Privacy by Design: Does It Matter for Social Networks?

Mohammad Badiul Islam, Renato Iannella

Privacy by Design: Does it matter for Social Networks?

Mohammad Badiul Islam [1, 2], Renato Iannella [1, 3]

[1] Computer Science Discipline, Faculty of Science and Technology, Queensland University of Technology
[2] NICTA (National ICT Australia), Queensland Research Lab, Brisbane, Australia.
[3] Semantic Identity, Brisbane, Australia.
mb.islam@qut.edu.au, ri@semanticidentity.com

Abstract: Privacy is an important component of freedom and plays a key role in protecting fundamental human rights. It is becoming increasingly difficult to ignore the fact that without appropriate levels of privacy, a person's rights are diminished. Users want to protect their privacy - particularly in "privacy invasive" areas such as social networks. However, Social Network users seldom know how to protect their own privacy through online mechanisms. What is required is an emerging concept that provides users legitimate control over their own personal information, whilst preserving and maintaining the advantages of engaging with online services such as Social Networks. This paper reviews "Privacy by Design (PbD)" and shows how it applies to diverse privacy areas. Such an approach will move towards mitigating many of the privacy issues in online information systems and can be a potential pathway for protecting users' personal information. The research has also posed many questions in need of further investigation for different open source distributed Social Networks. Findings from this research will lead to a novel distributed architecture that provides more transparent and accountable privacy for the users of online information systems.

Keywords: Privacy by Design, Social Networks, Privacy, Access Control, Mobile Social Networks, Distributed Social Networks, Open Source Social Networks, Diaspora, Clique.

1. Introduction

Privacy is an important component of the freedom of a person and plays a key role in protecting fundamental human rights. It is becoming increasingly difficult to ignore the fact that without appropriate levels of privacy, a person's freedom can be diminished. Failing to protect anyone's private, personal information affects everyone: friends, family, co-workers, relatives and so on. Any person has the right to share, disclose, access, rectify, delete, and block their own personal information unless there are legitimate reasons provided by the law [1]. However, privacy does not mean simply hiding information; it is the legitimate control over one's own personal information. Additionally, any person has the ultimate right and freedom to exit from the digital world. Without an individual's explicit consent, nobody has the right to access another person's personal information unless there are laws permitting access to in-

formation e.g. tax authorities may have access to income information from employers. This is particularly pertinent for Social Networks.

Users and consumers are beginning to show anxiety regarding privacy in different "privacy invasive" areas including Social Networks (SN), Cloud computing, Health records, Geo-location Services, Video Surveillance Cameras, Biometrics, Radio-Frequency Identifiers (RFID), Mash-up applications, Network monitoring and Whole body imaging, etc. Consumers' anxiety arises after experiencing incidents in their own lives that threaten their ultimate freedom. Not only users but also technology experts, researchers and industry professionals are expressing anxiety about privacy invasion areas. Unless we act now, privacy may not exist by the year 2020 [2].

However, ensuring privacy should not be a quick fix or a token add-on in the system. Privacy should be embedded in the system from the beginning of its design and development. Such a solution eventually might lead to a privacy friendly Social Network and attract more users in Social Networks.

This paper is organized into four parts. The first part defines privacy in Social Networks context whereas second part presents an overview of one of the leading "Privacy by Design (PbD)" principles. The third part presents case studies examining two open sources Social Networks Diaspora and Clique that have the objectives to be privacy-friendly. This part discusses how fare those Social Networks are meeting PbD principles. The final part discusses different barriers for adopting PbD principles. This paper is the first study to date to investigate how privacy can be ensured in Social Networks through the PbD principles and how far some of the claimed privacy-aware open sources Social Networks are meeting those principles.

2. What is privacy?

There is no rigid definition of privacy [3]. The information that uniquely identifies a person in some way is "Identifiable Information" and a person can probably detect the violation of privacy when others directly or indirectly abuse their identifiable information. Privacy can be defined as personal control over personal content and when a person fails to control personal identifiable information, this can become a privacy breach.

Privacy can be seen as a companion to access-control for Social Network users who are linked to other people. A person can allow access along with permissions for accessing personal content using different access control mechanism. The person can revoke the access control at their convenience.

