Special issue of the International Conference on Computational and Experimental Science and Engineering (ICCESEN 2014)

A New Methodology to Disambiguate Privacy

D. Alhalafi*
De Montfort University, Software Technology Research Laboratory, Leicester, UK

This paper addresses the pragmatic and semantic meaning of the term privacy by establishing a new method methodology of proceeding pragmatic, semantic and conceptual or combinations instances of privacy in relation to technology. The analysis of construct definition based on information published in the literature, for example Dictionaries are investigated under various conditions, for example semiotics. The new hybrid–privacy method is lexica–technical that investigates chronological definition of terms in relation to technology in distributed systems (DS); the method also looks at the impact of technological advancement on a particular innovation, polythematic or progress in pragmatic, semantic and conceptual characteristics of perception of privacy. The method's use is verified in an analysis of the unique meanings that underlie the term's usage both as a single word and in combination such as privacy law, privacy attack, privacy breach, and so forth. Literal (denotative) definitions and metaphoric (connotative) associations are examined to explain the use of privacy to refer to a physical entity and/or a mental representation, conceptual and perception. The method is also tentatively grounded in the disciplines of philology, cognition, information technology, and the philosophy of science. The lexica–technical analysis method is applied to the meanings of privacy starting with its original usage in the twenty first century and culminating with the definitions used by authors, IT developers and peoples in this paper. Finally, the paper aims at proposing a pragmatic, semantic and conceptual framework for measuring privacy. In this, technically introducing an extra button on the keyboard to indicate; whatever typed next is private to establish new link between cognition and neuron-computation systems.

DOI: 10.12693/APhysPolA.128.B-319
PACS: 01.50.hv, 89.20.Ff

1. Introduction

In spite of active work on dealing with privacy and security concerns during the early stages of design of distributed systems, there has been little work on synthesising the contributions of these fields into processes for specifying and designing a privacy policy framework. Without a better understanding of how to deal with both concerns at an early stage, the design process risks disenfranchising stakeholders, and resulting systems may not be situated in their contexts of use.

The disambiguation of the privacy process plays a critical role in transforming privacy policy from static to interactive or dynamic towards delivering user's privacy expectations. In this paper the author made substantial contributions to conception and design of privacy provision in DS.

First, privacy provision must incorporate user privacy expectation in an interactive manner. Second, privacy provision requirements are included at the design stage of DS. Finally, privacy lexica–technical terms of polythematic hybrid privacy semantic methodology are specified. The research problem this paper addresses is how techniques and socio–linguistics and socio–psychological tools can be integrated and improved to support the design of a new privacy term development method. To develop this, we present a hybrid–privacy term for specifying usable and secure privacy models for DS. This hybrid–privacy term method (HPTM) considers the system design process from three different perspectives — users, developers and infrastructure — and guides the selection of techniques towards integrating users, developers, and infrastructure engineering processes.

DS policies to protect privacy are similar, linear and less efficient in most DS. There exists a large number of cases of privacy breach in DS. Privacy breach is attributed in most cases to lack of conceptual, control and technical capacity towards resolving issues of confidentiality expected by the user. Current methods lack understanding of the underlying reasons and principles central to privacy in social–psychocontextual approaches. Moreover, these attributed method, methodology and processes mainly consist of DS architecture, lexicon and human, and systems errors. We are proposing a new method that incorporates system developers and users to formulate, standardise and guide DS privacy terms. The relationship between DS developers and users under the guiding principle of conformity is divided into user expectation, legal requirements and business risk strategy. The HPTM method will use social–psycho tools to extract perceptual terms from users and developers. Social–psycho tools are the main adjustment constructor for the proposed method to harness the relationship between the user privacy expectation and distributed systems developers.

The aim of using social–psycho tools is to find a solution to increasing privacy breach incidents in DS, formulate user developer relation and hybrid privacy terminology to reflect on both user's expectation and developer's design and interpretation of user requirements. Expanding the study into the psychoanalysis realms came in as

*corresponding author; e-mail: dhafer606@yahoo.co.uk

a result of the need for qualitative information to assist both users realisation of privacy in DS and developers interpretation of user privacy expectation.

