Identity Principles in the Digital Age: a Closer View

Rebecca Wong

Nottingham Law School
Burton Street
Nottingham
NG1 4BU
UK

E-mail: R.Wong@ntu.ac.uk

Joseph Savirimuthu

Liverpool Law School
University of Liverpool
Liverpool
L69 7ZS
UK

E-mail: J.Savirimuthu@Liverpool.ac.uk

Abstract:

Identity and its management is now an integral part of web based services and applications. It is also a live political issue that has captured the interest of organisations, businesses and society generally. High profile security breaches, the spread of online criminality and identity theft have led to increased focus on the design and implementation of sound identity management systems. Virtualisation of data not only raises issues concerning security. As identity management systems assume functionally equivalent roles like authentication, accreditation and determining access, their significance for privacy cannot be underestimated. The Center for Democracy & Technology (CDT) has recently released a draft version[1] of what it regards as key privacy principles for identity management in the digital age. This paper will provide an overview of the key benchmarks identified by the CDT. The focus of this paper is to explore how best the Data Protection legislation can be said to provide a framework which best maintains a proper balance between "identity" conscious technology and an individual's expectation of privacy to personal and sensitive data. The central argument will be that increased compliance with key principles is not only appropriate for a distributed privacy environment but will go

some way towards creating a space for various stakeholders to reach consensus relating to the standards applicable to existing and new information communication technologies**.** The Data Protection legislation provides the basis for achieving an optimal balance between security and privacy concerns. The conclusion however is that securing compliance with the legislation will prove to be the biggest governance challenge – standard setting and norms will go some way to ease the need for centralized regulatory oversight.

Keywords: Identity, privacy, governance, data protection, identity management systems

Reference to this paper should be made as follows: Rebecca Wong and Joseph Savirimuthu "Identity *Principles in the Digital Age: a closer view" International Journal of Intellectual Property Management,* Vol. X, No. Y, pp. 000-000.

Biographical notes:

Dr Rebecca Wong is Senior Lecturer in Law at Nottingham Law School, Nottingham Trent University with teaching and research interests in Tort, Intellectual property, Data Protection and Cyberlaw. Her main areas of specialism are in data protection and privacy. She holds an LLB (1998), MSc (2000), LLM (2001), PCHE (2004) and a PhD (University of Sheffield, 2007) in data protection. She has written widely on privacy and data protection and her recent publications have included *Data Protection Online: Alternative approaches to sensitive data*, 2007, *International Journal of Commercial Law and Technology*, 2(1) 9-16 (reprinted in *Journal of Internet Law*, March 2007 and *ICFAI Cyberlaw*, May 2007) and "Demystifying clickstream data: a European and US perspective" in *Emory International Law Review* 20(2), 563-590 (2006).

Joseph Savirimuthu is Lecturer in Law at Liverpool Law School, University of Liverpool. Teaching and research areas include Internet Regulation and Governance, Child Net Safety and Information Security. He holds an LLB (1987), LLM in International Business Law (1988), Diploma in Legal Practice (1997), PGCE (2004) and Certificate in Internet Child Safety (2007). Joseph is also a consultant with an online mediation company and a firm of copyright, patents and trademark attorneys. His recent publications include *P2P@softwar(e).com: Or the Art of Cyberspace 3.0* (2007), *DRMs, RFID and Disruptive Code: Architecture, Dystopia and Eunomics* (2006), *Reflections on the Google Print Library Project* (2006) and *'Open Source, Code and The Architecture: It's the Memes Stupid'* (2005)

1. Introduction

We have developed a range of measures and solutions to prove and even manage our identity well before the onset of the Internet. How we manage identity, address issues of authorisation, access and integrity is also context dependent. This is not to suggest a form of technological