Privacy can also be seen as part of managing PII such as their name, social security number or biometric records. A person can be traced or distinguished by the PII and linked or linkable to a specific individual, such as date and place of birth, mother's maiden name [3]. PII is managed in SN using traditional concepts, like access control, and new concepts, like "friends of friends". It is likely that PII is lacking comprehensive support across Social Networks. Eventually, privacy related issues for PII will be required to be harmonized and incorporated into existing Social Networks. In different research areas (e.g., database, data mining, network, security, social

science), the term "privacy" in social networks has quite different meanings. **Fig.1** represents multiple representation of privacy in Social Networks contexts.

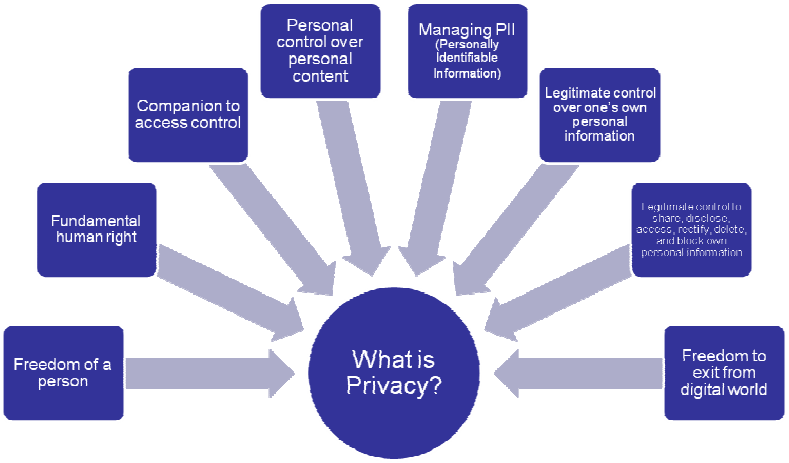

Fig.1. What is privacy?

3. PET and Privacy by Design Principles

Users want privacy but they seldom know “how to specify” and “what to seek” for their own privacy [4]. Embedded privacy-enhancing technologies (PETs) in the design level can be the solution for ensuring privacy from the beginning of a system development. The PET concept was developed in early 1990. PET stands for a coherent Information and Communication Technology (ICT) representation that protects privacy by eliminating or reducing unnecessary disclosure, collection, retention, sharing, trading of personal data without losing functionality of information systems. For example, use of personal data or preventing automated data capture through cookies, HTTP headers, web bugs, spyware using PET [5]. However, a PET is not necessarily something innovative or new; existing technologies can be accumulated into an information system and, subsequently, act as a PET [6].

PET might be considered as a supplement, complement or substitute for laws and regulatory bodies’ privacy protection schemes. Also the fact that PET might be considered as a magic bullet for solving the privacy problem is regrettable [7]. PET is necessary for Social Network privacy protection. However, PETs should complement existing regulatory and self-regulatory approaches since the law is, first and foremost instrument to incorporate legal principles into technical specifications. Additionally, legal, organizational and cultural conditions cannot be missing out of account in designing a PET approach to privacy protection.

PET concept alone may at times be found to be insufficient. For example, “positive-sum” paradigm was required to incorporate in ICT system which evolved the term to “PETs Plus” [5]. Additionally, it was emphasized to incorporate Fair Informa-

tion Practices (FIPs) directly into the design and operation of information systems which claimed to be part of the "Privacy by Design" philosophy.

Blarkom et al. [6] identified nine attention areas for compliance auditing: i) Intention and notification ii) Transparency iii) Finality principle iv) Legitimate grounds of processing v) Quality vi) Data subject's rights vii) Security viii) Processing by a processor ix) Transfer of personal data outside the EU and claimed that engaging all of these nines areas of attention is what is now commonly known as "Privacy by Design". Blarkom et al. also claimed that not all those nine areas can be implemented using PETs. For example, notification to the Supervisory Authority cannot be implemented since it is a purely administrative process. The other areas can, at least, partially, be achievable through PETs.

