Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation

February 23, 2005

Editor
Stephen Deadman, Vodafone

Contributors
Luc Mathan, France Telecom
Christine Varney, Hogan & Hartson LLP
Jeff Hodges, Neustar
Paul Madsen, NTT
Joe Alhadeff, Oracle
Piper Cole, Sun Microsystems
Stephanie Manning, Vodafone

Abstract:
This paper supplements the Privacy and Security Best Practices paper first released in 2003, and focuses on some of the implications of EU data protection and privacy law for organisations implementing the Liberty identity federation and Web services frameworks and specifications and seeking to establish robust and trusted business frameworks for federated communities, or

'Circles of Trust'. This paper also supplements the Liberty Business Guidelines (Raising the Business Requirements for Wide Scale Identity Federation), which provide guidelines for businesses seeking to establish Liberty-based Circles of Trust (CoTs). In particular, this paper focuses on the implications for the development of the underlying legal and contractual framework.

This paper should be of relevance and assistance to all organisations deploying Liberty-based technology and seeking to establish the necessary business frameworks in, or partly in, the EU. It should be of particular relevance to those organisations' privacy or data protection officers and their legal advisers, plus the relevant business managers responsible for establishing the commercial and business framework for Liberty deployments.

Within the EU, there are two Directives in the data protection and privacy field that will be of relevance to the activities of most participants of CoTs. These Directives regulate a number of categories of data or information and place specific obligations or restrictions on those who handle this information. Further, the Directives allocate compliance responsibilities according to the 'role' that any given participant is performing. Consequently, participants of the CoT will need to address the types of data that are being handled, what role they are performing in the CoT in respect of this data and, consequently, what obligations or restrictions this places upon them.

The Directives are likely to have a direct impact upon the necessary legal and contractual framework for a CoT. The CoT participants may be required to enter into particular types of agreements between each other. These will be dependent upon *who* is performing which role, *what* data they are handling and for *which* purpose, and *where* that data may be transferred. Addressing the *who*, *what*, *which* are *where* of the CoT is therefore an essential first step in developing the contractual framework. This paper provides guidance on each of these elements and highlights the potential impact upon the structure and terms of the contractual arrangements for a CoT.

Of course, different CoTs will often give rise to different conclusions regarding the impact of data protection and privacy law, depending upon the business sector, type and purpose or the CoT and relationship between participants, and this paper can only provide general guidance. At the end of each main section there are a number of questions intended to highlight relevant considerations and that will need to be answered by organisations seeking to establish a Liberty-based CoT.

The EU's approach to privacy and data protection regulation has also become an important international standard and may be useful as a reference to CoTs outside the EU.

Throughout this paper there are a number of 'exhibits' which describe potential deployments of Liberty technology and demonstrate how the legal principles discussed could have an impact on the participants of the CoT and the contractual framework.

Table of contents

Table of Exhibits

DISCLAIMER

This paper is provided for general information purposes only and does not constitute legal advice (or any other type of advice) and should not be relied on for this purpose. The Liberty Alliance is providing the information in this paper in good faith but no warranty or representation is given that the information is accurate, complete or up to date. Use of information from this paper is at your own risk. If you have a specific question on the subject matter of this paper, the Liberty Alliance Public Policy Expert Group will be pleased to assist you. If you require legal advice, please seek the advice of your legal adviser. Please also note that many of the examples and illustrations used relate to roles and obligations that are both fact specific and will be dependent on national implementations of the Directives.

1 Introduction

Establishing the legal framework for a federation of organisations implementing an identity management system based on the Liberty identity federation and Web services frameworks and specifications is a complex task. It requires an appreciation of the nature of the many different relationships between the parties and the various interactions between them. It also requires an understanding of the legal and regulatory environment, in particular privacy and data protection law. As the basis for addressing the wider legal issues for establishing a legal framework, this paper examines the implications of EU data protection and privacy law and the particular impact that this will have upon the structure and nature of that legal framework.

For the consumer, identity, particularly in relation to the Internet and electronic communications, is bound up with concerns about privacy and data protection. One of the greatest threats to privacy is the ability for organizations using information technology to accumulate large amounts of information about individuals, in a manner that is less obvious to consumers. Information in a digital form can facilitate the manipulation, alteration and communication to others very rapidly and at low cost. This was recognized from the very early stages of the development of computers and information technology, and led to the development at the international level of guidelines and legislation intended to ensure that these concerns were safeguarded[1]. Building upon this foundation, the EU began the process in the early 1990s of developing a comprehensive legal framework to regulate the processing and use of personal data and protection of privacy. Elsewhere, dozens of countries around the world have also developed data protection and privacy laws. In the US, apart from a Constitutional right to privacy, there has been a steady stream of sector specific legislation at the Federal level since the 1970s. More recently at the regional level, Ministers representing the APEC economies endorsed the APEC Privacy Framework[2]. The Framework promotes a consistent approach to information privacy protection across APEC member economies (21 in total including Australia, China, Japan, Mexico and the US), and is based upon the OECD Guidelines (see footnote 2), thus sharing a common heritage with EU data protection and privacy law.

1.1 Circles of Trust

The Liberty Alliance defines a Circle of Trust (CoT) as a federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment[3]. As federated communities create inter-dependencies and, consequently, the need for trust between participants, the CoT is viewed by the Liberty Alliance as an essential component of establishing a system of federated identity based on Liberty specifications. The CoT therefore creates a trusted framework for both the participating service providers and identity providers but, perhaps most importantly, the consumers, employees or end users whose identity is often the subject of federation.

The structure and nature of the legal framework will vary, depending upon the nature and scope of the CoT, i.e. business sector, type and purpose. Small single purpose federations made up of a small number of relatively static business partners may require a relatively light framework negotiated between the partners. There may be existing legal agreements or structures upon

[1] Some of the major international instruments in this field are as follows: OECD Guidelines on the protection of privacy and transborder flows of personal data (1980) (the "OECD Guidelines"), Council of Europe Convention for protection of individuals with regard to automatic processing of personal data (1981) (the "COE Convention"), OECD Declaration on transborder data flows (1985) (the "OECD Transborder Flows declaration"), Ministerial declaration on the protection of privacy on global networks (1998) (the "OECD Global Networks declaration"), OECD Guidelines for the Security of Information Systems and Networks (2002) (the "OECD Security Guidelines").

[2] See 20 November 2004 APEC Media release:
http://www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html

[3] See the Liberty Glossary at: https://www.projectliberty.org/specs/draft-liberty-glossary-1.3-errata-v1.0.pdf

which this legal framework can be built; an enterprise CoT may have existing mechanisms for dealing with security and other requirements and for enforcing these (e.g. internal corporate policies, enforceable undertakings or internal contractual arrangements); certain business alliances may have an established network of relationships which may be used as a foundation (e.g. the mobile GSM roaming community).

As CoTs develop and seek to encompass a larger number of participants from a wider range of economic spheres, existing structures are less likely to be of assistance as the foundation for the legal framework. Larger and more dynamic CoTs will also likely have a greater turnover of participants joining, leaving and changing roles, which will create further challenges. Consequently, the CoT will need to establish federation-wide rules and common operating procedures and processes. Simplifying and standardizing the process and rules of participation can minimize the problems of bi-lateral negotiations and multiple contracts with many inter-dependencies.

Regardless of the nature and scope, the starting point when seeking to establish a legal framework for a CoT or federated community within, or partly within, the EU is to identify the core requirements in the field of privacy and data protection law. This will identify the legal nature of the relationships between participants, their respective obligations and the extent of their reliance upon one another for the secure and lawful functioning of the federation. On this foundation, a legal framework can be built. This legal framework will likely need to comprise a mix of contractual duties and obligations, business and operating rules, policies, technical mechanisms and other elements.

1.2 Privacy and anonymity

It has long been acknowledged that the online world is fundamentally different from the offline world in that wherever we go in the online world we can leave more permanently and less obviously recorded digital traces, such as Web pages visited, content consumed and communications made with others. These digital traces may reveal our identity and enable the creation of detailed profiles of our activities and associations. Policy makers therefore recognize the need to provide the ability to interact, browse, and transact anonymously in similar circumstances to the offline world[4].

The creation of identity management frameworks and federated communities is intended, among other things, to enhance the speed and convenience of online interactions and transactions, through features such as single sign-on. Mechanisms are being designed specifically to enable the discovery and sharing of information about individuals within federated communities. If these mechanisms are not designed with privacy in mind, they could further erode the individual's privacy and control over their personal information.

Privacy has been a driving influence of the Liberty Alliance since its foundation and was the primary reason for forming the Public Policy Expert Group and publishing the Privacy and Security Best Practices[5]. The Liberty Alliance's federated identity framework provides an important means for individuals to link information about themselves held by different entities in a way that avoids the creation of a single unique identifier. While this cannot guarantee anonymity (this will always be a matter for individual service providers), it does provide the tools for CoTs to ensure that identity federation minimizes the creation of an ever-expanding pool of interconnected personal information. In addition, the Liberty Alliance's Web services framework provides for the discovery and sharing of attributes with built-in mechanisms to provide individuals with control over the use and dissemination of their personal information.

[4] See the European Commission's Recommendation on Anonymity on the Internet adopted 3 December 1997: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1997/wp6_en.pdf

[5] The Privacy and Security Best Practices document is available at https://www.projectliberty.org/about/whitepapers.php

Nevertheless, the right implementation and deployment of these tools is the responsibility of the entities comprising the CoT.

1.3 The European perspective

EU law provides the framework for examining the impact of privacy and data protection law of its Member States on the establishment of CoTs. Inevitably, any discussion of EU law is subject to the caveat that the precise implications often depend upon how EU principles have been implemented by the Member States[6]. Nevertheless, this approach is still beneficial, as the broad framework should not vary substantially. Indeed, it will often be essential to adopt an EU-wide perspective, as many CoTs will be expected to span political borders. However, EU law also provides a useful benchmark and, in a number of respects, extends beyond the boundaries of the EU. As a consequence, the EU's approach to privacy and data protection regulation has become an important international standard and may also be useful as a guide to CoTs outside the EU. More directly, non-EU participants in a Liberty deployment that includes EU participants will need to understand the legal framework that informs how the EU participants may share or disclose information about a principal, and how the relationships between the EU and non-EU participants need to be arranged in order for the EU participants' legal obligations to be met.