determinism in our attitudes toward identity management. Rather, it is intended to emphasise the values that we regard as being inalienable that will in turn be instrumental in shaping the technological and design solutions we have at our disposal. Consider the following account, as an illustration of one of the unresolved tensions relating to the management of identity in the digital age. Government agencies collect, process and store personal information to enable them to provide services and fulfill their statutory obligations. Law enforcement agencies access to information on private individuals to deal with security threats and public order issues. Personal internet security has become a live political issue in most countries. As collection, processing and distribution of data becomes decentralized, individuals are now finding that their expectations of privacy and control are now the subject of public interest goals. The reasons for the contestation to an individual's claim to manage his or her identity is not difficult to fathom. The Internet is also becoming a playground of criminals. Criminals are using sophisticated technologies to facilitate a range of criminal activities. The "Internet Security Threat Report" issued on September 17, 2007[2] describes the increased use of technologies to facilitate identity theft, and the acquisition of personal and sensitive information. The Anti-Phishing Working Group, noted that 25, 683 unique phishing reports were received in December 2007. Securing trust is now a priority. Access to and control of personal data by businesses and organisations is regarded as critical to maintaining consumer and business confidence in the online environment. 'Identity management', for the purposes of this work, is broadly concerned with the range of technologies that are used to manage 'data' relating to the attributes or characteristics of a person or a subject and which are relied upon when dealing with a person's credentials and rights to access. The infrastructures currently available on the market deal with a range of matters already familiar to us in the offline environment: authentication and access. A key feature of evolving identity management technologies is that the applications have embedded identity conscious software. The exponential growth in the market for identity management software reflects the concerns of organisations, businesses, governments and their agencies of the importance of providing greater security for information and the trust implications that accompany breaches or abuse of data. The concern is particularly acute as many mechanisms for data collection, storage and distribution are also automated. In short, the management of identity is now regarded as an integral part of securing web based services and applications. As identity management systems assume functional roles which erode the public and private space, privacy issues and the values we regard as being inalienable have to be considered. The controversy surrounding Facebook's use of the Beacon system[4] and more generally the use by social networking sites of personal information without the consent of individuals illustrates why any trade-offs between greater security and privacy must be subjected to regulatory oversight – the aim ultimately is to maintain an optimal balance between the

competing and at times conflicting interests. The key question that this paper addresses is what principles can industry and policymakers turn to when seeking to respond to security concerns whilst reflecting the values underpinned by the Data Protection legislation. We now have one set of principles which can assist businesses and identity management service providers. The Center for Democracy & Technology has recently released a draft version[5] of what it regards as key privacy principles for identity management in the digital age. This paper will provide an overview of the key benchmarks identified by the CDT. The focus of this paper is to explore how best the Data Protection Legislation can be said to provide a framework to ensure that a proper balance is maintained between "identity" conscious technology and an individual's expectation of privacy to personal and sensitive data. The Data Protection legislation provides the basis for achieving a balanced framework. The conclusion however is that securing compliance with the DPD will prove to be the biggest governance challenge – standard setting and norms will go some way to ease the need for centralized regulatory oversight.

2. Identity Management in Web 2.0

Imagine the life cycle of an individual's identity during the course of the day. He or she may login to his Internet service provider, run a range of applications, make purchases online, access social network sites and email accounts. A vast amount of information is likely to created by the individual – the content will reflect the multiple identities of the individual. The information may relate to the individual's status: a customer with a bank, a consumer, a user of products and services. The information may also relate to matters of reputation and intimacy. The operating system platforms and web applications will each have their own identity management processes. This individual may also be an employee of an organisation with the following authenticating system:[6]