"Privacy by Design (PbD)" [5], is a concept that can be used to protect Personally Identifiable Information (PII). The PbD concept includes seven principles. System development costs increase substantially in later stages so it is useful if privacy can be incorporated from the design phase of a system. To comply with PbD concepts, this research suggests that seven principles are required to be incorporated into a system at the design level. One of the objectives of this research is to encourage engaging privacy in the system design level since in the later stage of system is extremely difficult to incorporate privacy, whereas privacy functionality can easily be engaged in the initial design stage of the system.

The term "Privacy by Design (PbD) [5] was conceived by Dr. Ann Cavoukian in early 1990. Gradually the author has modified the PbD principles down to seven key principles (Table **1**). So far, PbD principles remain at the conceptual stage. To comply with the PbD concept and to ensure privacy, a system has to be systematic, predictable and repeatable [5].

Table 1. Privacy by Design (PbD) principles [5] and analysis

#	Principle	Principle Details	Comment
1	Proactive not Reactive; Preventative not Remedial	Privacy protection comes before-the-fact, not after.	The principle underpinning how the information privacy will be observed and resolved before problems arise.
2	Privacy as the Default	No action is required on the part of the individual to protect their privacy. It is built into the system, by default.	The principle underpinning the rules is how the information will be collected and used with respect to individual privacy.
3	Privacy Embedded into Design	Privacy is integral to the system, without diminishing functionality.	The principle underpinning the mechanism is how to implement the system policies to ensure user privacy.
4	Full Functionality – Positive-Sum, not Zero-Sum	It is possible to have both such as privacy vs. security	The principle underpinning the methodology is how to create full functionality while protecting individual privacy.
5	End-to-End Security- Full Lifecycle Protection	PbD ensures cradle to grave, lifecycle management of information	The principle underpinning the assessment is how to secure information along with privacy.
6	Visibility and Transparency-	Trust but verify.	The principle underpinning the investigation is how the accountable organization

	Keep it open		will be open and honest with individual privacy.
7	Respect for User Privacy	Keep the system user-centric.	The principle underpinning the investigation is how to share, disclose or access, rectify, delete, and block information that is consistent with respect to individual privacy.

PbD principles can be used for adopting PET directly at the system design level. Adopting PbD principles will also increase the use of PET, FIP and implement nine attention areas [6] exclusively which may eventually increase user satisfaction and confidence in using the system. Additionally, PbD principles can ensure legitimate rights to control user's own private information which may assist in gaining confidence and trust to use the system. That may finally lead to an increase in the user reliability of the system and engage more users in Social Networking.

However, Privacy by ReDesign (Pb^RD)[i], an innovative approach and an extension to PbD might be applicable to established systems. PbD principles might not be engaged with previously developed and implemented system as like the developed system from scratch. The scope of this paper is limited to PbD principle. A future study investigating Pb^RD would be very interesting.

4. Case studies

This section includes two case studies for two claimed privacy-aware systems: Diaspora and Clique. This section also includes an assessment on how these test cases follow the PbD principles.

Case study: Diaspora

Diaspora [8] claims to be a privacy-aware, personally-controlled and distributed open source Social Network. Diaspora was created to replace centralized social networks since these have failed to protect the user's privacy. Diaspora also states its aim is to protect user information with a philosophy of "secure as much as you can, but no more". Diaspora claims to make private sharing easy and simple without increasing the user's burden. The Diaspora architecture (Fig. 2) includes a Server (Pod) to host user accounts (seeds) and claims that the seed is owned by the user which can then be used to aggregate other profiles, tweets or social data.

The Diaspora system has the attention of the media[ii] and some technologists [iii] [iv] claim that Diaspora might see users change from other well recognized Social Networks[v] . Hence, Diaspora has been selected for evaluating PbD principles as first test case. The privacy-aware Diaspora Social Network has been analyzed in terms of how it follows the PbD principles because it claims to be the first "privacy-aware" social network.