More particularly, this paper examines the two primary EU Directives in the data protection and privacy field relevant to the electronic communications sector – the Data Protection Directive (DPD)[7] and the Electronic Communications Privacy Directive (ECPD)[8]. It does not seek to provide a comprehensive overview of EU data protection and privacy law, but attempts to draw out those elements relevant to the establishment of the legal and contractual framework underpinning a CoT by virtue of the nature of Liberty technology and what it is enabling businesses to do. Of course, in addition to privacy and data protection requirements, there will be many other legal requirements for establishing Liberty-based CoTs, and these will vary depending upon the precise nature and purpose of the CoT, the potential diversity of legal systems and rules concerned, business sectors, participants, types of transactions and use case scenarios involved. Therefore, contractual structures, recommended legal terms, specific issues relating to liability and risk allocation are out of scope. This paper is intended to be applicable to a wide range of business sectors, although some examples are taken from particular sectors.

1.4 Applicable references

The reader is assumed to be familiar with the Liberty ID-FF and ID-WSF frameworks and ID-SIS specifications. The published specifications under ID-FF, ID-WSF and ID-SIS can be found at http://www.projectliberty.org/specs/, along with implementation and business guidelines, policy documents and related materials at www.projectliberty.org. In particular, this paper is intended to supplement the Business Guidelines (Raising the Business Requirements for Wide Scale Identity Federation – https://www.projectliberty.org/resources/whitepapers/LibertyBusinessGuidelines.pdf) which provide general guidelines for businesses seeking to establish Liberty-based CoTs, and the Privacy and Security Best Practices guidelines (available at https://www.projectliberty.org/about/whitepapers.php), which provide an overview of international privacy and security principles and laws and recommended best practices.

[6] For details of the divergences in implementation of the Data Protection Directive, see the Commission's First Report on the implementation of the Data Protection Directive, available at http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm

[7] 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 (*Official Journal L 281, 23/11/1995 P. 0031 - 0050*)

[8] 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 (*Official Journal L 201, 31/7/2002 P. 0037 - 0047*)

2 Scope of EU data protection and privacy law

The DPD and the ECPD both apply to the processing[9] of personal data, and in the case of the ECPD, to other aspects of privacy. However, the scope of the EU Directives does not extend to state and public security, defence, and activities of the state in the area of criminal law[10]. In most cases, the exclusion of these activities will not have any relevance to commercial entities. Also excluded from the scope of the DPD (but not the ECPD) are activities of a purely personal or household nature. While this means that the activities of individuals using Liberty enabled services in the ordinary course of their private lives may fall outside of the scope of data protection law, the activities of the commercial entities involved will still be caught.

Another important issue, particularly where participants in a CoT span political borders, is the question of the applicable law and the potential extra-territorial effect of the DPD. The key principle under the DPD is that the national provisions adopted by EU Member States shall apply to the processing of personal data where the processing is carried out by a "controller" (see section 5.2 below for an explanation of the meaning of this term) established on the territory of a Member State (or, if not established on the territory, where its national law applies by virtue of international public law). If the controller is established on the territory of more than one Member State, then the applicable law shall be the law of the Member State on which each part is established[11].

Importantly, even if the controller is *not* established on any Member State's territory, a Member State's law may still apply if the controller makes use of equipment situated on the territory of a Member State (other than simply for transit)[12]. Consequently, certain types of remote access to personal data on EU users' PCs or other terminal devices could subject the entity engaging in this activity to the data protection laws of the country where the user's terminal is situated. The impact of this aspect of EU data protection law may be largely unknown to non-EU companies, yet its impact on participants in an international CoT could be significant.

3 Creating a compliant framework

In the vast majority of cases, the EU Directives are likely to apply to the activities of most EU based participants of a CoT. Participants will therefore need to ensure, as a minimum, that they can achieve compliance. Some of the key areas for any CoT to consider are as follows:

- What 'role' are the participants in any given CoT playing within the scheme of the EU Directives?
- What legitimate grounds do participants have within the scope of the EU Directives to process personal data?
- What are the minimum security obligations that apply and which participants bear the burden of compliance?
- Is there any transfer of personal data outside of the EU?

[9] The term "processing" is defined extremely broadly – it covers collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying personal data. Indeed, it is difficult to identify many activities that are not caught within its terms, and this is the manner in which the term should be understood (Article 2(b) DPD)
[10] Article 3 DPD
[11] Article 4.1(a) and (b) DPD
[12] Article 4.1(c) DPD

Before examining these questions, however, the first issue is to identify the types of information that are to be processed by the CoT participants. This is an essential first step, as many of the regulatory requirements discussed here only become operative where certain types of information are being processed.

4 Categories of information

Under the DPD and the ECPD, there are essentially four categories of information that are specifically protected: personal data, sensitive personal data, traffic data and location data. The latter three categories are subsets of 'personal data', while 'traffic data' and 'location data' are overlapping categories. Each of these categories may encompass a principal's identity and/or attributes and is discussed below. The rules governing the processing of each category of information vary and are discussed in section 6 below.

4.1 Personal data

The DPD defines personal data to mean any information relating to an identified or identifiable natural person[13] (i.e. the "data subject" – see section 5.1 below for further discussion). This therefore excludes companies, incorporated entities and other 'non-natural' persons. Under the Liberty framework, the data subject will often equate to the principal.

There are two important elements to the definition of personal data that should be considered. Firstly, does any particular data "relate to" an individual? Secondly, is the individual either identified or identifiable?

4.1.1 Data relating to an individual

The information in question must *relate* to an individual. While there is little guidance on this specific requirement, it may simply act to exclude information that contains a passing reference to an individual (e.g. information in the body of an email or SMS). Other than this, it seems likely that a great deal of information that identifies an individual will also 'relate to' them in a meaningful sense. In the UK in 2003, the Court of Appeal considered the specific issue of when data can be said to "relate to" an individual[14]. In essence, the court determined that information relates to an individual if it "…is information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity". In determining this issue, the court recommended two notions that might be of assistance. Firstly, is the information "… biographical in a significant sense, that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations…"? Secondly, does the information "… have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest…?". In response to this decision, the Information Commissioner, the UK's privacy authority, issued guidance on the interpretation of personal data in the UK's Data Protection Act (which implements the DPD in the UK) in May 2004[15]. While this is a national court decision, the judgment and the Information Commissioner's response nevertheless provide guidance which should be of relevance and interest to other EU jurisdictions[16].

What should be apparent from this brief summary is that in many instances in which data is being processed within a CoT, the information in question will certainly relate to an individual, as the primary purpose will often be to enable a principal to federate accounts, enjoy the convenience of

[13] Article 2(a) DPD
[14] John Durant v Financial Services Authority [2003] EWCA Civ 1746
[15] See: http://www.informationcommissioner.gov.uk/eventual.aspx?id=5152
[16] This may not be end of the matter; the European Commission sent a letter of formal notice to the UK Government in 2004 about the conformity of several aspects of the Data Protection Act 1998 with the DPD, believed to be as a result of the Durant decision.

single-sign-on, facilitate transactions to which they are a party or to enable the exchange of attributes concerning a principal.

4.1.2 Identity and identifiability

The other key element in the definition of personal data is that the individual must be *identified* or *identifiable*. This is an important issue for any identity management framework. However, the legal meaning of identity and identifiability may not be the same as what is commonly understood by these terms.

An 'identified' natural person is likely to mean an individual that is identified *by the information in question*, for example, a person's full name and address. This perhaps most closely relates to what many people would think of as one's 'identity'.

The meaning of an 'identifiable' person in the DPD is explained to mean one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to a person's physical, physiological, mental, economic, cultural or social identity. The focus of this definition on the criterion of direct or indirect identifiability (i.e. on the potential of information to facilitate identification of a person) makes it capable in theory of encompassing much data that *prima facie* would not ordinarily enable a particular person to be identified. Therefore, data may be "personal" even if it allows a person to be identified only in combination with other auxiliary data that is reasonably likely to be available to or come into the possession of the person processing the data.

The UK's Information Commissioner has issued general guidance on the UK's Data Protection Act 1998[17] which specifically addresses the issue of what it means to be identified: "*If the information about a particular web user is built up over a period of time, perhaps through the use of tracking technology, with the intention that it may later be linked to a name and address, that information is personal data. Information may be compiled about a particular web user, but there might not be any intention of linking it to a name and address or e-mail address. There might merely be an intention to target that particular user with advertising, or to offer discounts when they re-visit a particular web site, on the basis of the profile built up, without any ability to locate that user in the physical world. The Commissioner takes the view that such information is, nevertheless, personal data. In the context of the on-line world the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others*". It is clear from this statement that a great deal of information could be caught within the definition of personal data.

Consequently, the types of data that are likely to amount to personal data are much broader than simply name and address data. Indeed, in the online environment, name and address data are usually less important than other data such as IP addresses, mobile numbers, account numbers, and other unique identifiers. Similarly, the use of pseudonyms, which remove an element of identifiability, are unlikely to prevent information amounting to personal data where the pseudonym is simply used as an alternative identifier. Questions of whether or not any particular information is personal data cannot be looked at out of context (theoretically, all information may be capable of being linked). The better view is that it must be considered in the context of particular processing operations being carried out by a particular entity or entities.

4.1.3 Common identifiers

The architecture of the Internet, the Web, domain name system and other communications networks is such that there are a number of common identifiers used by organisations. Here are some of the most common:

[17] Available on the UK Information Commissioner's website at: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%201998%20Legal%20Guidance.pdf

4.1.3.1 Email addresses

Any email address that comprises the whole or part of a person's natural name (e.g. santa.claus@northpole.com) is likely to be personal data. Not only does it reveal the person's natural name, but also possibly the company they work for and sometimes also the country in which they are based. However, even an email address that does not reveal a person's natural name may still be personal data if it becomes a unique identifier for the user. Obviously, use of anonymous re-mail services may conceal the sender's identity from the recipient, but not from the email service provider.