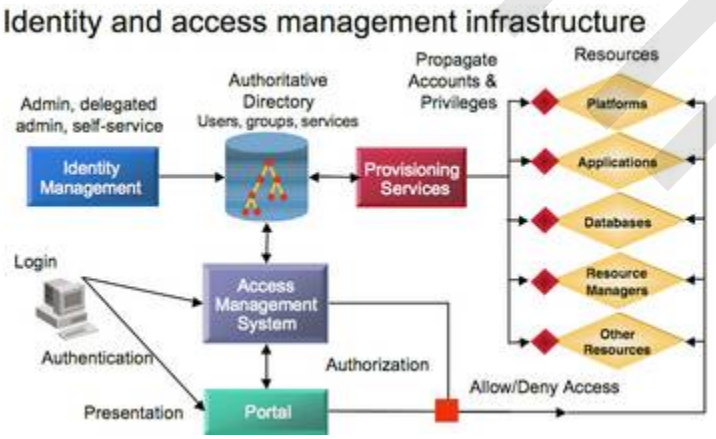

Figure 1: Identity and Access Management Infrastructure

The individual's 'identity' in this context is managed by the infrastructure set in place by the organisation. For example, data relating to the individual's identity is stored in a centralised directory. 'Identity aware' tools enable the organisation to determine access requests from the individual, undertake authentication and implement controls over the identity transactions. Updates or modifications to the individual's identity can also be addressed by the provisioning service component. For example, changes in bank account details, or expiry of access privileges or amendments to these can be addressed. It is customary to provide the user with a personalized platform interface so that relevant inputs can be made. Notwithstanding the usefulness of these innovations, an individual has multiple identities. The fact that the individual is employed by an organisation does not assist him when negotiating other identity related transactions. There are numerous instances of transactions requiring of the individual other attributes or digital identity. For example, a smart card that permits the individual to access the car park or building can be said to be concerned with one aspect of an identity, and could not similarly be used to purchase airline tickets online or books from an online publisher. An individual's identity can take a number of life cycles – sometimes having no connection with each other. The following illustrates the possession of 'trust constituting' credentials.

Figure 2: Ing Direct: Login

Identity management is not purely a security matter – it also involves managing expectations between the collector and the user.

What do these two examples of a hypothetical life cycle tell us about the deep seated tensions between 'security' and 'privacy? More importantly, how do we begin to construct a set of principles that provides a legitimate and pragmatic solution to the governance challenges? The former question can be quickly answered.

First, digitalised data processed by automated systems carry the risk of unauthorised persons gaining access to personal and sensitive data belonging to an individual. Second, there is no regulatory oversight both in respect of the collection and storage of data in identity management systems or for that matter ensuring that the data is not subsequently used for purposes without the consent of the individual. In both instances, issues of accountability, transparency and integrity needed to be confronted at the design, application and substantive level. It is beyond the scope of the objectives of this paper to deal with the architectural issues. But these issues can be addressed obliquely in the following illustration.

Consider as an example the governance challenges that stem from the fact that the data transmitted by 1.3 billion online users can be potentially tracked, manipulated and used by data controllers.[7] Yahoo Inc, for example, is reputed to make 110 billion collections on its web sites and also an estimated 1,709 other opportunities for collection at its disposal from sites where it has advertisement placements.[8] Data is commercially and strategically valuable. Companies such as AOL and Microsoft are positioning themselves to acquire online data silos. Google has received approval from the EU authorities over its proposed acquisition of DoubleClink Inc. DoubleClick Performics, which is the performance-based marketing division of DoubleClick Inc, provides online marketing services and technologies for multimedia marketers.[9] Its data collection strategy is designed to provide its clients with a comprehensive understanding of customers' knowledge and use of the Internet. Issues of interoperability and security now compete with the growing recognition of the commercial value of leveraging personal information.

The examples regarding the employment and the financial transactions and the value of data in one respect draws our attention to the relationship between an enterprise's needs and goals and the IT infrastructures that are instituted. The Yahoo example illustrates the broader context within which identity management issues operate.

Three observations can now be made before we address the issues raised by the guidelines issued by the CDT. First, we have multiple

identities. Second, identity management raises an important issue about the end-to-end architecture of the Internet. There is no identity layer. Digital identity is not readily amenable to a set of meta data or for that matter an agreed set of protocols that can be configured as a form of 'identity layer'. Third, as Kim Cameron[10] observes, the lack of agreement in terms of designing a meta-system for identity management reflects the fact there are complex trade-offs between identity, trust, security and convenience. The maintenance of trust, it is suggested, is an important aspect of data governance and identity management. The threats posed by privacy invasive technologies to trust and confidence is not new of course. As the World Summit on the Information Society noted:[11]

> Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

That said, identity management systems require us to reassess the privacy values we regard as being inalienable and challenges us to find optimal solutions to emerging governance challenges posed. How do we ensure that the systems of identity reflect the complexity and granularity of 'data' and multiple identities? The CDT identifies a set of principles that regards 'norms' rather than centralised regulatory frameworks as being the mechanism through which standards can emerge. The principles identified by the CDT[12] are consistent with the prevailing regulatory attitude towards the design of infrastructures that seek to maintain a balance between the creation of a robust system of identity management and privacy management. The publication of the privacy principles are, according to the CDT, aimed at government and commercial entities 'in developing programs or systems for the creation, authentication and use of identity.' The principles are divided into two categories: the umbrella principles of diversity and decentralisation, proportionality and architecture; and specific fair information practices, namely, purpose and use, notice, choice, security, accountability, access, and data quality.