The aim of carrying out a descriptive survey using social–psycho tool on users and developers perception is to verify the paper hypotheses of hybrid–privacy terms of privacy information and hybrid–privacy terms of domain infrastructure capacity, in addition to establishing success/failure factors in relation to technology and client, and finally to identify if other reasons exist that determine enterprise privacy policy success/failure in distributed systems. The social–psycho descriptive approach is rapid and practical in terms of potential and is flexible enough to cope with important new directives, information or distributed system issues as they arise during the development phase. Furthermore, this method is used to describe the privacy situation, as it exists at the time of the study and to explore the cause or causes of particular phenomenon. Finally, the social–psycho method can use either qualitative or quantitative data or both, giving the researcher greater options in selecting the instrument for extracting and assembling data. While developing the social–psycho tool, two issues are considered first; the distributed system user's trajectory as a guiding measure, second; standards, protocols and methodology governing data sharing in distributed systems. Considering these two elements at the design stage of the social–psycho devices survey will help in facilitating a holistic non-biased approach to the problem.

2. Privacy terms specifications in distributed systems

The epistemological fragmentations mount from positivist sensory-logical framework as the primary conceptual source of the hybrid–privacy method, where Hybrid refers to Distributed Systems Architecture and user's perception. Social–psycho tool constructor designs hybrid–privacy terms keywords list, standards and framework. Example: typical conventional question verses communication of perception questionnaires derived from 2.1 – 2.2 One of the fundamental problems with customary socio–centric distributed systems is that they require services to be built for '*one hypothetical point in time*'; whereas users expect and require accessing those lexicon services over a '*time continuum*', i.e. in continuous, anytime, anywhere environments. In today's DS architectures this is guaranteed to cause major problems and user disappointment. However, a fully integrated hybrid–privacy term will bring about the advantage of a single holistic view of the user expectation [1].

2.1 Primary specification:

- hybrid–privacy terms of privacy information,
- hybrid–privacy terms domain infrastructure capacity.

2.2 Secondary specification:

- hybrid–privacy terms scale,
- hybrid–privacy terms domain weight communication perception.

A simplified view that distinguishes conceptualisation (knowledge), action in the world (practice), and text, diagrams, and computer programs (descriptions, commonly called "representations") [2] is illustrated in Fig. 1.

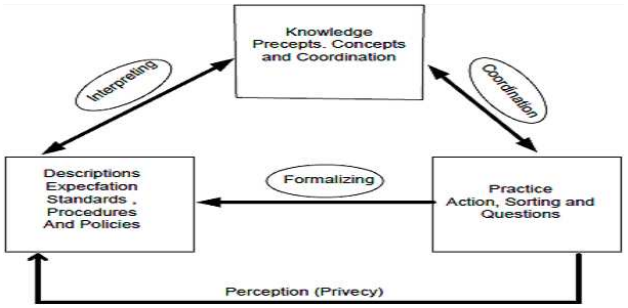

Fig. 1. Description, knowledge and practice.

Examining the extremes of human experience, studies of creativity and dysfunction have discovered that conceptualisation concerns much more than relating words; our knowledge includes conceptualisation of scenes, rhythm, sequential ordering, identities, and values [3].

Therefore a descriptive method of research was used. The reasons behind selecting this method are as follows:

1. To determine the factors of success/failure in relation to technology.
2. To establish the factors of success/failure in relation to perception.

The success or failure constitute one of the two dimensions that this paper seeks to define, the first dimension is the technology factor — what is permissible in terms of architectural design methodology- and the second dimension is the human factor scale represented by perception — what is permissible in term of expectation of user's perception.

Thus the objectives of the social–psycho tool methodology study are to:

1. Establish the level of awareness / understanding of privacy.
2. Establish the level of interest in privacy.
3. Establish the extent of barriers (human and technological) to provision of privacy.
4. Establish the level of satisfaction of sharing information and privacy measures.
5. Identify the most desired scenario of privacy measures.

The findings from the social–psycho methodology survey will form the basis for the evaluation of success/failure in realising strategies, policies and plans for privacy provision in distributed systems.

The followings six benchmarks are used as constructors of the social–psycho methodology survey questions:

1. User empowerment/user centric privacy.
2. User empowerment/transparent distributed system.
3. User space.
4. Developer space.
5. Effective scalability.
6. Key enablers.