4.1.3.2 Network addresses

While accessing resources over the Internet, a user's PC is identified by a single numerical IP address. The IP address can be static or dynamic depending on the type of Internet connection (e.g. by using a permanent ADSL connection or a dial up modem). With the introduction of IPv6, which will make sufficient IP addresses available for every user, it seems likely that at some point static IP addresses will become far more common. A fact specific analysis is, of course, required since a terminal in an Internet café or library may be considered in a different fashion to a personal PC with only one user.

Internet access providers will often be able to link the IP address assigned to an account holder to the account holder's subscription information, thereby identifying the account holder who may also be the primary user. In those circumstances, the IP address processed by the Internet access provider is likely to constitute personal data (assuming the account holder is a natural person). Where the IP address is static, then the processing of the IP address by other organizations may also amount to the processing of personal data, even if they are unable to identify the real name or postal address of the account holder or user.

In the mobile environment, the two key items of network identification data are the IMSI (International Mobile Subscriber Identity) and the MSISDN (Mobile Station International Services Digital Network) numbers. The IMSI is the number that identifies the mobile subscriber on the transmission path through the mobile network. The identity is stored on the Subscriber Identity Module (SIM), as well as in the mobile network. The MSISDN is the directory number that is used to reach a particular subscriber. It is determined by the national number plan, and is ultimately derived from the ITU numbering plan. MSISDN numbering ranges are distributed by national regulatory authorities to mobile network operators, who in turn may distribute them to their mobile service providers (i.e. resellers, where the mobile network operator operates a wholesale business), and finally to the subscriber (either by the mobile network operator or the mobile service provider). The design and format of the MSISDN is standardised. However, due to mobile number portability, it may not be possible to determine details, such as the subscriber's network, from the number itself.

Both the IMSI and MSISDN are identifiers, although they are used in different ways by different entities. The IMSI is used by mobile network operators to identify their subscribers when providing network connectivity and is the identifier that is used between mobile network operators when subscribers roam between networks. However, the MSISDN is the number that is visible and is often the identifier used by mobile network operators, and content and application providers to identify subscribers for providing various services.

Some national privacy authorities have already identified IP addresses as personal data. In 2004[18], the Spanish Data Protection Agency issued a report on the possible identification of Internet users through static or dynamic IP addresses[19]. The Agency determined in its report that ISPs and local network administrators can identify, using reasonable means, Internet users to whom they have previously assigned IP addresses. An ISP that has a contract with an Internet subscriber normally maintains a log file with the IP address (static or dynamic) assigned, the identification number of the subscriber, the date, time and the duration of the address assignment. Consequently, an Internet user can often be identified. The Agency concluded that, even though it is not always possible by using an IP address to identify a user, IP addresses should nevertheless be considered personal data. The reasoning applied by the Spanish Agency, as well as that provided by the UK's Information Commissioner (see section 4.1.2 above), is capable of being applied to other network identifiers, such as the IMSI and MSISDN, and to other unique identifiers which enable the creation of profiles, even if there is no means to communicate with the individual concerned.

An important point to be made here is that network identifiers are also used to identify machines, rather than natural persons, e.g. vending machines connected to a network. In such cases, the identifier will not likely be personal data, as there is no particular person to whom the data relates.

4.1.3.3 Cookies

Essentially all Web browsers are capable of reading HTTP cookies. The intended function of cookies is to supplement Web protocols with state management (or session) capabilities. Cookies can be transient (used just for the lifetime of the browser session) or persistent. A persistent cookie is saved to permanent storage so that it is available the next time the user starts a new session using their Web browser. Persistent cookies are often used in order to uniquely identify a user on a subsequent visit to a website and may also store other personal information relating to the user, such as pages viewed, e-mail address, user ID, which advertisements the user has clicked on *etc*. Depending on the type of information the cookie contains, a cookie may be considered personal data. The UK Information Commissioner's guidance above on the meaning of personal data would also apply to the use of cookies, particularly where used to create profiles and to personalise services.

In each of the examples above, an important question from the perspective of Liberty-based CoT participants is whether the identifier concerned, in the absence of any other data that enables the further identification of a subscriber or user, is personal data. The language of the DPD appears to be capable of applying to these common identifiers on their own, as in many cases they may relate to a specific identifiable natural person (i.e. the subscriber or primary user). In respect of network addresses specifically, the availability of IPv6 and the spread of mobile number portability may, in some circumstances, increase this likelihood as the connection between subscribers and their numbers becomes more permanent.

Even where data does not have a uniquely identifying characteristic, it may be "personal data" if it allows a person to be identified in combination with other auxiliary data that is reasonably likely to be available to or come into the possession of the person processing the data. Questions of whether or not any particular data is personal data will therefore depend as much upon the entity

[18] See the Spanish DPA's report (in Spanish): https://www.agpd.es/index.php?idSeccion=390
[19] In 2002, the European Commission's Article 29 Working Party published an opinion on the use of unique identifiers in telecommunications terminal equipment, using the example of IPv6 (http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp58_en.pdf), and which also declared that IP addresses attributed to Internet users are personal data under the DPD

that is processing the data, and the other data that that entity has, or has a reasonable prospect of obtaining or having access to, as any assessment of the data itself. Therefore, any determination of whether or not any given information amounts to personal data is highly context specific and will need to be addressed by the CoT both at the outset and throughout its lifecycle.

The Liberty Web services framework enables the discovery and exchange of attributes between entities utilizing Liberty protocols. In some cases, these attributes may be personal data (by virtue of their identifying characteristics), and in other cases they may be the auxiliary data referred to above, which in combination with other data may amount to personal data.

4.2 Sensitive personal data

Certain special categories of personal data, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as data concerning health or sex life (referred to here as "sensitive personal data"), are considered to be particularly sensitive, and are subject to stricter rules on processing (see section 6.1.2 below)[20]. It should, however, be noted that a number of Member States go beyond this list and include other categories of data that are to be treated as sensitive.

This list may appear quite limited in scope and application. However, there may be many types of data or attributes that are caught by this definition. A popular example is of the airline that keeps a record of frequent flyers' meal preferences; if certain customers have indicated that they require Kosher or Halal food, this is a good indication of their religious beliefs and such information may therefore be considered sensitive personal data. Similarly, if a service provider retains logs of customers' Web site visits, and these logs indicate the nature of the content contained on those sites, this may also be sensitive personal data if it reveals information relating to the data subject on the subject areas listed above.

4.3 Traffic data

Under the ECPD, traffic data means data that is processed for the purpose of the conveyance of a communication (i.e. data as well as voice communications), or for the billing of such communications[21]. It therefore covers call data, addressing or numbering data (such as IP address), clickstream data, data relating to the routing, duration, time or volume, protocol used or location of the device, or data generated for the purpose of billing (even if it is merely a copy or cached version).

Transactional data of this type can be useful for various service providers. There are, however, specific restrictions that apply as described in section 6.1.3 below.

4.4 Location data

Under the ECPD, location data means any data processed in an electronic communications network, such as a mobile or cellular network, indicating the geographic position of the terminal equipment of a user of an electronic communications service[22]. Location data can be generated in a number of different ways, most commonly via GPS and similar satellite systems, and terrestrial mobile or cellular networks, but also newer technologies, such as RFID and other near field communications technologies. However, it seems unlikely that location data generated by GPS and similar 'pure' positioning systems is caught by this definition as such systems are not 'electronic communications' systems. Location data generated on such a positioning system and

[20] Article 8.1 DPD
[21] Article 2(b) ECPD
[22] Article 2(c) ECPD. As mentioned at the beginning of Section 4, traffic data and location data are overlapping categories, i.e. some location data may also be traffic data (e.g. cell ID in the case of a mobile network).

then subsequently transmitted over an electronic communications system (say, the Internet or a mobile network) is likely to be viewed as content in the same way as a textual description of location.

Careful consideration will need to be given to whether or not any given positioning data is caught by the ECPD. The situation may be complicated by combinations of positioning technologies. For example, 'Assisted GPS' involves the processing of location data by a mobile network operator to 'assist' the GPS device in improving the performance of GPS positioning.

Location data can be a useful attribute in order to location-enable other applications. As with traffic data above, specific restrictions also apply to location data caught by the ECPD as described in section 6.1.4 below.

4.5 Some questions for consideration

- What types of data are being processed by the participants of a CoT in view of the comments above?
- Is any personal (sensitive or otherwise), traffic or location data being transferred or passed between participants?
- Even if the identity information that is being transferred or passed between participants is not personal data in itself (e.g. only an opaque handle is exchanged during single-sign-on), will a combination of attributes constitute personal data in the possession of a participant because of other data that that participant has or has a reasonable prospect of obtaining?

5 The roles of Circle of Trust participants

The Liberty framework identifies a number of different roles that entities can play, e.g. the identity provider (IdP), service provider (SP), attribute provider (AP), discovery service (DS), etc. In a CoT, the participants, such as network operators, communication service providers, application or content providers, could be playing any one or more of these Liberty defined roles. In addition, the legal obligations of participants in any given CoT under EU data protection and privacy law will, however, depend upon the classification of those participants according to the role or roles they are performing within the scheme established by the Directives – as described below. It can be seen, therefore, that there are at least three different and parallel schemes for defining the roles of CoT participants[23].

The Liberty framework itself is agnostic as to how roles defined by EU data protection and privacy law are mapped to Liberty-defined participants' roles and responsibilities. Set out below is a description of some of the most important roles and how they are likely to map onto the Liberty framework. Of course, it must be recognised that the actual characterisation of different roles is fact specific and there is no predefined mapping between a Liberty role and the nature of a relationships or obligation under the Directives. Examples provided below are merely illustrative.

5.1 Data subject

As explained above in relation to personal data, the data subject is the individual that is the subject of the personal data and, under the Liberty framework, the data subject will almost always equate to the principal. Companies, incorporated entities and other 'non-natural' persons are excluded from protection. While this exclusion of corporate entities may exclude many businesses and organisations, this will not always be the case. Small businesses and

[23] In order to link these different schemes together, references throughout this paper to any given role within one of these schemes are followed, in brackets, by the most likely parallel role in the other scheme or schemes

partnerships that are not incorporated may still receive protection; if any of their individual members or partners can be identified, they may be treated as data subjects depending on the national implementation of the DPD. The determining factor is not whether the organisation is acting in a business or consumer capacity, but the legal nature of the entity concerned. In addition, individual representatives of corporate entities (e.g. staff, users, etc) continue to have rights as data subjects.