A few words of explanation are needed to understand the CDT principles.

According to the principle of *proportionality*, the amount and type of information collected or stored by an identity system should be proportionate to the purpose for which the identity is created. Therefore, information that is collected beyond the purposes for which it was originally obtained would not be regarded as being proportionate. Similarly, information that has been obtained, but is subsequently used for another purpose without obtaining the user's consent can also be viewed as disproportionate. An example is *R v Department of Health ex parte Source Informatics* (1999) 52 BMLR 65 (CA) whereby patients' data in anonymised form were provided (without personal identifiers) to a pharmaceutical company *Source Informatics* without the patient's consent. Although the case dealt with the common law of confidence and whether personal information in anonymised form fell within the ambit of the common law of confidence, the processing of the data *for other uses* than was originally obtained could be argued to be disproportionate.[13]

The principle of *diversity and decentralization* is intended to illustrate the point that identity systems should be designed to exist in a marketplace offering multiple services that deliver varying degrees and kinds of identity creation, authentication and use. The CDT gave an example that accessing a health record would be different from accessing an e-mail account. This hinges on giving the consumer a choice. There is no similar principle under the current European Data Protection Framework.

On the principle of *individual control and choice*, this reflects the aim of enabling individuals to have to have reasonable control and choice over the attributes, identifiers and credentials that can be used within the identity systems.

As for *notice and consent*, individuals should be given a clear statement about the collection and use of identifying information. Again, this is similar to the European Data Protection Framework which requires an individual's unambiguous consent before personal data can be processed or an individual's explicit consent in the case of sensitive personal data (as defined under Art. 8(1) of the Data Protection Directive 95/46/EC).

The principle of *limited use* needs no further explanation. Personal information should only be used for specific, limited and disclosed purposes.

Regarding the principle of *onward transfer*, the CDT provides that 'any organization that handles identity information should include in its contracts provisions requiring that the entities with which identity information and linked information is shared will afford that shared data a level of protection consistent with or exceeding the organization's own

standards, consistent with these principles.' This principle is slightly different from the principle of transborder data flows as provided under Art. 25 of the Data Protection Directive 95/46/EC, which prohibits the transfer of personal data to non-EEA countries without an adequate level of protection (which can be satisfied by a Commission ruling to this effect or through binding corporate rules agreed by the company concerned). What would be clearer is the destination to which the personal data is transferred, and the likely remedies for the misuse of personal data transferred. The authors will discuss this in the context of the European Data Protection Framework.

The principle of *privacy and security* by design refers to factors that should be considered into an identity system including safeguards for the physical system components and policies and procedures that guide the implementation of the system.

Finally, the principles of *security, accountability and access*, *data quality* and *due process* are understandable without further discussion.

We can simplify the CDT statement of intent by reconceptualising the governance issue raised by identity management in the following terms. First, the design and implementation of identity management systems must be alive to considerations of efficiency. Users are unlikely to respond positively if the system requires excessive information and/or if there are interoperability issues, as might be the case if a user has to memorise a number of usernames and passwords. Second, the managing identity is about managing expectations and sustaining trust relationships. As Microsoft discovered, identity management must be user-centric and negative perceptions of the Identity service provider can impair the adoption of the technology.[14] Third, implementation of strategies must not overlook the fact that data cycles may have a life span and are always subjected to change. Flexibility, audit and updating are critical to ensure that a user is not denied his access rights. User control, and the amenability of identity management systems to next generation applications are an integral part in the creation of norms that become mainstream in the online community. Identity management is not an issue that can be divorced from the broader goal of the Information Society. Paragraph 44 for example notes that:

> Standardization is one of the essential building blocks of the Information Society. There should be particular emphasis on the development and adoption of international standards. The development and use of open, interoperable, non-discriminatory and demand-driven standards that take into account needs of users and consumers is a basic element for the development and greater diffusion of ICTs and more affordable access to them, particularly in developing countries. International standards aim to create an

environment where consumers can access services worldwide regardless of underlying technology.