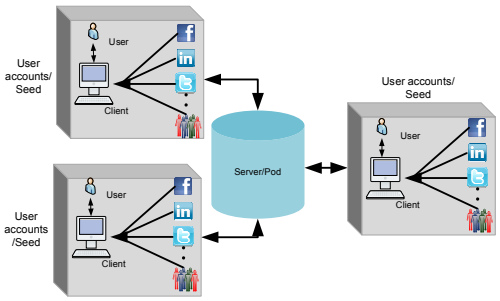

Fig. 2. Diaspora System including User, Client, user accounts and Server

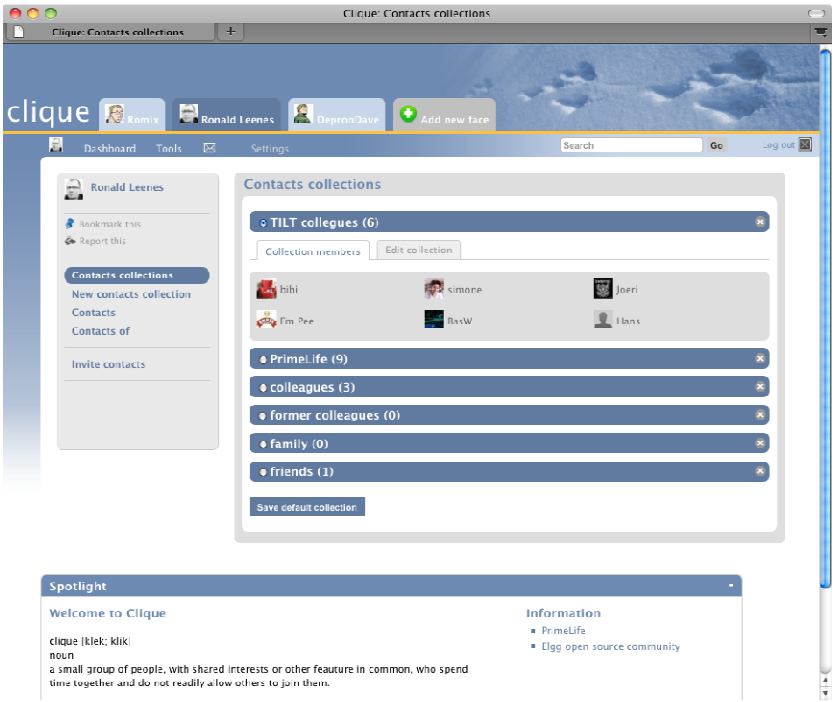

Fig. 3. Clique interface

Case Study: Clique

Clique[vi] claims to secure user privacy by enabling users to create their own set of faces or profiles. The faces or profiles can be defined as segregation in real life such as work, private or family faces [9] . The system also clusters contacts and claims to define accessibility of contact information by the contacts. The users are able to cus-

tomize audience segregation through their own set of faces and collections in their system. Clique is built using Elgg[vii] Open Source software making the source transparent and visible. Clique is produced through a research project Primelife[viii] funded by the European Commission's 7th Framework Program and illustrates how to reconcile privacy and sociality in social networks in a user-friendly way[ix]. Moreover, it claims that users use a system named "Scramble"[x] along with Clique. Scramble uses a hybrid encryption scheme for protecting the content from the platform provider and other unauthorized parties. The Clique has been selected for this case study because of its open source and primary worthwhile features. **Fig. 3** shows the interface of the Clique system.

Assessment of Diaspora and Clique

Table 2 shows how the Diaspora and Clique systems follow the PbD principles. Assessment of Diaspora and Clique has been designed on a 4-point Likert scale. If the Diaspora and Clique system feature does not comply with the PbD principles then it scores a "0", "Low Comply" scores "1", "Medium Comply" scores "2" and "Highly Comply" is "3". For example, Table 2 illustrates a Diaspora system feature which "Provides security levels such as 'None', 'Low', and 'High'" where highly complies with the PbD principles and scores a 3. On the other hand, "Produce a Privacy Impact Assessments (PIA) to outline the possible future privacy impacts" does not comply with the PbD principles and scores a 0. The second column "Assessment Criteria" in Table 2 demonstrates system features which are supported or not and which also assist to encode a "Privacy Score" for each test case.

As the next step, a set of "Assessment Criteria" is formulated. For each of the PbD principle- relevant, objective, complete and measurable criteria have been utilized to assess Diaspora and Clique systems. Each system has a set of features and has views on privacy on the system main page, along with Terms of Use (rights and responsibilities, roughly comparable to a privacy policy), "Wiki", "Frequently Asked Questions for users", "Developer Resources" and "Contributor Resources". Assessment criteria have been formulated from those available system features. Each PbD principle has a set of objectives, requirements, responsibilities and standards. Each assessment criterion has been formulated and classified according to the relevant objectives, requirements, responsibilities and standards for each PbD principle. Diaspora and Clique's system and privacy features have been mapped with each of the PbD principle features to produce a "Privacy Score" based on the earlier mentioned Likert scale.