5.2 Controller

The controller is defined in the DPD to mean any person or entity which, alone or jointly with others, determines the purposes and means of processing personal data[24]. Identifying which participant/s is/are a controller/s should, along with identifying the categories of data involved, be one of the first steps in any analysis of any CoT, as it is generally the controller that is required to comply with data protection laws. There are a number of key points to note here:

- The definition envisages the possibility of there being more than one controller per data-processing operation (i.e. control can be shared). In a federation, it is quite possible that more than one participant could be the controller in respect of any given transaction;
- It implies that a controller need not be in *possession* of the personal data concerned; it merely must exercise *control* over the processing. Again, in a federation, data will be transferred between participants but the transferor may retain some control over that data;
- It envisages that who is controller may change from one data-processing operation to another, even within one information system. Participants in a CoT could quite possibly be playing different roles in respect of different transactions;
- It indicates that determination of who is controller hinges not on the formal allocation of control responsibilities (as set down, for example, in contractual provisions), but on the factual exercise of control. This underlines the importance of business rules that establish clear operating practices for the federation.

Where attributes are being transmitted over an electronic communications network, the operator providing the transmission services is normally not to be regarded as the controller of any personal data contained in a transmitted communication; rather, the controller will be the person or organization from whom the communication originates. Nevertheless, the operator, as a transmission service provider, will normally be considered a controller in respect of the processing of the additional personal data necessary for the service, i.e. traffic data.

In a CoT, it is likely that the network operator, the communications service provider, and any content or application provider will be the controller in respect of the personal data that they each process in respect of their customers and/or employees. Consequently, regardless of the Liberty defined role of a given participant, they may nevertheless be classified as a controller (or joint controller) in law. This will ultimately depend upon how the participants define their roles and responsibilities in the business framework but, more importantly, the roles they actually perform in practice within their CoT.

5.3 Processor

Under the DPD, the processor is a person or entity that processes personal data on behalf of the controller[25]. The processor merely carries out a processing operation on behalf of the controller, but does not determine the purposes or means of processing; control remains with the controller.

[24] Article 2(d) DPD
[25] Article 2(e) DPD

As mentioned above in relation to controllers, the agnostic nature of the Liberty framework as regards participants' roles and responsibilities under EU data protection and privacy law, means that any Liberty-defined participant may be acting in the capacity of a processor at any given time. Again, this will ultimately depend upon how the participants define their roles and responsibilities within their CoT.

Understanding the distinction between the roles of controller and processor is essential to understanding the impact of the DPD on the establishment of a CoT. See section 6.2 below for a fuller discussion of the interaction between these two different roles, and the implications of this relationship.

Exhibit 1: Smartcard infrastructure services

One possible application for Liberty technology is to enable the providers of smartcards of various types (such as chip enabled credit cards and the SIM in a mobile device) to become Infrastructure Service Providers, enabling IdPs to add their identity credentials to the providers' smartcards. This could enable the provision by the IdPs of remote access authentication, banking and other applications.

Hosting identity credentials and associated data on the smartcard may amount to the processing of personal data relating to the user of the smartcard (assuming the data amounts to personal data). If the smartcard provider is positioned as merely providing the infrastructure, the provider is essentially in the same position as any other entity providing hosted data services. If so, then the smartcard provider may well be acting as a processor on behalf of the IdP, who would ultimately be controlling the processing of personal data on the smartcard.

Participants in many CoTs will also likely fall into the following roles under the ECPD, which will be necessary to understanding the impact of the ECPD on their relationships:

5.4 Public electronic communications network provider

The public electronic communications network provider is, not surprisingly, the entity that operates the relevant public electronic communications network[26]. An "electronic communications network" is defined as the transmission system and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit and packet-switched, including Internet) and mobile terrestrial networks, and electricity cable systems, to the extent that they are used for the purpose of transmitting. This therefore captures the operators of the relevant network infrastructure, regardless of the technology used.

The 'public' element simply means that the network must be made available wholly or mainly for provision of electronic communication services to the public. Therefore, enterprise networks, such as corporate LANs and other internal systems, will not be caught by this definition.

5.5 Public electronic communications service provider

The public electronic communications service provider is the entity that provides electronic communications services to the public[27]. An "electronic communications service" is a service (normally provided for remuneration) which consists wholly or mainly in the conveyance of signals

[26] Article 2 ECPD, and Article 2(a) of Directive 2002/21/EC of The European Parliament and of The Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ('Framework Directive')
[27] Article 2 ECPD, and Article 2(c) of the Framework Directive

on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting. This excludes, however, 'information society' services[28], such as services which consist of the provision of, or the exercise of editorial control over, content transmitted using electronic communications networks and services.

This will therefore include resellers of access to public electronic communications networks. In some cases the public electronic communications network operator and service provider are one and the same. For example, traditional telecommunications operators may both provide the network infrastructure and services on those networks to the public.

5.6 Subscriber

A subscriber is the person or entity that is a party to a contract with the service provider for the supply of electronic communications services. The subscriber may or may not be the user (see section 5.7 below). Further, if a subscriber is a natural person (i.e. an individual), he or she will also be a 'data subject' (as per the DPD – see section 5.1 above) in respect of any personal data processed about him or her. Under the Liberty framework, the subscriber will often be the principal in a consumer-facing CoT.

5.7 User

The user is the person or entity that uses or requests an electronic communications service and may also be the subscriber. For example, a corporate entity may be the subscriber whereas the corporate entity's employees will be the users. Similarly, a parent may be the subscriber while their child may be the user. The significance of the distinction between subscriber and user is that both have certain rights under the ECPD. Further, a user will also be a data subject in respect of any personal data processed about him or her.

Although the subscriber will often be the principal, in cases where the subscriber is a corporate entity, the subscriber may in fact be acting as an IdP (for example, if the corporate entity is providing Liberty enabled identity federation and authentication for its employees), the network operator may be an SP and the user may be the principal.

5.8 Some questions for consideration

- What roles are the participants in a given CoT performing according to the above? This may depend upon the type of CoT and different CoTs may give rise to different relationships.
- Are any participants acting *on behalf of* other participants in respect of the processing of personal data? For example, does the IdP process personal data *on behalf of* the SP when it carries out authentication?
- If an infrastructure provider provides hosting services to other identity providers, who is the controller of the personal data contained in the identity credentials stored on the hosting providers infrastructure? Does the provider act as the processor for the IdP?
- Does the participation in a CoT entail the provision of public electronic communications services?

[28] As used in the Electronic Commerce Directive (2000/31/EC) and defined in Directive 98/34/EC

6 Implications for compliance

The types of data and the role that any given participant has within the scheme of EU data protection and privacy law will have a number of implications for the legal framework of any given CoT.

6.1 Ensuring legitimacy of processing

A fundamental principle of EU data privacy law is that personal data collected in any situation should be limited to that which is necessary and relevant to the purpose[29]. This derives from the fundamental principle described in the introduction that individuals should be able to interact, browse and transact anonymously in the online world in a similar manner to the offline world. On the grounds that any collection of personal data may place an individual's privacy at risk, it is therefore necessary to ensure that the processing of any personal data, including its collection, may only be carried out on legitimate grounds. If there is no reason to identify an individual in respect of a given transaction, then identifying data should not be collected.

Consequently, for every item of data, the controller must be able to identify the legitimate grounds for processing that information, and for this purpose EU law provides a finite list. The most likely grounds available (although there are other grounds not considered here) for the different categories of data discussed above are explained below.

6.1.1 Personal data

Personal data may only be processed on one or more specific grounds, most importantly:

- The data subject has consented unambiguously[30] (see section 6.1.1.1 below); or
- The processing is necessary for the purpose of performing or considering entering into a contract to which the data subject is a party[31] (see section 6.1.1.2 below); or
- The processing is necessary for the legitimate interests pursued by the controller or by third parties except where overridden by the fundamental rights and freedoms of the data subjects concerned[32] (see section 6.1.1.3 below); or
- The processing is necessary for compliance with a (non-contractual) legal obligation[33].

6.1.1.1 Consent

The DPD states that the data subject's consent shall mean "… 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"[34]. While it does not stipulate any specific mechanism for obtaining consent, it is important to note some key points:

- Consent must be freely given. If the data subject is effectively given no choice, then it is arguable that any consent is not freely given. The precise circumstances in which consent can be said to be freely given will likely vary according to the circumstances and will need to be assessed on a case-by-case basis.

- The data subject must be informed of the purposes for which consent is sought, i.e. the purposes for which the data will be processed (see section 6.2 below for further discussion).

[29] Article 6.1(c) DPD
[30] Article 7(a) DPD
[31] Article 7(b) DPD
[32] Article 7(f) DPD
[33] Article 7(c) DPD
[34] Article 2(h) DPD

This information must be sufficiently specific, i.e. it cannot be so broad as to capture any possible use that the controller may happen to decide.

- The scope of any consent obtained is effectively limited to the purposes described in the information provided to the data subject.

Exhibit 2: Usage Directives, Interaction Service and consent

Various mechanisms have been designed into the Liberty framework to support the communication of consent, such as Usage Directives, Consent Attributes and Consent Headers. Usage Directives enable principals to communicate their privacy preferences, and service providers to communicate their requirements, with regard to the use of a principal's personal information. Usage Directives are supported in all transactions, and allow for the use of any privacy preferences expression language (PPEL)[35], although Liberty does not specify any particular language. For example, a subscriber may wish to use an interactive gaming service. The gaming service provider would like to use certain personal data (attributes) of the subscriber (principal) and exchange these with other players. The subscriber's (principal's) personal information is held by his ISP (AP). The subscriber (principal) can set his policy in a Usage Directive regarding the extent to which the personal information held by the ISP (AP) can be used and exchanged. If the service provider has adopted a Usage Directive that offers a 'lower' level of protection than that specified, then the subscriber's (principal's) personal information cannot be processed. If the service provider offers an equivalent or higher level of protection then the data can be processed in accordance with the principal's Usage Directive. By adopting Usage Directives the subscriber (principal) is able to communicate the extent to which they consent to their personal information being processed by the ISP (AP) and, if the data is exchanged, the subsequent processing of this data by the service provider.