Finally, the evolution of a user-centric identity management system is also dependent on service providers not only creating sound and secure systems but that efforts are made to inculcate in users an awareness that identity management is everyone's responsibility. Norms and standards take time to evolve and any successful outcome will require the issues raised by the 'security'-'privacy' dimension are identified and addressed in an impartial and objective manner. There have been a range of standard setting initiatives. The Markup Language for service provisioning provides standards for request and response and message exchanges (SPML).[15] A number of identity management service providers have provided security assertion markup language (SAML).[16] Organisations utilise these mechanisms for exchanging trust constituting credentials. The eXtensible Access Control Markup Language (XACML) is an encoded data exchange standard enabling organisastions to enforce access control policies. [17] The Liberty Alliance Project has been at the forefront of standard setting initiatives and particularly prominent in developing federated identity management services.[18] Standards for security token formats have resulted in the development of WS-* specifications and which have been supported by major identity management service providers like Microsoft and IBM.[19] A number of user-centric identity management initiatives are emerging: Light-Weight Identity (LID), OpenID and Yadis (Yet Another Decentralized Interoperability System.[20] The growing complexity of the web based services and applications, the emergence of the open source commons has important implications for the future of standard setting initiatives. Clearly there will need to be a threshold, where issues of security, privacy and convenience are negotiated. Single sign-ons (sso), auditing processes, and securing compliance with established privacy or data protection policies will ensure that minimal standards are maintained.

What follows below is an examination of the value of the EDPF as a standard setting framework for identity management which respects privacy principles.[21]

3. European Data Protection Framework

The European Data Protection Framework is good starting point to address the key critical issues as applied to the digital age. Although the Data Protection Directive 95/46/EC ("DPD") was enacted before the internet became the main medium for communication, the Directive has since been supplemented by the Directive on Privacy and Electronic Communications 2002/58/EC. The latter complements the DPD and applies to the processing of personal data in the electronic communications sector.

By way of background, the DPD was originally modelled on the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also influenced by the OECD), and its objective was to harmonise the data protection laws within the European Union. The main data protection principles can be found in Art. 6:

> 1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.

The definition of "personal data" is interpreted broadly under Art. 2(a) to encompass 'any information relating to an identified or identifiable natural person.' The Directive does not include legal persons, but countries including Austria, Italy, Luxembourg have extended their data protection laws to legal persons (Korff, 2002). The European Court of Justice's decision in *Lindqvist* further confirms the broad scope of this definition in its judgment:

> The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, *constitutes the processing of personal data* wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Directive places emphasis on the data controller(s) to ensure that the data protection rules are followed. Where special categories of personal data are involved (Art. 8(1) defines this as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life), there are additional requirements laid down under Art. 8(2) before processing can take place. For example, processing sensitive data is permitted if the data subject gives his explicit consent. Explicit consent is not defined in the Directive, but consent is given a wide definition under Art. 2(h) as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.' Germany has interpreted "explicit consent" to refer to written consent. UK, however, does not specifically require that consent be written and that implied consent, may, under specific circumstances be allowed. There is no uniform consensus amongst EU countries on this. Consent by silence, however, will not satisfy this requirement. This leads onto the next question whether identity management systems can adequately obtain the consent of the individual? Is the data subject aware that his personal information is being used for specified purposes? As I have argued in an earlier paper (2007), the application of sensitive data on the internet or even on computerized databases raises significant problems because an individual's name may reveal his/her ethnicity and thus, a higher standard of care is required to process this data. Secondly, data may become sensitive according to its context. For example, a list of individuals' names that when combined with other personal information shows that they belong to a trade union. The Directive does not address this for understandable reasons (considering the background of the Directive). However, it is an anomaly that the Directive on Privacy and Electronic Communications 2002/58/EC does not also tackle this issue, leaving the onus upon data controllers to decide what standards apply ie. Art. 7 (normal data) or Art. 8 (sensitive data). One should look at the contextualised approach when approaching the processing of sensitive data (Simitis, 2007) such that data could become sensitive data according to its context (Wong, 2007). A pressing issue is the transfer of personal data (normally referred to as "transborder data flows") in accordance with Art. 25 of the Data Protection Directive:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data

> transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
>
> 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
>
> 4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
>
> 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
>
> 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
>
> Member States shall take the measures necessary to comply with the Commission's decision.