Additionally, Table 3 shows the final assessment for Diaspora where the average of the privacy scores indicates the final assessment level of complying with the PbD principles. The final assessment of the Diaspora and Clique has been designed on a 4-point Likert scale. An approximate average privacy score of 0 –will give a final level of 'None', 1 is –'Low', 2 is –'Medium', and 3 is –'High' comply with the PbD principles. The exception in the final assessment scoring for values greater than '0' –will produce 'Low Comply' with the PbD principles. For example, an average score of 1.36 gives a final level 'Low Comply' for Diaspora and 'High Comply' for Clique in terms of 'Privacy as the Default'. **Fig. 4** represents the privacy Assessment comparison for Diaspora and Clique.

Table 2: PbD Principles [5] assesment for test cases

#	Principle	Assessment Criteria	Privacy Score Diaspora	Privacy Score Clique
1	Proactive not Reactive; Preventative not Remedial	Users are able to use own servers	3	0
		Provides flexibility for user to setup own server.	3	0
		Provides security level such as 'None', 'Low', and 'High'	3	3
		Produces a Privacy Impact Assessment (PIA) to outline possible future privacy impacts	0	0
		Produces Privacy Risk Assessment	0	0
		Documents Privacy policies & made them available to users &third parties	0	0
		Addresses personal information collection strategy in privacy policy	3	3
		Identifies and classifies personal Information such as private, protected or public information	3	3
		Classifies profiles such as personal, business or public profile	3	3
		Provides features for privacy awareness & trains user through System features	3	3
		Develops or uses universal, user-centric privacy symbols or icons that indicate how information will be collected & used	1	2
		Engages users to use provided privacy protections features	3	3
		Practices Fair Information collection policy	3	3
		Represents understandable form of user information	3	3
		Represents ongoing procedures for monitoring effectiveness over personal information.	1	2
2	Privacy as the Default	Ensures privacy using open source architecture	3	3
		Uses privacy model	0	3
		Considers encryption whereas possible	3	3
		Encrypts automatically user information	3	3
		Allows users to differentiate between roles	3	3
		Notifies user about implicit or explicit collection, use & disclose personal information	0	3
		Notifies user consequence of denying or withdrawing consent	0	2
		Notifies user types of personal information collection and methods of collections such as cookies or web beacons[xi]	0	2
		Monitors information access by third parties	0	3
		Abides by Global Privacy Standard	1	2
		Uses privacy protective default settings	2	3
3	Privacy Embedded into Design	Uses open source Privacy guard such as GNUPG or own designed privacy guard	3	3
		Uses built in privacy protections	3	3

		Provides quick & easy privacy setup process	0	3
		Ingrates fine-grained, cross-platform privacy controls	3	3
		Defines privacy requirements & security standards for provided services	3	3
4	Full Functionality – Positive-Sum, not Zero-Sum	Considers philosophy of "Secure as much as you must, but no more"	3	3
		Documents how information is used in a client and server side	1	2
		Accesses personal information easily by individual user information	3	3
		Provides solutions thus users are able to review, update & correct information	3	3
		Provides solutions thus users are able to control access to their personal information for other users and third parties	3	3
		Facilitates reporting mechanism for users	2	2
5	End-to-End Security-Full Lifecycle Protection	Maintains "Security by Default" as policy	3	3
		Handles end-to-end lifecycle protection using existence procedures	0	2
		Provides functionalities and policies for deleting user contents	0	3
		Provides functionalities and policies for redistributing user contents	0	0
		Maintains personal information retention time unless a justified business or legal reason	0	0
		Provides functionalities and policies for disposing user contents	0	0
		Provides functionalities and policies for disposing original, backup & archived information	0	0
		Provides functionalities and policies for retention of original, backup & archived information	0	0
		Provides functionalities and policies for redaction of original, backup & archived information	0	0
		Provides functionalities and policies for destructing original, backup & archived information	0	0
		Provides consistent security measures for personal Information	0	0
		Provides logical access controls such as access information considering level & type of information	1	3
		Provides restricted physical access controls for personal information	0	0
		Provides protected information transmission over Internet, over public and other non secure networks.	1	0
		Provides effective test procedures for security safeguards	1	2
6	Visibility and Transparency-Keep it open	Ensures open source code availability	3	3
		Provides transparent third party communication with server	3	3
		Provides transparent third party communication	3	3