In addition, the Liberty Interaction Service allows an AP to contact the principal in real time when consent or permission is needed or when there is a 'mismatch' between the Usage Directive communicated by a principal and Usage Directive communicated by a service provider. In the example above, if the service provider's Usage Directive offered a lower level of protection than that required by the subscriber (principal), then the ISP (AP) could use the interaction service to obtain specific consent from the subscriber (principal) in this particular case.

What Usage Directives essentially do is enable a principal to identify service providers with which it is prepared to interact based on standardized privacy policies using a particular PPEL. It does not ensure that the AP or service provider will actually comply with the policy expressed in a Usage Directive or provide any sanctions for non-compliance, neither can it address the fact that the regulatory framework applying to the AP or the service provider may not impose any particular obligations on the AP or the service provider regarding complying with the policy (e.g. because they are established in a jurisdiction with no applicable data privacy laws). To ensure that subscribers (principals) have sufficient trust in the policies contained in Usage Directives, it is likely to be essential for the CoT participants to agree that Usage Directives are binding on participants and enforceable by subscribers (principals). These issues will therefore need to be addressed by participants in the legal and contractual framework and provide appropriate remedies for principals.

At first glance, obtaining consent would appear to be the preferred means of ensuring legitimacy of any particular processing operation. This may be appropriate where the data subjects (principals) are all adults and are capable of giving consent. However, where an identity management framework is built primarily on consent, limitations on the legal age of capacity to consent could place those in reliance on consent in a difficult position where children are concerned, as consent may not be legally valid. Given the popularity and widespread use of Internet and mobile services among younger users, this presents a number of potential challenges to participants of a CoT, and to legislators, regulators and industry in general.

[35] For an illustration using P3P as an example, see the white paper on Liberty architecture framework for supporting Privacy Preference Expression Languages, available at http://www.projectliberty.org/about/whitepapers.php

However, consent is not the only ground upon which processing is permitted.

6.1.1.2 Contractual necessity

For many transactions involving federated identity and attribute sharing, this ground will provide a legitimate basis for processing personal data. For this ground to apply, the processing must be *necessary* and not merely desirable or convenient, e.g. without the processing being performed, the relevant contractual obligations could not be performed at all or by any other means. However, two points should be noted about this. Firstly, the contract does not need to be between the data subject and the controller, e.g. it could be between the data subject and a third party, such as a service provider that needs certain data about the data subject in order to provide a requested service. Secondly, the relevant performance could be performance by either party, not just the controller.

6.1.1.3 Legitimate interests of the controller

Processing may be justified if it is necessary for the purposes of the legitimate interests pursued by the controller, or by third parties, except where overridden by the fundamental rights and freedoms of the data subjects concerned[36]. The meaning of this ground is not entirely clear, though it appears to require some balancing of interests between the controller and the data subject. It is probably safe to assume that this ground is only likely to be available in relatively limited circumstances, and is unlikely to be available where one of the other grounds would have been a more appropriate basis to legitimize the processing.

6.1.2 Sensitive data

In respect of sensitive personal data, additional more restrictive conditions must be satisfied to permit processing in addition to those that apply for personal data. In most cases, the data subject's explicit consent is required before sensitive personal data can be collected or processed[37]. The expression "explicit consent" requires an active and positive indication of consent, which may be contrasted with consent required in respect of non-sensitive personal data. This is likely to require that the data subject perform some recordable action as an indication of consent. In some cases this may be sufficient by means of a click in a box, but certain jurisdictions interpret explicit consent to mean that written authorisation is needed. In these cases, this may rule out the acquiring of consent online unless the 'written' requirement can be achieved, such as with a digital signature[38]. Unless and until such explicit consent has been obtained, sensitive personal data cannot be processed.

Further, certain EU countries stipulate that the processing of certain sensitive data also requires the prior approval of the national regulatory authority (in addition to explicit consent)[39].

Therefore, exchanging sensitive personal data within a CoT may give rise to some complex requirements. Some CoT may decide to prohibit the use or sharing of sensitive personal data to avoid it becoming distributed within the CoT and the need for these requirements.

[36] Unfortunately, implementation of this ground varies quite substantially between Member States according to the European Commission's First Report on implementation of the DPD. Only eight Member States use the same or substantially similar wording to the Directive. Some Member States use similar language to the DPD, allowing controllers to make assessments as the application of this ground in any given case, while others have essentially pre-determined the circumstances where this ground can be used.
[37] There are other grounds available, such as where the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law. See Article 8.2 DPD.
[38] For example, in Spain, the legislation requires that consent be both explicit and written. While a click in a box is probably sufficient to meet the "explicit" requirement, a digital signature is probably needed in order to meet the "written" requirement when online.
[39] Spain and Portugal, for instance.

6.1.3 Traffic data

The processing of traffic data is subject to specific provisions under the ECPD. Traffic data may only be used for a limited number of specific purposes. The default position is that traffic data must be *erased or anonymised* upon termination of the call or connection in question (anonymisation must be permanent in that it should not be possible to reconstitute the personal data)[40]. However, this does not apply to the extent and for the duration that it falls within one of the following specified purposes:

- It is necessary for making interconnection payments and subscriber billing (and dealing with any disputes);
- Marketing *similar* electronic communications services or providing value added services (i.e. services that require the processing of traffic or location data beyond what is necessary for the transmission or billing of a communication), provided the subscriber or user has given prior consent; or
- Traffic management, customer enquiries and fraud detection.

If traffic data is proposed to be used by participants of a CoT, e.g. as an attribute, it may only be processed in accordance with these more restrictive rules under the ECPD. In many cases, this will likely mean the need for consent, as Liberty-enabled services will often be value added services, and the processing of traffic data must be limited to the extent and duration necessary for the value added service. In addition, the service provider must inform users and subscribers of the type of traffic data that will be processed and of the duration of processing. However, in respect of marketing similar electronic communications services or providing value added services, this information must be provided *prior* to obtaining consent. As discussed above in section 6.1.1.1, the scope of any consent obtained is effectively limited to the types of data and duration of processing described by the service provider to the user or subscriber. Therefore, if the service provider wishes to use other types of traffic data not informed to the user or subscriber, it would need to ensure it had sought further consent to the processing of this other data.

Of particular importance to a CoT are the restrictions in the ECPD on the entities that are permitted to process traffic data. This is restricted to the electronic communications network or service provider (i.e. the internet access provider, mobile operator, etc) and to certain other entities that are acting under its authority and that are handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service. The requirement that these third parties act only *under the authority* of the electronic communications network or service provider suggests that traffic data can only be handled by a third party if it is appointed as a *processor* by the network or service provider, in accordance with the DPD.

The restriction on the entities that can control traffic data will clearly have an impact if the participants of a CoT wish to process traffic data as an attribute within a CoT. It will not be permitted for traffic data to be passed to an SP in the capacity of controller, i.e. to pass 'control' of the data. The only entity that could act as an AP would be the public electronic communications network or service provider, and any service provider to whom that attribute data is passed would

[40] Article 15 of the ECPD provides that Member States may adopt legislative measures that allow the retention of traffic and location data in certain prescribed circumstances. Where Member States have adopted such measures, the requirements to erase or delete data do not apply and the data that is subject to such mandatory retention requirements may be retained for the purposes set out in Article 15. At the time of writing, the issue of mandatory traffic data retention is subject to a DG INFSO – DG JAI consultation by the Commission issued on 30 July 2004 and a report is expected in 2005. In parallel, a proposal for a draft Framework Decision on the storage of electronic communications data was presented earlier in 2004 by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004) and a report by the Article 29 Working Party was issued on this proposal on 9 November: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_en.pdf

be required to be appointed as the network or service provider's processor (see section 6.3 below).

6.1.4 Location data

The processing of location data is also subject to specific provisions under the ECPD. The general requirement is that location data can only be processed if it is anonymised or if the subscriber or user concerned consents[41]. So, once again, consent is essential.

If the subscriber or user concerned consents then, as with traffic data, the processing of this information must still be limited to the extent and for the duration necessary for the provision of a value added service.

In addition, the service provider must inform users and subscribers, prior to obtaining consent, of the type of location data which will be processed, the duration of processing, and whether it will involve transfers to any other third parties in order to provide the service. As discussed above in section 6.1.1.1, the scope of any consent obtained is effectively limited to the purposes described by the service provider to the user or subscriber. Therefore, the service provider should inform users and subscribers of the type of location data being processed, which could include the degree of precision of such data. As location services technologies develop, it is expected that the greater precision could be used. While this may be a benefit to the user / subscriber, the service provider may need to ensure they had sought further consent to the processing of this more precise location data.

Even where a user or subscriber has consented to the processing of their location data, they always have the right to, and must be provided with a simple means free of charge to block or refuse the processing of their location data, either for each connection to the network or for each transmission of a communication. This is likely to be a feature provided by the mobile operator, which must always be available regardless of whether or not the subscriber has consented to the processing for any particular service. For example, if a location service provider obtains a subscriber's (principal's) consent to process the location data of the subscriber, the subscriber (and user) should continue to have the ability to 'switch off' the positioning of their mobile device on a per message or per connection basis.

As with traffic data, there are also restrictions on the entities that can process location data. This is restricted to the electronic communications network or service provider (e.g. the mobile network operator or service provider) or to the value added service provider (i.e. the location service provider), or to an entity acting under their authority. In contrast to the restrictions on traffic data, the value added service provider is seemingly not restricted to handling location data under the authority of the electronic communications network or service provider and can therefore handle this data in its own right (i.e. as a controller). However, if any entity other than the mobile network operator, service provider, or the location service provider is provided with location data, it must be appointed as a processor by the relevant controller (i.e. the mobile network operator or service provider, or the location service provider) in accordance with the DPD.