This is relevant because personal information is regularly transferred by multinational companies beyond national borders to non-EEA countries such as India and China. Under those circumstances, the Directive requires that the transfer of personal information *can only* take place where the adequate standards are met:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Currently, India does not have data protection laws, but they have amended the *India Information Technology Act* 2004[22] to address the

question of off-shore processing of personal data. China is set to introduce privacy laws in 2008,[23] but whether this will be modelled on the European Data Protection Framework is less than clear.

4. The Directive on Privacy and Electronic Communications 2002/58/EC and the Data Retentions Directive 2006/24/EC

This leads to the next question on the application of Directive on Privacy and Electronic Communications 2002/58/EC and the Data Retentions Directive 2006/24/EC.

The Directive on Privacy and Electronic Communications complements the existing DPD and applies to 'providers of a publicly available electronic communications services in public communications networks in the Community'. This could be an internet service provider; mobile or telephone operator(s) using a publicly available electronic communications service. The key words are "*publicly available*" and therefore, private networks such as intranets could fall outside the scope of the DPEC. In the context of identity management systems, it would be quite difficult to identify that an identity management system data controller was also a provider of electronic communications services. However, in a hypothetical example, where an identity management systems data controller that was also providing internet access (as an internet service provider), then they may fall within the scope of Art. 3 (and is not simply a private network). On the basis that the identity management system data controller was a provider of publicly available communications service, they would be required to adopt technical and organisational measures as provided under Art. 4.1 DPEC. This states that 'publicly available *electronic communications service* must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with *the provider of the public communications networks* with respect to network security.' Art. 4.2 further states 'that the provider of a public available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.' This provision emphasises the CDT principle concerning the privacy and security of the system. The ISO standards/IEC 17799 is a recognised international standard that could be adopted by identity management system data controllers. The other provisions within the DPEC are not applicable in the context of Identity Management System Data Controllers and are therefore not considered in this article.

Finally, the Data Retentions Directive 2006/24/EC (DRD)[24] further adds another dimension to the Data Protection framework. The DRD

requires that providers of publicly available electronic communications services or of publicly communications network retain the data of the subscriber or registered user for a minimum of six months to a maximum period of two years from the date of the communication (Art. 6 DPD). Again, it would need to be shown that an identity management data controller was a provider of publicly available electronic communications service. Users are defined under Art. 2(b) as 'any legal entity or natural person using a publicly available electronic communications services, for private or business purposes, without necessarily having subscribed to that service.' The types of data to be retained are categorised under Art. 5. What is of more relevance is Art. 5(1)(a) data necessary to trace and identify the source of a communication; Art. 5(1)(b) data necessary to identify the destination of a communication; Art. 5(1)(c)(2) data necessary to identify the date, time and duration of a communication concerning internet access, internet e-mail and internet telephony. Member States could, by virtue of Art. 15.3 postpone the application of the retention of communications data relating to internet access, internet telephony and internet e-mail until 15 March 2009. Some of the Member States including the UK have postponed the retention of this data until then (see Art. 15.3 of the DRD).

It should be added that the DRD does not require the provider to retain the *content* of the communication (Art. 5.2 DRD) but rather the data to be retained originates, date identified, time and duration of the communication. A further provision is made of Art. 7 on the data security principles to be adopted.

The Data Protection framework (through the DPD, DPEC and the DRD) which has been implemented by individual Member States[25] complement the identity principles referred to above. The identity principles, however, further reinforces the notion of the identity of the individual through the use of identity management systems. However, there are a few notable differences. The Data Protection Framework provides remedies to individuals against organisations or individuals (as "data controllers") for not adhering to the DPD or the DPEC The application of the DPD is fairly broad with each Member State having implemented the DPD[26] and the DPEC into their own national laws. Furthermore, the Data Protection Authorities oversees the application of the data protection laws within their own Member States.