		with client		
		Provides transparent personal information accesses by authorized person	3	3
		Notifies users implicit or explicit access personal information third parties	0	0
		Provides process to address inquiries, complaints, and disputes	0	0
		Uses direct relationship with users to promote privacy education	0	3
7	Respect for User Privacy	Contains a model for securing private communications and data between the server, client & user.	3	3
		Claims as trusted system	3	3
		Provides procedures for user content collection by third parties	0	0
		Confirms identity and authenticate individual user who are given access to other users	2	3
		Provides functionality to change information type such as public information to protected information	0	2
		Provides updating or correcting functionality personal information for users	2	3
		Provides appealing procedure for correction of denied correcting personal information.	0	0
		Provides sharing/disclosure procedures for personal information to third parties	0	0
		Notifies users for implicit or explicit sharing information with the third parties.	0	0
		Provides remedial action in response to misuse of personal information by the third parties	0	0

Table 3: PbD Principles [5] final assessment for Diaspora and Clique

System	PbD Principle	Average Score and Final Assessment Diaspora	Average Score and Final Assessment Clique
Principle 1	Proactive not Reactive; Preventative not Remedial	2.13 2-Medium Comply	1.87 2-Medium Comply
Principle 2	Privacy as the Default	1.36 1-Low Comply	2.73 3-High Comply
Principle 3	Privacy Embedded into Design	2.40 2-Medium Comply	3.00 3-High Comply
Principle 4	Full Functionality – Positive-Sum, not Zero-Sum	2.50 2-Medium Comply	2.67 3-High Comply
Principle 5	End-to-End Security- Full Lifecycle Protection	0.40 1-Low Comply	0.87 1-Low Comply
Principle 6	Visibility and Transparency-Keep it open	1.71 2-Medium Comply	2.14 2-Medium Comply
Principle 7	Respect for User Privacy	1.00 1-Low Comply	1.40 1-Low Comply

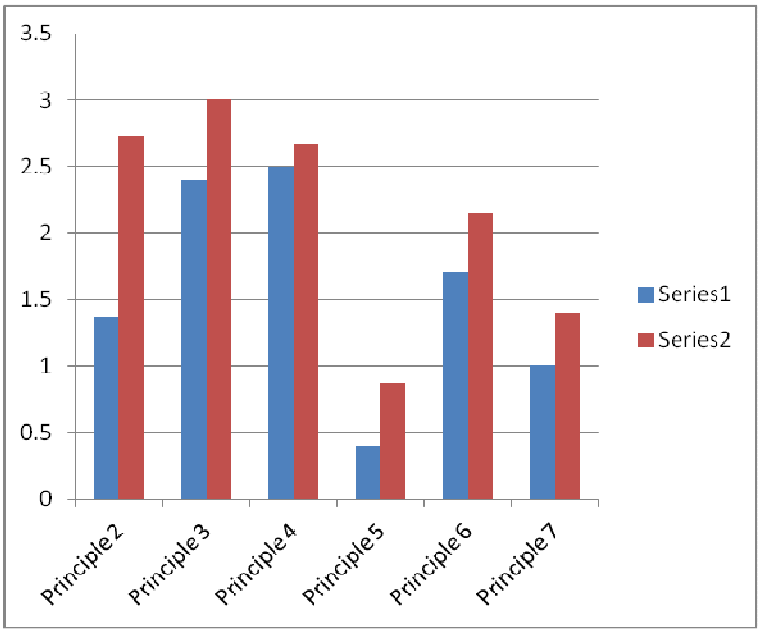

Fig. 4: Privacy Assessment comparison for Diaspora and Clique

The Diaspora system claims to be "Proactive not Reactive; Preventative not Remedial" and this is supported by the current case assessment. That is, the Diaspora system is a 'Medium Comply' with Principle 1. Neither Diaspora nor Clique produces a Privacy Impact Assessment (PIA) to outline possible future privacy impacts and therefore both score a '0' in that assessment criterion. Diaspora follows principle 1 more than Clique.