TABLE

Framework factors hybrid privacy system.

dimension	surveyed	social–psycho-devices method	DS relationship
technology factor	developer	expert question	DS-to-human-to-DS
human factor	users	survey	human-to-human-to-DS

In Table the possible distributed system dependencies are formulated under the DS Relationship column and are DS-to-human-to-DS, which is an 'outwards' relationship and human-to-human-to-DS, which is, an 'inwards' relationship. social–psycho tool methods are divided into qualitative and quantitative outputs capturing dimensional factors from users and developers.

3. Discussion

As we make our way through everyday life, data is collected from each of us, frequently without our consent and over and over again without our comprehension. The question is how do system developers of DS provide for the privacy context so that applications are aware and responsive to the full context of human-computer interaction?

We pay our bills with credit cards and leave a data trace consisting of purchase amount, purchase type, date, and time [4]. Data is collected when we pay by check. Our use of supermarket discount cards creates a comprehensive database of everything we buy. When our car, equipped with a radio transponder, passes through an electronic tollbooth, our account is debited and a record is created of the location, date, time, and account identification [5].

Data sharing requires balancing many facets of privacy, security, and legal interests [6]. Anonymisation of data can mitigate privacy and security concerns and comply with legal requirements. Anonymisation is not invulnerable. However, countermeasures that compromise current anonymisation techniques can expose protected information in released datasets.

Progressively networking and security researchers are engaging in work that challenges our existing ethical frameworks [7]. If we are to continue to occupy a moral high ground in which we claim the benefits of our work as necessary and the risks of our work minimal, we need to more explicitly justify this reasoning to other researchers and society as a whole. In this paper, we proposed a new method HPTM that incorporates system developers and DS users to formulate, standardise and guide DS privacy provision. The relationship between DS developers and users under the guiding principle of conformity is divided into user expectation, legal requirements and distributed system risk strategy [7].

The HPTM method enables parsing of grammar based descriptors into socio–perceptive lexicon morphing conscious design of privacy-enabled systems. However, a range of dependencies exists surrounding system design and perception of privacy such as, spatiotemporal, lexicon attenuation, connection and not premeditated processes [8].

Let us consider a script running on a web server. The main functions of the script are to encrypt and then delete operating system log files responsible for capturing users IP and MAC addresses daily (see Fig. 2). In this case scenario the web server certainly provides a high degree of privacy assuming encrypted files are safe. However, unwanted visitors "Hackers" may benefit from log files deletion. Moreover, users' data holds extremely important data for system scalability and efficiency effort. Therefore, if we consider the same script to receive user interactive feeds of their privacy expectation through a keyboard or user interface (see Fig. 3), both objectives are feasible. Another example is an individual who is the only male born in 1920 living in a lightly populated area. This individual's age, gender, and postcode represent a unique instance among other data that the developers and the distributed system are unaware of, if revealed via his IP address he could be joined with a voter registry from the area to obtain his name, revealing his medical history.

Natural languages have a progression cycle of implicit characteristics that change into different semantics from its original lexical dynamics. In this, only connectionist interpretation may offer a traceable link in both socio–systems as well as behavioral domains. This is because DS are procedural by design, while socio–systems are connection-based. In some cases semantic attributes may survive the progression cycle, in which no explanation is available. Nevertheless, the poly-thematic paradigm offers opportunity for parsing grammar-based descriptors into socio–perceptive lexicon resulting in huge computational time saving.

In this HPTM method processing contextual stream of semiotics is the function of socio–systems via

connections, simultaneously for DS behavioral domains corresponding function is sensory. Schilit et al. [9] refer to context as 'location, identities of nearby people and objects, and changes to those objects'. In a similar definition [10], define context as 'location, identities of the people around the user, the time of day, season, temperature, etc. [11]' define context as 'the user's location, environment, identity and time [12]' enumerates context as 'the user's emotional state, focus of attention, location and orientation, date and time, objects, and people in the user's environment'. These definitions are similar in some part and vary considerably in others, such as Dey [12] definition of 'emotional state' that is difficult to apply.

However, a better approach will be to look at breaking down or adapting discreetness to the concept of 'Privacy expectation state' such that it becomes (need privacy, unaware, needless privacy and not sure of privacy needs). These four discrete values of 'privacy expectations state' are a lot easier to handle compared to the ambiguous definition by [12]. In a recent survey carried out by the UK Government showed that despite the availability of technology, participants still prefer to go to the government entity concerned to obtain information about services and conduct transactions. When asked by the researcher they stressed their concerns about their privacy. However, in contrast to the assurances by the UK Government and the money they spend, 30 percent of the participants considered themselves "realists" which is huge number that represents the missing link between citizens privacy and the UK Government online services initiative. Consumers' privacy is under considerable pressure from a number of threats including the harvesting of personal data and the processing and selling of data without the customer permission.