5. Improving the CDT Principles

The CDT principles would complement the Data Protection Framework, in providing clearer guidelines on what identity management data controllers would need to do to protect the identity of individuals. A further issue is the protection of *multiple identities* of an individual, who may be known as X in one identity management system, but may be

known by a pseudonym in another identity management system. It was acknowledged by the CDT's paper on *Privacy Principles for Identity in the Digital Age* that in a 'networked world the urge to link identity systems and databases together will always exist…Linking should occur in cases where its specific benefits exceed the associated privacy and security risks. When linking is deemed necessary, *strong safeguards* should be erected to ensure that unnecessary linkages do not occur (emphasis added).'

The subject of multiple identities is not specifically addressed in the DPD, but the notion of "personal data" under the DPD is sufficiently broad to encompass any 'information relating to an identified or identifiable natural person' and thus, multiple identities would fall within the scope of the DPD.

The CDT principles could be strengthened if these principles were not only embraced by identity management system data controllers, but also there was a body overseeing the application of these principles. The work of the Data Protection Authorities could be a starting point not only in highlighting the national data protection laws that apply, but also how it applies to identity management systems at a European level.[27]

6. Conclusion

As identified in this paper, the CDT principles are a good starting point when tackling the collection and storage of personal information held in identity management systems. *The question is the application of identity management systems to the online environment.* Art. 4 of the DPD is fairly clear about the application of data protection laws in particular domestic settings. That said, practical and conceptual issues may have to be confronted when identity system management systems co-exist in Member States and non--EEA jurisdictions. In addition to the choice of law issues, the mechanisms for securing compliance with established data protection principles must be put in place. In which case, each Member State's data protection laws could be applicable or in the case of non-EEA data controllers that make use of "equipment" to process personal data unless this was used for transit purposes. The over-reaching effect of the Data Protection Directive 95/46/EC to non-EEA data controllers does lay itself to particular difficulties in terms of enforcement. Under those circumstances, the work of the National Data Protection Commissioners would be a good starting point. The European Data Protection Framework is, however, relevant when considering whether personal information held in Identity Management Systems is collected within Europe. The Data Protection Directive places an onus on EU data controllers to adhere with the relevant national data protection laws that apply. Oversight of the Data Protection Laws is further supported by the work of the European Data

Protection Authorities. The issue is not whether there is the legislative framework to support the protection of an individual's identity in identity management systems. The current framework can provide the support and the necessary remedies (in instances of breach) for individuals whose personal information (be it in the form of profiles or pseudnonyms) are held on these systems. An important factor will be how robust these systems are in securing the personal information of individuals and the choice provided for individuals to control their own identity. Art. 17 of the Data Protection Directive 95/46/EC lays emphasis on the technical and security measures adopted by data controllers, but other than security measures, user awareness and the ease with which their profiles are easily managed from identity management system will be an important factor. Furthermore, it should also be added that the data protection principles laid down under the Data Protection Directive 95/46/EC should continue to be upheld but as Peter Hustinx, the European Data Protection Supervisor[28] indicated, when considering the existing Data Protection Framework, it is not existing data protection principles that need to change, but rather how the Data Protection Framework could be made more effective. There is still some way to go over the protection of identity. It is not so much as regulation, but rather a clearer understanding over the broad application of the current European data protection framework. The CDT goes some way to demonstrate how this will work. The challenge is for Data Protection Authorities to take this onboard and ensure that there is sufficient guidance for industry and consumers alike.

References

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63

Jay, Rosemary and Angus Hamilton (2002), *Data Protection Law,* 2nd ed. Sweet and Maxwell, London.

Kuner, Christopher, (2007) *European Data Protection Law: corporate regulation and compliance*, 2nd ed., Oxford University Press, Oxford.

Center for Democracy and Technology. *Privacy Principles for Identity in the Digital Age*, v1.4 December 2007 (http://www.cdt.org/security/identity/20080108idprinciples.pdf).

---

[1] CDT. *Privacy Principles for Identity in the Digital Age* (draft version 1.4 (http://www.cdt.org/security/identity/20080108idprinciples.pdf), Dated December 2007.

[2] *Symantec Internet Security Threat Report*, September 2007 (http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf), September 2007.