The Diaspora system claims to be a "Privacy as the Default" policy. However, only control over personal content can be mentioned that the advance user is able use own prepared server in Diaspora. The Diaspora system uses utilized encryption where possible with different security models and settings. But the average user may have no idea of encryption. After initial analyzing Diaspora features, the system can be better called a "Security by Default" system whereas the Clique system preserves privacy as the default and is therefore better than Diaspora in terms of the policy. Clique highly complies with principle 2.

The Diaspora claims to embed Privacy in their design though this depends on having an open source for the third party privacy guard GNUPG instead of its own architecture. This GNUPG could be a possible future privacy issue. Clique scores 3 and shows to comply highly with Principle 3. However, Clique uses Scramble tools such as Firefox[xii] browser add-on to protect information from service providers. Such a solution would be much more useful if privacy was embedded directly in their architecture.

Diaspora claims to provide full functionality in a win-win scenario and privacy and security are both ensured. However, how the user is to control access for other users is

not included. Diaspora documentation provides a multiple security access for other users, but this may not be sufficient to ensure privacy. The assessment of Diaspora indicates that 'Medium' complies with principle 4 whereas Clique 'Highly' complies with principle 4. However, both have a similar limitation for the reporting mechanism and documentation. More transparent documentation by both would help users establish a greater degree of satisfaction which would in turn engage more users.

One of the important PbD principles are that all data be securely destroyed at the end of its life cycle and provide end to end security. However, the Diaspora and Clique system did not seem to provide this end-to-end lifecycle protection including content deletion, alterations, updates and re-distribution policies or content access by the third parties. This assessment identifies Diaspora and Clique both as 'Low Comply' for Principle 5.

Visibility and transparency is one of the major goals of the Diaspora and Clique Social Network which they have demonstrated in the system, so far. Fig 4 demonstrates, there are similarities between the attitudes expressed by Diaspora and Clique and both show 'Medium Comply' with Principle 6.

The principle aim of developing Diaspora is to protect and respect user privacy. However, as with other distributed systems 'trust' becomes more complicated in the Diaspora system. Additionally, Diaspora and Clique are both 'Low Comply' with Principle 7 because no procedures exist for Information collection by third parties. Both systems are inadequate in procedure for correcting denied personal information or detail procedure for sharing/disclosure of personal information to third parties. Another problem is that they fail to take 'Notification of implicit or explicit sharing' into account. Further research needs to be undertaken to provide more respect to the user.

Overall, Diaspora and Clique followed only some of the PbD principles. At this stage, the Diaspora system does not truly support full privacy as it primarily substantiates securing personal content using encryption features. The Diaspora system can be better classified as following "Security by Design" principles instead of "Privacy by Design" principles. The Clique system is more focused on solving user privacy issues. More works need to be undertaken to respect user privacy for both systems. However, since privacy aware Diaspora and Clique Social Network are in the early development stages, there are opportunities to address these issues in the future.

5. Conclusion and future work

The PbD principles are more conceptual than a technique or framework. To comply with the PbD principles requires focusing on both regulatory and engineering issues [10]. Information and privacy commissioners can help solve the regulatory and legislation issues and for the technical issues, engineers and researchers should adopt the PbD principles in their information system design practices. However, the PbD concepts are not only limited to compliance or technical issues but also organizational and managerial issues. Business managers also have a definite responsibility for engaging PbD principles and should have clear perceptions of engaging PbD concepts in an organization ecosystem to avoid future privacy corruption issues. However, sever-

al challenges such as management, process and technology may affect the issue of privacy at the design level of information systems. The reluctance of management engagement, poor attitudes towards privacy and data protection, lack of appropriate privacy languages and uncertain benefits of privacy management, are all factors that impact on privacy support in online information systems. PbD can also be a matter of political choice [11]. Additionally, information system design with PbD principles may need to support different legislation requirements. Hence, harmonizing the understanding between regulators, engineers, business managers and politicians will assist in achieving the ultimate success of protecting user privacy when implementing the PbD concept in information systems.