As regards both traffic and location data, it should be noted that it is the user or subscriber that must consent. Practically, it may be very difficult to determine whether the data relates to a subscriber or a user. Therefore, the ECPD recognizes that whether consent is that of the user or subscriber will depend on the data to be processed and on the type of service to be provided and

[41] An exception to the requirement for consent is the mandatory provision of location information to emergency services. Article 26.3 of the Universal Services Directive (2002/22/EC) requires mobile network operators to provide caller location information to the emergency services where it is technically feasible. As a result of this requirement, the European Commission established the Coordination Group on Access to Location Information by Emergency Services (CGALIES) with the mission to define requirements for a pan-European common location provisioning mechanism that can be accessed and used by the European 112 community and emergency service operators. The final report was issued in June 2002 (available at: www.telematica.de/cgalies/index.html) and concluded that the regulatory requirement should be to make available a service that reflects the commercial equivalent in the national market

on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

Exhibit 3: Location services – roles and requirements

A possible use case for a location service may be as follows. An individual (principal) is a customer of a public mobile service provider that provides Liberty enabled identity federation and Web services and acts as the principal's identity provider (IdP). The principal has an account with the provider of an online travel service (TSP). This account is federated with his IdP, enabling the user to browse using his mobile device to the travel service with the benefit of single-sign-on. The mobile service provider is also the user's location service provider (LSP) and has registered this fact at the discovery service (DS) so that other service providers can know where to obtain location data on the user. The SP also provides the user with a map of his local area, and uses a third party map provider (TP) for this purpose.

The user has authenticated with his IdP and browses to the TSP and wishes to obtain information on traffic conditions in his area. The TSP issues a query to the principal's DS to identify the principal's LSP. The DS replies with details of the principal's LSP. The TSP contacts the principal's LSP requesting location data of the principal. The LSP will evaluate the principal's policy about revealing his location data. If OK, the LSP provides the principal's location data to the TSP.

What is the potential impact of EU privacy law on this use case? Below is an illustration of the likely roles of the participants under EU privacy law and some of the potential implications as regards ensuring the legitimacy of use and disclosure of location data:

Actors	***Roles and requirements***
IdP	The mobile service provider is acting as the IdP. As such, it will be holding the principal's identity information and will therefore likely be a controller in respect of this personal data. As the IdP and the principal have a contractual relationship, the IdP may be permitted to process the principal's identity information in order to fulfil the contract for the provision of the identity service (as per the 'contractual necessity' ground – see 6.1.1.2 above). If the IdP wishes to use the principal's identity information beyond what is necessary to fulfil the identity services contract, it will need to find another ground, most likely consent.
LSP	The mobile service provider also falls into the category of electronic communications service provider, and, if it also operates the network, it would also be the electronic communications network provider. The mobile service provider will also be the controller in respect of the location and other personal data held on its subscribers and users. While the DPD sets out certain grounds for ensuring that the processing of personal data is legitimate, the more limited grounds for processing location data under the ECPD mean that the LSP will only need to consider the impact of ECPD as regards the legitimacy of processing of location data. Under the ECPD, the LSP can only provide the location data to the TSP if the data is anonymised or if the principal consents. As the LSP will know the identity of the principal, the processing of the location data will not be anonymous (to the LSP), even if the data that is transferred to the TSP does not reveal, of itself, the principal's identity. The LSP is therefore likely to need consent. The LSP must also ensure that it only provides the principal's location data to a value added service provider to the extent and duration necessary for that value added service (as per the restrictions under the ECPD). The LSP therefore has to trust the requesting TSP that it requires the location data of the principal in order to provide the requested service and does not exceed this requirement in any manner. This will likely need to be dealt with within the contractual framework.

TSP	The TSP would likely fall into the category of 'value added service provider' under the ECPD. The TSP will receive the location data of the principal from the LSP. While the data transferred may not reveal the principal's identity, the TSP will be able to link that data to other information that the TSP has relating to the principal, e.g. account information, usage history, etc. Therefore, this data is likely to be personal data processed by the TSP and, as it exercises control over this information, will also be the controller in respect of this data. The TSP must ensure that it has legitimate grounds for processing this personal data, including the incoming location data. The TSP will need to consider the application of the DPD. In this use case, the principal requested a value added service that required the use of his location data. The TSP may therefore be able to rely upon the contractual necessity ground in receiving and processing the user's location data. However, this ground is only likely to apply provided the data are only retained and used for the purpose of that transaction. If the TSP wishes to retain location data history or use the data for another purpose, it will need to rely upon on another available ground. In many cases this will require the principal's consent. However, note the likely restrictions that the LSP will impose on the TSP above.
DS	The DS will not be receiving or processing traffic or location data and so the ECPD will not be relevant to the DS, but by managing the principal's service list, it might be processing personal data under the DPD, and therefore may be a controller in respect of this data. If the DS is a controller of the principal's personal data, it would likely be able to rely upon the contractual necessity ground in processing the principal's personal data. If it processes any personal data beyond what is required to provide the discovery service, then it would need to rely upon another ground, such as consent.
TP	The TP is contracted by the TSP to deliver map information to the principal based upon the principal's location data. As the TP needs to process personal data of the principal on behalf of the TSP (e.g. MSISDN and location data), the TP is likely to fall into the category of a processor. The TP, as a processor of the TSP, is simply carrying out the TSP's instructions. It should not therefore attract any responsibilities as regards the legitimacy of the processing of location data. However, the TSP, as the controller, will be responsible for the TP's use and processing of the data processed by the TP on its behalf, and will need to take steps to ensure it can exercise effective control over the TP in this respect, e.g. by contractual measures (see section 6.3 below for further explanation of the requirements on processors). Should the TP carry out any processing upon its own initiative (e.g. retain MSISDN for its own future marketing purposes), not only would it likely be in breach of breach of contract with the TSP, but, by determining the purposes for the processing of that data, it would be acting as a controller of that data. It would therefore become subject to the obligations under the DPD to ensure legitimacy of processing, which may be a difficult task if it does not have any direct relationship with the principal.
Principal	The principal would equate to the user in the ECPD scheme, and may or may not be the subscriber, depending upon whether he is the contract party for the electronic communications service. The principal will therefore have various rights under the ECPD in respect of his location data. Regardless of the fact that the LSP may have obtained the principal's consent, the principal must continue to have the right (free and charge and using a simple means) to block the processing of his location data for each connection to the network or for each transmission of a communication. The principal will also be the data subject in relation to each of the participants above and will have various rights set out in the DPD, such as a right to object to the processing of his personal data and a right to compensation in event of a breach.

6.2 Transparency

Controllers are required to provide certain information to data subjects whenever they process personal data, except where the data subject already has this information[42]. The required information should be given prior to the start of any processing (i.e. before the capture or receipt of data) or at the very least simultaneously with such capture or receipt.

6.2.1 Information to be provided

The information that must be provided to the data subject is as follows:

- The identity of the controller, i.e. the corporate legal identity of the entity that is controlling the processing;
- The purpose or purposes for which the data may be processed;
- Where it is necessary to ensure fair processing, the categories of data processed, the recipients or categories of recipients of the data, the specific rights that data subjects have and any other information which in the circumstances is needed to ensure fairness.

There are also more specific transparency obligations in respect of traffic and location data (see reference to this in sections 6.1.3 and 6.1.4 above).

These obligations apply regardless of whether the data is collected directly from the data subject, or if the data is received from a third party and the controller has no direct contact or relationship with the data subject.

6.2.2 Data captured from a third party

Where the data is captured directly from the principal, compliance with the transparency requirement is clearly easier, as there is an interaction between the controller and principal (data subject). However, where the data is captured indirectly and received from a third party compliance is more difficult, and this is likely to occur frequently in CoTs. The requirement to ensure that the processing is legitimate (particularly if consent is to be the basis for this) and the requirement to ensure transparency by providing adequate information to the data subject present practical challenges, as there is often no interaction directly with the data subject. CoT participants may wish to establish common rules regarding the communication of information and notice on privacy practices to principals to ensure that these transparency requirements can be met.

Fortunately, where the data is received from a third party, the obligation to provide information is not absolute, and there are exceptions. If the provision of information to the data subject is impossible or would require a disproportionate effort, then the information does not have to be provided. However, all the other requirements do still apply – if processing is legitimized on the grounds of consent, and consent can only be obtained in the light of clear and unambiguous information, these exceptions may be of little assistance.

6.3 Controller / processor relationships

The nature of the relationship between the controller and the processor is essentially that of 'master and slave' i.e. control of the use of the personal data remains with the controller; the processor merely carries out the controller's instructions. Therefore, this relationship is subject to specific requirements under the DPD. The requirements for the appointment of processors are primarily intended to ensure that the obligations and stringent security controls imposed on controllers are also imposed, by the controllers themselves, on their appointed processors[43].

[42] Articles 10 and 11, DPD
[43] Processors are generally not directly subject to the DPD in respect of processing undertaken *in their capacity as*

Therefore, whenever a controller wishes to appoint a processor to process personal data on its behalf, it must do the following:

- Only select a processor that provides appropriate levels of technical and organisational security for personal data (see section 6.3 below on appropriate security standards). Security considerations should therefore form a part of the selection process.

- *Ensure* compliance with the security measures adopted. The controller should take active steps to monitor compliance, e.g. by carrying out regular security audits.

- Require the processor to act solely on its instructions and enter into a written contract (or other legally binding act) that contains certain provisions regarding the security standards for the processing of personal data. This provides the mechanism for enforcing compliance with these security standards.

It follows from the above requirements that it is not sufficient for CoT participants that are acting in their capacity as controllers to simply put in place contracts with appropriate warranties and indemnities with CoT participants that are acting in the capacity as processors. They must go further than this and only outsource or sub-contract to entities that have demonstrated adequate security. Further, controllers are under a continuing obligation to ensure these security standards are adhered to.

The controller will remain primarily liable for the processing carried out on its behalf. Any person who suffers damage as a result of any unlawful processing operation is entitled to compensation (this is not limited to data subjects). In the event of an unlawful processing operation by the processor in breach of the processing contract which causes damage to any other person, it is likely that the controller would remain primarily liable due to its on-going obligations to ensure compliance by the processor. It is only likely to avoid this liability for compensation if it could show that it had taken all reasonable steps to monitor and ensure compliance by the controller, but this may vary from country to country.

Also, CoT participants will have to pay regard to the rules on applicable law as outlined in section 2 above. If one participant is acting as the processor on behalf of another (the controller), compliance will be the responsibility of the *controller* and the applicable law in respect of the processing will be that of the country of establishment of the controller, not the processor. However, if the first participant is actually processing personal data in the capacity of a controller, then the law of the place of establishment of the first participant will apply.