[4] Facebook Beacon at http://www.facebook.com/business/?beacon; Solove, D. *Facebook's Beacon, Blockbuster and the Video Privacy Protection Act* http://www.concurringopinions.com/archives/2007/12/facebooks_beaco_1.html; Dated December 10, 2007; *Is Facebook Beacon a Privacy Nightmare?* http://gigaom.com/2007/11/06/facebook-beacon-privacy-issues/; Davis, Wendy, *Blockbuster sued for participating in Facebook's Beacon programme Blockbuster Sued For Participating In Facebook's Beacon Program* http://publications.mediapost.com/index.cfm?fuseaction=Articles.san&s=80839&Nid=41637&p=918739;

[5] CDT. *Privacy Principles for Identity in the Digital Age* (draft version 1.4 (http://www.cdt.org/security/identity/20080108idprinciples.pdf), Dated December 2007.

[6] J Lewis, *The Emerging Infrastructure for Identity and Access Management.* Open Group In 3 Conference. January 2002. < http://www.opengroup.org/security/lewis.pdf

[7] L Story, "Web companies track users' Internet activity hundreds of times per month", International Herald Tribune, March 10, 2008 (accessed on 11 March, 2008) available at http://www.iht.com/articles/2008/03/10/technology/privacy.php.

[8] *Ibid.*

[9] *DoubleClick Performics* available at www.performics.com

[10] K. Cameron. *The laws of identity* available at http://www.identityblog.com/?p=352.
Dated 8 January 2006.

[11] World Summit on the Information Society (WSIS), Declaration of Principles, *Building the Information Society: a Global Challenge in the New Millennium*, http://www.itu.int/wsis/docs/geneva/official/dop.html.

[12] CDT. *Identity Principles* available at http://www.cdt.org/security/identity/20080108idprinciples.pdf.

[13] Beyleveld, D. and E. Histed. "Betrayal of Confidence in the Court of Appeal", *Med. L. Int.* (2000) 4, Parts 3/4, 277-311.

[14] Microsoft Live ID available at

https://accountservices.passport.net/ppnetworkhome.srf?vv=550&lc=2057 ; Bowman, L. M. *Microsoft defends passport privacy* available at https://accountservices.passport.net/ppnetworkhome.srf?vv=550&lc=2057 .

[15] *Service Provisioning Markup language* available at http://www.service-architecture.com/web-services/articles/service_provisioning_markup_language_spml.html

[16] See *Security Assertion Markup Language* available at http://en.wikipedia.org/wiki/SAML and http://www.microsoft.com/presspass/press/2004/may04/05-25IMVRallyPR.mspx

[17] *XACML: A New Standard Protects Content in Enterprise Data Exchange* http://java.sun.com/developer/technicalArticles/Security/xacml/xacml.html

[18] *Liberty Alliance Strategic Initiatives* http://www.projectliberty.org/liberty/strategic_initiatives

[19] http://en.wikipedia.org/wiki/WS-* and IBM, *Web Services Policy Framework* http://www.ibm.com/developerworks/library/specification/ws-polfram/

[20] See *LID Features and Benefits* http://lid.netmesh.org/wiki/LID_Features_and_Benefits, *Open ID.net* http://openid.net/, http://yadis.org/wiki/Main_Page and *Marco Casassa Mont's* "*Research on Identity* Management" Blog http://h20325.www2.hp.com/blogs/mcm/archive/0001/01/01/2680.html.

[21] When discussing the European Data Protection Framework, the authors are primarily referring to the Data Protection Directive 95/46/EC; Directive on Privacy and Electronic Communications 2002/58/EC and the Data Retentions Directive 2006/24/EC.

[22] Indian Trade Body sets up a trade body group

(http://www.out-law.com/default.aspx?page=8149) and Debasis Nayak (Amen!)dments to the Information Technology Act (http://www.networkmagazineindia.com/200702/focus01.shtml)

[23] EU-China Information Society Project: Research Final Workshop: "Personal Data Protection" available at http://www.eu-china-infso.org/Regulation/regulation094158@2007-06-20.html.

[24] The full title is *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, OJ L 105, 13.4.2006, p. 54–63

[25] European Commission. Transposition of the Directive (http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm), Last accessed 9 March 2008.

[26] *Ibid.*

[27] See the work of Liberty Alliance available at http://www.projectliberty.org/ and the European Commission Project, PRIME at https://www.prime-project.eu/.

[28] Out-law news. *Privacy laws should be overhauled, says European regulator* available at http://www.out-law.com/page-8623. Dated 9 November 2007.