In a separate study by the consumer privacy organization (TRUSTe), 70 percent of online customers are aware that their browsing information may be collected by a third party for advertising and marketing goals, but only 40 percent are familiar with the term "behavioural targeting". Moreover, 57 percent of survey respondents are not comfortable with advertisers using browsing history to serve ads, even when that information cannot be tied to their personal information [13].

4. Conclusion

For several reasons this paper is relevant within security, access control and distributed systems. Firstly, and most importantly, this paper focuses on privacy policy in DS. This paper contributes to the scarce literature in privacy issues, while privacy today is the most talked about issue in the media and blogging websites. Privacy is the biggest concern for organisations and governments alike.

This paper has implications on the implementation of privacy provision strategies in DS. This paper showed privacy issues, terms and concepts in light of new approach and introduced radical concepts into privacy as

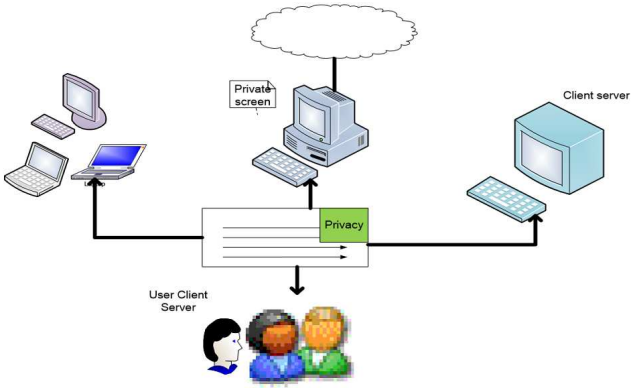

Fig. 2. HPTM method application illustrations.

Fig. 3. Illustration user privacy input captured.

such, realisation, perception and expectation. Moreover, the cognitive arena imposed a new paradigm on digital design as to why polythematic, lexica–technical, and hybrid–privacy modular forma exert a heuristic solution. We showed privacy realisation of users are linked to privacy terms interpretation. Further, guidelines for privacy disambiguation are defined; a privacy based framework is proposed to fill the gap in privacy implementation and to provide guidance in translating the vision and strategy into practice.

References

[1] P.C. Noble, *Met. Forum* **6**, 59 (1983).

[2] M.S.C. Thomas, M.H. Johnson, *Develop. Psychobiol.* **48**, 337 (2006).

[3] L. Carlson-Sabelli, H. Sabelli, M. Patel, K. Holm, (1992). *J. Group Psychoth. Psychodr. Sociom.* **44**, 143 (1992).

[4] S. Gong, M. Cristani, S. Yan, C.C. Loy, *Person Re-Identification*, Springer 2014.

[5] T. Xie, E. Martin, T. Yu, in: *Proc. 8th International Conference on Information and Communications Security*, 2006.

[6] T.W. Bynum, S. Rogerson, *Computer Ethics and Professional Responsibility: Introductory Text and Readings*, Blackwell Publishers, Cambridge (MA) 2003.

[7] E. Kenneally, M. Baily, D. Maughan, in: *Workshop on Ethics in Computer Security Research*, January 2010.

[8] M.S.C. Thomas, A. Karmiloff-Smith, *Psych. Rev.* **110**, 640 (2003).

[9] B. Schilit, M. Theimer, *IEEE Network* **8**, 22 (1994).

[10] P.J. Brown, J.D. Bovey, X. Chen, *IEEE Pers. Comm.* **4**, 58 (1997).

[11] N. Ryan, J. Pascoe, D. Morse, *Enhanced Reality Fieldwork: the Context-Aware Archaeological Assistant*, Eds.: V. Gaffney, M. van Leusen, S. Exxon, in: *Computer Applications in Archaeology* 1997.

[12] A.K. Dey, in: *AAAI 1998 Springer Symposium on Intelligent Environments*, Technical Report SS-98-02, 1998, p. 51.

[13] R. Arias, *Keeping Secrets: Internet Ethicist Lori Fena Explains Why the Biggest Cost of Going Online May Be Your Privacy*, Springer 1997.