFEWARE] Nancy Leveson, *Safeware: System Safety and Computers*, Addison-Wesley 1995.

[TERM] A Pfitzmann and M. Hansen, *A terminology for talking about privacy by data minimisation*, v0.34, 10 August 2010. Available from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[VENN ID] Eve Maler, Drummond Reed, *The Venn of Identity*, IEEE Security and Privacy, vol 6 no 2, pp 16-23, March/April 2008.

[VRM] *Project VRM*, Berkman Center for Internet and Society at Harvard University. Available from: http://cyber.law.harvard.edu/research/projectvrm#

enisa
European Network
and Information
Security Agency

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu