Net-ID 2007
Identity, Trust, Privacy and Security in Europe

LIBERTY ALLIANCE PROJECT

# Privacy Summit

hosted by the Public Policy Expert Group
of the Liberty Alliance
in conjunction with the Net-ID 2007 conference

**Monday February 26th 2007**
**Berlin**

## Meeting Summary

## Foreword

The aim of this Privacy Summit was to bring together a wide range of stakeholders, so as to stimulate a multi-disciplinary discussion of the technical, legal, social and other perspectives on identity and privacy. To that end, the participants included academics, lawyers, user organisations from the public and commercial sectors, technologists, industry analysts and so on.

The discussion was held under the 'Chatham House Rule'[1] – so the participants are free to repeat what was discussed, but may not reveal who said what, nor the affiliation of any of the participants.

This document is an attempt to summarise the topics discussed; it is not an exhaustive record of the meeting, and participants are encouraged to reply with any further notes or comments they would like to add to the output of the Summit.

Anyone wishing to comment on, add to or correct this document should do so by sending an email to robin.wilton@sun.com.

Many thanks for your participation

and your contribution to this ongoing programme.

Dr. Hellmuth Broda - Chairman

Robin Wilton - Moderator

Document date: 21st March 2007

Document reference: PS-Berlin-2007

[1] The Chatham House Rule
"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed" (http://www.chathamhouse.org.uk/index.php?id=14).

# Table of Contents

## The 'Dimensions' Of Privacy

As well as the “Technical vs. Contractual” spectrum of privacy measures, we also added Structural and Social dimensions to the model for privacy and online relationships. Examples of these four dimensions are as follows:

- Technical

For instance, giving users the means to apply technical protective measures to their Personally Identifiable Information (PII);

- Contractual

Establishing a binding agreement between the user and service provider, under which the service provider may not further distribute the user's PII. NB – 'contractual' here has been used as shorthand for legal/regulatory/contractual, and to encompass both commercial and public-sector cases. However, it was also noted that these different sectors imply very different liability models

- Structural

Although the relationship between a user and a service provider may mimic certain aspects of an interpersonal relationship, it was noted that it is not such a relationship in fact, and tends always to embody an asymmetry in favour of the service provider. Structural privacy measures might seek to redress this balance in some way;

- Social

A comment on this aspect was that “Digital Rights Management (DRM) technology does not seem to have delivered... because 'socially' there is a strong incentive for the user community to try to overcome it. In other words, DRM – sometimes characterised as “Digital Restrictions Management” -- is 'technology plus policy', imposed without regard to user acceptance. Is there good reason to suppose that analogous 'PII protection' mechanisms would fare any better?”

It was also noted that human social interactions are currently based on a 2-300 year history of “close social context” based on personal and collective memory. In one sense this provides a strong social 'enforcement' of respect for privacy, in that negative behaviour tends to have direct negative consequences. Conversely, though, personal and collective memory may actually be more fallible (even 'forgiving') than today's technical capability for the storage and mining of almost unlimited data, however trivial.

There is thus a 'loss of transience' about PII today; data tends to persist unless it is actively expunged from storage. Future privacy mechanisms may want to address the question of (forced) 'computer forgetfulness'.

Returning to the frequent tension between contractual and technical measures, we noted that technical measures often tend to express privacy in terms of two-party relationships... whereas the need is increasingly to cater for multi-party relationships involving parties with a wide range of roles – some expressed technologically, and some legally or otherwise (such as socially).

Those relationships may also involve notions of 'transfer' and/or 'delegation'; in other words, service providers sharing information beyond the scope of the original two-party relationship with the data subject[2]. There can be difficulties in going beyond two-party contractual provisions – a point which was encapsulated in the phrase “no lien, no obligation”. Under many (most?) systems of contract law, a contract between two parties cannot be binding on a third party... which implies that the abuse of PII by third parties must be countered by some other means.

[2] E. g. a service provider might have outsourced certain business functions to third parties

## Data 'Ownership'

We discussed the implications of several terms, including “data subject”, “data owner”, “data controller” and “data custodian”. Without trying to produce normative definitions, these were the descriptions we gave to these terms:

| ***Term*** | ***Description*** |
|---|---|
| Data subject | The person or entity 'referred to' by some data. In the case of PII, the data subject is more or less identified by that data; in the case of transaction records, the data itself may not identify the data subject but may provide a log of historical activity which records behaviour. Used in conjunction with PII, the behaviour could be ascribed to a specific entity. |
| Data 'owner' | This reflects the concept that a data subject may have some kind of right (perhaps a statutory one) to know what data someone else has about them. Thus, although someone else has the data, the data subject might be said to have some degree of 'ownership' of it. |
| Data controller | A legally-defined role expressed in the EU Data Protection Directive; the person who determines how and why personal data are to be processed. |
| Data custodian | A legally-defined role providing for the controlled disclosure of PII through a form of 'trusted proxy'. For instance, in Germany a company could  be legally prohibited from disclosing the PII of its employees, but might legally do so by entrusting the disclosure mechanisms to an independent 'data custodian' within the organisation. This could serve as a good example of privacy protection through a combination of legal, policy and structural measures. |

NB - the legal standing and interpretation of such terms may vary from one legislative environment to another.

While the role of data controller may appear to be a clearly defined one, it can sometimes prove difficult to establish who is the data controller in a given instance, particularly where parties exchange information through an intermediary. The example of SWIFT was cited, as a case in which one party denied that it had data controller status, as it acted merely as a 'switch', transferring information between other parties.

The notion of a 'co-controller' was raised in this context – in other words, a party which may share some of the data controller responsibility with other participants in a multi-party exchange of data.

A further example of this role, located since our discussions, is referred to in a 2005 white paper produced by the Article 29 Working Group, with the reference number 1022/05/EN WP 110[3]. This paper describes the role of the European Commission – relative to that of individual Member States – in the operation of a pan-European Visa Information System (VIS).

[3] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_en.pdf

## Privacy Policy in Multi-Party Relationships

Under this heading we discussed the concept of whether privacy preferences can be effectively expressed and enforced, particularly in multi-party exchanges of data. The term “sticky policy” was used to describe a policy which can be expressed in such a way that it persists even after data has passed beyond the original recipient. We nevertheless noted the underlying tension between “the wish to disclose” (usually for a specific purpose or benefit) and the necessarily discretionary nature of some of the protective measures one can apply as a result...

The suggestion was made that it might be desirable to develop “a machine-readable icon bound to a set of contractual terms”. Such an icon (or set of icons) might address the 'social' dimension of privacy adoption by being intuitively or easily understood – in much the same way as the 'Creative Commons' icons embody a simple set of rights assertions on the part of individual authors.

It was noted that the set of security management disciplines required to underpin such a scheme are already well-understood and can be found, for instance, in many outsourcing operations:

- Secure operations requirements
- Security Service Level Agreements (SLAs)
- Mutual Audit by the parties concerned
- A clear structure for liability and/or recourse in case of a breach of terms
- Fines or other penalties in the event of a breach.

An example was given of how such agreements have been used in practice in a multi-national corporate context. In this instance, a corporation has multiple enterprises located in (155) different countries and therefore operating under different privacy legislation regimes. There is a frequent need to exchange data between corporate entities and across national boundaries.

In this instance, the company instituted a Binding Corporate Rule which governs its internal treatment of personal data, and establishes a voluntary internal minimum standard of governance which helps to overcome the different national levels of data privacy legislation. This is made easier by the fact that most national legislative regimes at least define some form of 'adequacy test' for privacy protection.

The Binding Corporate Rule is backed up by liability provisions and financial penalties.

Other contractual approaches

These might include measures such as agreements to limit disclosure to only such information as is necessary for and appropriate to a given context/transaction. For example, to disclose an assertion of creditworthiness up to the requested amount rather than credit-card details, or to disclose an assertion that someone is “over 18” rather than disclosing their date of birth.

Contractual agreements might also include measures to reduce “linkability” - that is, the ability to infer that two transactions or activities were undertaken by the same individual, even if different identifiers were used. These measures could include:

- providing the ability to interact anonymously or pseudonymously;
- agreements to impose a 'persistence limit' on data (for instance, that it will only be stored for a specified period);
- auditable deletion or 'non-storage' of data.

## Sector-Specific Identifiers in Austrian e-Government

Continuing from the topic of 'linkability' raised above, the Austrian government example was described, as a case in which a single state-issued identifier is used as the basis for multiple sector-specific identifiers – which can only be correlated by the Privacy Commissioner. The sector-specific identifiers are generated using one-way cryptographic functions, so that the sector-specific identifier can easily be derived from the original identifier on the citizen card, but conversely, the original identifier cannot be derived from the sector-specific identifiers.

A concise description of this scheme can be found here[4], on the European Commission's IDABC website, and a web search using the argument "Austrian Citizen Card" will return a wide range of further documentation.

## BIPAC Example of Federation and Privacy

The US organisation BIPAC[5] was used to give an example of the extent to which identity federation can affect privacy-related issues. For instance, the 'before and after' illustrations of BIPAC's case show a significant over-all reduction in the amount of data which has to move between parties.

There are also qualitative differences in the data exchanged; for instance, BIPAC is able to grant authenticated, single-sign on access to the employees of other organisations without having to know the names, user IDs or passwords of those users on their 'home' authentication server.

BIPAC operates in a highly regulated environment, because of the strict US laws on lobbying activities. The fact that BIPAC simply never has the personal details of the users referred to above means that it has a reduced regulatory burden... in that it does not need to prove that it is securely managing those personal details – because it never has them.

A white paper describing BIPAC's implementation of federated identity using the Liberty standards can be downloaded from the Liberty website, here[6].

[4] http://ec.europa.eu/idabc/en/document/4486/5584

[5] http://www.bipac.org/home.asp

[6] http://www.projectliberty.org/index.php/liberty/resource_center/case_studies

## 'Parking Lot'

As ever, the discussion raised many interesting themes which, in the interests of time, we had to simply note and leave for another time. This is the 'parking lot' list of those themes:

- 'Self-generated' assertions (what are they, and how do they differ from other forms of assertion in digital identity systems?)
- 'User centricity' (Is there a consensus as to what it is? What different things have been labelled as 'user centric'?)
- Purpose creep and function creep in digital identity systems
- Platform complexity and the 'Trusted Computing Base'; how far are attempts to safeguard user privacy and identity undermined by the complexity and the security shortcomings of computing platforms?
- Privacy issues specific to the public sector identity schemes.