Exhibit 4: Mobile roaming and the proxying Identity Provider

Mobile roaming allows the mobile subscribers / users of one mobile operator to use basic mobile services, i.e. access and connectivity for voice and data, on another network. However, the roaming user does not usually have access to specific services available on the visited network. As the range of services available on mobile networks increases, mobile operators and service providers may wish to allow roaming users to access these additional services (“service roaming”). In that case, authentication of the user may be necessary. However, even with roaming agreements in place between the user’s home mobile operator and the visited mobile operator, a service provider on the visited network may not be able to accept authentication assertions directly generated by an identity provider on the user’s home network. The service provider may not even know of the existence of the identity provider on the home network. This situation might necessitate the intervention of an identity provider on the visited network to bridge the two networks and act as a proxy for the identity provider on the user’s home network.

processor - although they may be acting in capacity of controller in respect of other data, such as their own customer and employee data

The use of proxying means that when roaming, the principal will contact a local service provider which will direct to its local IdP. The local IdP will not be able to authenticate the principal, but it can act as a proxy for the principal's home IdP. The local IdP finds out the principal's IdP by examining the Liberty Enabled Client (LEC) list and sends an authentication request to the home IdP (i.e. the local IdP acts as a proxy). The home IdP then provides this response to the proxy and the proxy provides the authentication response to the SP.

By acting as a proxy in examining the IdP list in the LEC and carrying the authentication request and response, the proxy may well be acting as the processor on behalf of the home IdP, as the home IdP is likely to be the controller of the identity information relating to the principal. As such, the home IdP will be responsible for ensuring that the local IdP complies with its instructions and the applicable law relating to the processing of personal data by the local IdP will be the law of the place of establishment of the *home* IdP. In establishing their CoT, the home and proxying IdP will need to address the requirements outlined above, which includes, among other things, ensuring that the required terms are included in the contracts between participants.

6.4 Security standards

An essential ingredient in any CoT is the assurance of security in respect of identity related information and attributes, and of the exchanges between participants. Security is also, not surprisingly, a key component of EU privacy law and both the DPD and the ECPD set out legal requirements for the security of personal data and electronic communications services.

6.4.1 Personal data

Controllers are bound to ensure that they implement appropriate technical (e.g. encryption and ciphering) and organisational (e.g. building security and personnel management) measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other forms of processing. There are a number of points here that should be highlighted:

- What is an appropriate level of security is a function, on the one hand, of the nature and sensitivity of the data concerned and the type of processing being carried out and, on the other, the state of the art and the cost of implementing particular security measures. Put simply, the more sensitive the data and the riskier the processing, the greater the security measures required. Accordingly, in general, sensitive personal data should be afforded greater security than non-sensitive personal data[44].

- The DPD requires that the security measures should be taken both at the time of the *design* of the processing system, and at the time of the *processing* itself. It is therefore a requirement that CoT participants consider privacy enhancing techniques during system design, and during ongoing operation.

- Security is as much a matter of ensuring that there are appropriate organisational measures in place, such as policies, procedures and processes, and training in respect of these, as it is about technical security. Indeed, one of the main security risks is internal, i.e. the risk presented by employees having unauthorised or unnecessary access to systems and data. Therefore, technical measures will be of little use if individuals within the participating organizations of a CoT are not managed to ensure that they abide by the security policies and procedures in place.

- It should be noted that the security requirement is not just concerned with deliberate attacks or fraud, but also accidental loss. Consequently, simple back up of systems will be a legal

[44] Of course, some personal data may not be classified as 'sensitive' under the DPD, but are nevertheless clearly very sensitive, most notably, financial data.

requirement in most cases and a failure could, if it causes loss to a data subject (principal), give rise to claims for breach of security obligations.

- Adequate security is a continuing obligation. Therefore, the level of security needs to be continually assessed as new technologies become available, costs of existing ones come down, and new security risks become known.

- Particularly relevant to federated communities is the need for secure transmission of identity and attribute data over networks and particular attention is required in this respect. Consequently, the use of encryption, VPNs and other methods of securing the communications channel should always be considered. This is in addition to the security obligations that apply in respect of electronic communications services provided by network operators – see section 6.4.2 below.

- International security standards, such as ISO 17799, can provide a useful benchmark in ensuring participants attain the required levels of security. Adherence to such standards should be considered for inclusion in the legal framework.

These requirements do not just relate to the storage of personal data, but also to the way it is shared or made available, including authentication and authorisation.

6.4.2 Electronic communications services

Electronic communication service providers are also obliged to ensure that they take appropriate technical and organisational measures to safeguard the security of the electronic communications services provided by them. Similar considerations as detailed above in relation to personal data apply in terms of assessing security of electronic communications services.

In addition, however, the service provider must ascertain whether there still remain significant security risks to subscribers even after having taken the appropriate measures. If there are, then the service provider is required to inform the subscriber of the nature of the risk, any appropriate measures they can take to safeguard against that risk (e.g. such as use of a VPN) and the likely costs involved.

The security principles outlined above are very high level. The Directives do not stipulate particular levels or types of security measures, but the more sensitive the data and the riskier the processing, the greater the security required[45]. The only practical way for a CoT to manage compliance with this type of obligation is to undertake risk assessments and make security decisions (at least partly) on the basis of security risks presented to the individuals concerned (as opposed to the risk to service providers' own commercial interests).

Exhibit 5: Liberty security features

The Liberty framework provides a number of technical security features. These include the following:

- Authentication - The Liberty ID-FF, based on the OASIS SSTC SAML standard, defines a protocol that allows a service provider to generate an authentication request and receive an authentication assertion in response from the IdP. In addition, Liberty specifies bindings for that protocol, which allow the protocol to be performed in a web-based context (either solely over HTTP, or with some

[45] It should nevertheless be mentioned that certain Member States have set out detailed security requirements for personal data: both the technical regulations under the Italian Data Protection Code (No. 196 30 June 2003) and the Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data contain detailed minimum security requirements.

communication using SOAP+HTTP). In addition to the protections available via ID-FF, Liberty provides standard SOAP-based authentication and single-sign-on service interfaces to an identity provider.

- Identity protection - Once an identity provider has authenticated the user requesting service access, they can claim to know the identity of that user. Liberty allows the creation of *opaque* (not necessarily visible to all parties) privacy-protected name identifiers. These identifiers may cross business entities without revealing the identity of the user. Given that particular resources (a personal profile document or set of location attributes) may be associated with an identity, Liberty also provides an opaque, privacy-protected *resource identifier* – this combines the concept of a user's identity (and name identifier) with the idea of a specific personal profile resource belonging to *that* named user.
- Message Protection Mechanisms - Liberty specifies ways in which entities can be assured that requests and responses between participants are genuine. These range from transport security mechanisms, ensuring that the underlying transport is secure (for example, by use of TLS [RFC2246]), to token-based mechanisms (such as the propagation of a SAML assertion in a WS-Security [wss-sms, wss-saml] SOAP header block). In addition, Liberty specifies a SOAP binding ([LibertySOAPBinding]) that includes header blocks that provide *message threading* (so that a message received may be correlated to a message that was sent) and the ability for a message sender to make a claim about the sender's identity, which can be confirmed by the message recipient.

Inclusion of these features in the Liberty specifications does not guarantee correct or good implementation. The CoT participants will need to consider how to ensure conformity to these technical features in their legal framework. For instance, they will need to ensure that all participants implement these technical features, and implement them to an appropriate standard (which may also need to be specified). In addition, they will need to address procedural and administrative measures employed by participants to ensure that internal processes and procedures are robust and do not undermine the carefully designed technical measures described in the Liberty framework.

6.5 Trans-border data flows

In order to ensure the free flow of personal data between EU Member States there are to be no restrictions on the flow between Member States of personal data, as all EU countries should provide a harmonised level of protection. However, transfers of personal data outside the EU may only take place if an adequate level of protection is provided in the recipient country. Whether the protection afforded is adequate or not is a complex issue and in many cases will not be practical for participants of a CoT to undertake on a case-by-case basis.

The European Commission has power under the DPD[46] to provide specific approval of certain countries as providing adequate protection – see further comment on this in section 6.5.1 below. Failing this, transfers of data to non-EU countries may only take place if one of a number of exceptions applies. Consequently, the participants of a CoT must examine the extent to which personal data is being transferred from EU Member States to states outside the EU. If it is, and it is not one of the countries approved by the Commission, they will need to identify at least one of the applicable exceptions for each transfer. The most relevant exceptions are as follows:

- The data subject has consented unambiguously to the transfer[47]. This will in many cases, be the most feasible option particularly for transactions initiated by the principal, although note the comments above on the limitations of consent in section 6.1.1.1; there may therefore be circumstances where consent is not sufficient and one of the following exceptions will be needed.
- The transfer is necessary for the performance of a contract between the data subject and the controller, or forms part of the pre-contractual measures taken in response to the data

[46] Article 25.6 DPD
[47] Article 26.1(a) DPD

subject's request[48], e.g. credit checking or authorization (note comments above on contractual necessity in section 6.1.1.2), or the transfer is necessary for the conclusion or performance of a contract concluded in the interests of a data subject between the controller and a third party[49].

- Where the transfer takes place on standard contractual terms approved by the European Commission[50]. See the further explanation of this in section 6.5.2 below.
- Where the transfer takes place with the prior authorization of the relevant Member States' privacy authority[51]. See the further explanation of this in section 6.5.3 below.

It is important to note that, even if the transfer can be permitted under one of the exceptions above, compliance with all the other requirements concerning data capture, processing, etc, is still required (see sections 6.1 and 6.2 above on ensuring the legitimacy of processing).

6.5.1 Countries outside the EU approved as providing adequate protection

As at the date of this paper, the European Commission has determined that Switzerland, Hungary[52], Argentina, Guernsey and the Isle of Man have laws providing adequate protection of personal data. Canada is also on the Commission's list but only in relation to certain classes of data export[53]. Transfers to these countries are therefore permitted.

The US does not provide adequate protection under its general laws. However, the US has established a specific data privacy "Safe Harbour" with the agreement of the European Commission[54]. This provides that US organizations that sign up to the Safe Harbour will be bound by certain basic rules on data protection. Consequently, transfers are permitted to organizations that have signed up to the Safe Harbour. The list of organizations that has signed up is available at http://www.export.gov/safeharbor/. However, of particular relevance to a Cot involving telecommunications carriers is that the Commission only recognizes the Safe Harbour Agreement as providing adequate protection for organisations subject to the jurisdiction of the Federal Trade Commission and the US Department of Transportation[55]. As neither of these two authorities is responsible for telecommunications carriers, the participation of US public telecommunication operators will not provide the protection that EU based participants need.

While specific approval by the Commission for the transfer of personal data to certain countries provides a mechanism for participants in a Liberty-based CoT to share data with participants in those destination countries, the rate at which countries are being approved and the difficulty in obtaining approval means that an international CoT will often need to use one of the exceptions available for many transfers. If and to the extent that consent is not available or appropriate, or the transfer is not contractually necessary, the following exceptions will need to be considered.

6.5.2 Approved standard contractual terms

Transfers can be one of two types, depending upon the capacity of the entity to which the data are being transferred (i.e. the recipient may be classified as a controller or a processor). Sometimes transfers may be made by one controller to another, i.e. the receiving entity will

[48] Article 26.1(b) DPD
[49] Article 26.1(c) DPD
[50] Article 26.4 DPD
[51] Article 26.2 DPD
[52] Since the Commission's decision on the adequacy of protection in Hungary, Hungary has now joined the EU, and so transfers would no longer be restricted anyway.
[53] i.e. only data subject to the Canadian Personal Information Protection and Electronic Documents Act and it does not extend to public corporations or non-commercial organisations
[54] Commission Decision (2000/520/EC) of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), *Official Journal L 215 , 25/08/2000 P. 0007 - 0047*
[55] Recital 6 and Annex VII of Commission Decision 2000/520/EC

determine the manner and purposes for which the data may subsequently be processed. On the other hand, the receiving entity may be a processor, carrying out processing on the controller's behalf, with no control over, or interest of its own, in the data.

In either case, one of the exceptions from the adequacy requirement for transborder data flows out of the EU is where the transfer takes place on standard contractual terms. The European Commission initially approved two sets of standard contractual terms; one for transfers to controllers (so called 'controller to controller' transfers)[56] and one for transfers to processors (so called 'controller to processor' transfers)[57]. The clauses are complex and have been criticised by the business community as exceeding the requirements of the DPD. The International Chamber of Commerce, along with other industry groups, officially submitted an alternative set of clauses to the European Commission for approval by the committee of European Data Protection Authorities set up under the DPD, the Article 29 Working Party, in September 2003. These clauses have now been approved by the Commission and will come into effect on 1 April 2005[58].

The use of bi-lateral contractual arrangements may be workable for many closely defined and relatively static CoTs. However, for CoTs with a large number of participants or where membership is very dynamic, with new participants joining or leaving frequently, managing a series of bi-lateral contractual arrangements could pose significant practical difficulties. A possible alternative to using the standard clauses would be for a CoT to establish a binding code of practice which CoT participants could sign up to. There is provision for this type of arrangement in the DPD, which would require prior authorisation from the applicable Member State's privacy authority.

6.5.3 Prior authorisation

At the date of writing, most of the discussion concerning the use of this exception has focused on the approval by the Member States' privacy authorities of internal rules for use by a multinational company to enable it to share personal data outside the EU but within the corporate group (referred to as Binding Corporate Rules). The Article 29 Working Party published a working document in June 2003[59] on the potential application of Article 26.2 to multinational corporate groups[60]. On 24th November 2004, the Article 29 Working Party organized its first public hearing on Binding Corporate Rules. The expectation at the end of the hearing was that early in 2005 a number of national Data Protection Authorities would jointly be able to approve a number of Binding Corporate Rules[61].

In the enterprise environment where the CoT is established between entities within the corporate group, the approval of Binding Corporate Rules could provide a far more flexible and workable solution to trans-border data flows outside the EU. However, it should be noted that the prior authorisation exception is not limited to internal transfers within multinational companies. It may be feasible that such rules could be adopted for other CoTs, such as consumer facing federations, albeit using the CoT's governance and contractual framework as the means of enforcement, as opposed to internal corporate policy. This could avoid some of the problems with

[56] 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; *Official Journal L 18 , 04/07/2001 P. 0019 – 0031*
[57] 2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC; *Official Journal L 006, 10/01/2002 P. 0052 - 0062*
[58] See Decision C(2004)5271 and overview at:
http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm
[59] See: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf
[60] This was followed in the UK by the publication in September 2003 by the Information Commissioner of a guidance note on how to apply the rules on prior authorization to Binding Corporate Rules: http://www.informationcommissioner.gov.uk/eventual.aspx. In 2004 a consultation begun with industry on the development of such rules. See overview provided in the Information Commissioner's 2004 report: http://ico-cms.amaze.co.uk/DocumentUploads/information%20commissioner%20ar%202004%20web%20pdf.pdf
[61] See report of the hearing published by the Dutch Data Protection Authority:
http://europa.eu.int/comm/internal_market/privacy/docs/consultations/hearing_bcr_en.pdf

the other exceptions described above. However, if the time it has taken to gain initial acceptance of Binding Corporate Rules within corporate groups is anything to go by, obtaining regulatory approval could be convoluted and lengthy.

Exhibit 6: Cross-border e-commerce

Where a CoT straddles borders within and outside the EU, trans-border data flow issues are likely to arise. In such a CoT, a user (principal) based in the EU may wish to transact with a service provider in the US (that has not signed up to the Safe Harbour). In order for a particular transaction to take place, certain attributes of the user (such as payment details, delivery address, etc) may need to be provided by the attribute provider to the service provider. This will likely involve the transfer of personal data to the US. Consequently, as the US has not been determined as offering adequate protection, the participants will need to rely upon the exceptions to the adequacy requirement described above.

One exception will be for the user to consent to the transfer. This will necessitate the user being informed of the fact that the service provider is located in the US, and that their data will be transferred there. The CoT participants will need to agree upon how this information is to be delivered to the user to ensure that consent is lawfully obtained.

Alternatively, the transfer of attributes may be necessary for the performance of a contract to which the user is a party, e.g. if the attributes are payment details. In this case, it may not be necessary to seek consent. However, any use of attributes beyond what is strictly necessary will not be permitted on the contractual necessity ground. For example, the service provider could not rely upon this basis to retain payment details in the event that the user wishes to return to the service provider for future transactions; it would have to either obtain consent or rely upon one of the other available grounds.

If either of the above two options are not available for any of the purposes required, the participants of the CoT could incorporate the standard contractual clauses into their CoT contractual framework and transfer the data on that basis.

In practice in many cases, a transfer of attributes will have to be based upon a number of exceptions, depending upon the attributes concerned, and the purposes for which the attributes are requested by the service provider.

6.6 Access to terminal devices - Cookies and similar mechanisms

The use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user (e.g. the use of cookies or similar mechanisms) is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information, among other things, about the purposes of the processing, and is offered the right to refuse such processing by the controller. However, this requirement does not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service (as described in section 5.5 above) explicitly requested by the subscriber or user.

Exhibit 7: Remote updating of the IdP list

One of the issues that the Liberty framework had to address was how a service provider could know which IdP a principal used where the principal was not directed to the service provider by the IdP. In the PC environment, one way this may be achieved is by placing a cookie on the principal's browser with a list of the IdPs used by the principal. However, this list needs to be maintained as new IdPs may be

added or removed. The remote updating of this list on the user's PC by IdPs may well fall within the ambit of these restrictions. If the purpose is neither for facilitating transmission nor strictly necessary for provision of an information society service, then the IdP would need to provide the subscriber (principal) with notice and offer the subscriber (principal) the possibility to refuse the updating.

6.7 Some questions for consideration

- How will consent be obtained by participants processing personal data if they do not have a direct relationship with the data subject / subscriber / user?
- Will participants need to rely upon each other to obtain consent?
- Can participants rely upon consent or will they require age verification in addition?
- Will the CoT involve the transfer of personal data to a participant that is based outside of the EU?
- Are cookies or similar mechanisms used and if so where, how, by whom and for what purpose?

7 Summary of potential implications for the legal framework

The above overview of some of the compliance issues relevant to CoTs highlights a number of particular areas that will need to be addressed in the legal arrangements between participants in a CoT:

- If any participant is processing personal data on behalf of another participant, the parties will need to comply with the requirements outlined in section 6.2. This will necessitate a contractual agreement containing the minimum requirements as outlined.

- The parties will also have to specifically address the security requirements to be complied with by the processor. The contract will therefore need to set out the minimum security standards to be adhered to. This will depend upon the purpose and type of CoT and the type of data involved. In addition, because of the ongoing nature of the obligations on the controller, the controller should ensure that it has a right of audit of these security measures to ensure that they are being adhered to in practice. This may be something that the participants in a given CoT could entrust to a third party acting on behalf of all participants.

- The participants may wish to mandate adherence to security standards specified in the contract, such as ISO 17799, where appropriate. The contractual framework will need to build in flexibility to enable standards to be improved as new risks become known and new technologies and mechanisms become available.

- The participants will wish to specify conformity to the Liberty specifications and may need to set out implementation requirements and standards.

- Where participants are reliant upon one another to collect consent from principals, then the contractual arrangements may need to address issues concerning age verification to ensure that consent is legally valid. Where sensitive data is concerned, participants may also need to address the means by which explicit consent was obtained to ensure that consent is explicit and, where required, also meets the requirements for writing, such as a digital signature.

- The participants may wish to make legally binding any policies expressed in Usage Directives and give principals direct rights of enforcement to give participants trust and ensure that parties are bound to comply with their stated policies.

- If there is a transfer of personal data by one participant to another participant outside the EU, the parties will need to consider the impact of the trans-border transfer issues outlined in section 6.4. If consent cannot be used as a ground for permitting the transfer, one of the other grounds will have to be sought. If the recipient participant is not in an approved territory, the parties may need to ensure they include or incorporate the applicable standard contractual terms, or alternatively seek regulatory approval for a specific binding scheme for the CoT.

End of document