It is hard to justify investment in privacy functionality until a severe incident occurs. An organization might use a "privacy policy" to protect themselves from negative outcomes. The organization may also fail to plan appropriate information system privacy support due to inadequate risk analysis as well as limited PIA and, fail to consider the value of personal information of their consumers. External pressure to share personal information with "privacy-friendly" third parties can also lead to different privacy-related issues.

The PbD principles indicate that a service provider needs to increase both the visibility and transparency of its operations. The service provider has to be accountable for any service provided through their information system such as external links or third party services. As the PbD principles can have different data protection legislation requirements [12], these barriers must be overcome to successfully the PbD principles and protect user information.

This paper has argued that the PbD principles are the current best instrument, to design protection for user privacy in online information systems. This research indicates that Diaspora, Clique and other open source distributed social networks need further investigation. The Distributed Friends and Relations Network[xiii], GNU Social[xiv], Lorea[xv], NoseRub[xvi], StatusNet[xvii] will next be investigated on how they address the PbD principles and which one better supports these. Such reviews of privacy aware information systems establish a greater degree of accuracy on PbD principle approaches and assist researchers to design explicit technical solutions for ensuring privacy in Social Network.

"Privacy by Design" is an emerging and important concept. The current findings add substantially to the understanding of how and why PbD principles can be used to protect user privacy in information system. The conclusion can be drawn from the present study that the "PbD" concept does matter for the design and operation of Social Networks to manage user privacy more effectively and transparently.

6. References

1. European Commission, A comprehensive approach on personal data protection in the European Union. 2010: Brussels.
2. Cavoukian, A. (2010) Landmark Resolution passed to preserve the Future of Privacy.
3. Krishnamurthy, B., I know what you will do next summer. 2010.
4. Shapiro, S.S., Privacy by design: moving from art to practice. Communications of the ACM, 2009. **Volume 53**(Issue 6): p. 27-29.

5. Cavoukian, A., Privacy by Design … Take the Challenge. 2009, Information & Privacy Commissioner of Ontario.
6. Blarkom, G.W.v., J.J. Borking, and J.G.E. Olk, Handbook of Privacy and Privacy-Enhancing Technologies. Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 2003.
7. Raab, C.D., The future of privacy protection. 2004.
8. Diaspora. Diaspora* Alpha. 2010 [cited 2011 17 February]; Available from: https://joindiaspora.com/.
9. Berg, B., et al., Privacy in Social Software. Privacy and Identity Management for Life, 2011: p. 33-60.
10. Davies, S. (2010) Why Privacy by Design is the next crucial step for privacy protection.
11. Le Métayer, D., Privacy by Design: A Matter of Choice, in Data Protection in a Profiled World, S. Gutwirth, Y. Poullet, and P. De Hert, Editors. 2010, Springer Netherlands. p. 323-334.
12. Lusoli, W. and R. Compañó, From security versus privacy to identity: an emerging concept for policy design? info, 2010. **Vol. 12**(Iss: 6): p. 80-94.

---

[i] http://privacybydesign.ca/content/uploads/2011/05/PbRD.pdf
[ii] http://www.nytimes.com/2010/05/12/nyregion/12about.html
[iii] http://www.kickstarter.com/projects/196017994/diaspora-the-personally-controlled-do-it-all-distr
[iv] http://blog.joindiaspora.com/2010/04/30/a-response-to-mr-villa.html
[v] http://www.techclump.com/diaspora-facebook-killer/
[vi] http://clique.primelife.eu/
[vii] http://www.elgg.org/
[viii] http://www.primelife.eu/
[ix] http://www.future-internet.eu/news/view/article/privacy-and-identity-management-research-presented-at-the-ict-event-2010-in-brussels.html
[x] http://www.primelife.eu/images/stories/primer/clique.pdf
[xi] http://www.allaboutcookies.org/web-beacons/
[xii] http://www.mozilla.org/
[xiii] http://info.dfrn.org/
[xiv] http://foocorp.org/projects/social/
[xv] http://lorea.org/
[xvi] http://noserub.com/
[xvii] http://status.net/