PP-SDLC
The Privacy Protecting Systems Development Life Cycle

Geoff Skinner, Elizabeth Chang
Curtin University of Technology,
Perth, WA, Australia.
geoff.skinner@newcastle.edu.au

Abstract

Many new Privacy Laws and Regulations have placed an increased importance on the correct design and implementation of information systems. This is an attempt to preserve and protect user and information privacy. Incorporating privacy regulations and guidelines into an active information system is often unsuccessful and ineffective. In addition, systems that have already progressed through the development life cycle can very expensive to change once implemented. We propose the integration of privacy preservation methodologies and techniques into each phase of the system development life cycle (SDLC). This is to preserve the privacy of individuals and to protect PII (Personally Identifiable Information) data. The incorporation of IT Security measures in each SDLC phase is also discussed. This is due to its direct relevance and correlation with information system privacy issues. The proposed methodology involves identifying the privacy and security issues in each phase. From there appropriate privacy protecting and security techniques are applied to address these issues. Special mention is made of the recently proposed Common Criteria. The CC is an international standard for IT Security for Information Systems. Specifically, this paper will analyse the way the Common Criteria currently deals with privacy in information systems, and what is needed to improve its current inadequate handling of information privacy.

Keywords: Privacy, Privacy Protection, Information Privacy, Systems Development Life Cycle (SDLC), Security, Trust, Common Criteria, Personally Identifiable Information (PII) privacy impact assessments (PIA).

1 Introduction

Privacy is something that everyone expects but usually only pursued on their own terms and conditions. Each individual or entity has their own ideas of privacy that varies not only in definition but also the degree to which each person desires it. For most individual cases they define it on a sliding scale dependant on a number of factors. These dependencies include: context; experience and knowledge; time frames and points of reference; personal interests; and operational, physical and mental environmental conditions. Not surprisingly then there is no single well established all-encompassing definition for privacy. However, what is well known is that privacy is a seen as being a fundamental need. Privacy is perceived as a right (moral and/or legal) of an individual entity [2]; such as a person, group of people, and/or organization. In this paper we primarily are concerned with the concept of information privacy [1]. Information privacy is a combination of privacy of personal communications and privacy of personal data [1]. Defined in more detail as '… the claims of individuals that data about themselves should generally not be available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.' [2]. Recent research and surveys [32] have suggested that a right to privacy is increasingly important to individuals. People, such as information system users, have concerns about how and why their personal information is collected, used and shared [3]. These concerns have only been escalating in response to the ongoing advances in computing, network, and data processing technologies [4].

Cyberspace, the Internet, or the World Wide Web depending on what term one prefers to use when referring to the 'online' environment out there, has been one of the primary factors for the growing concerns regarding information privacy. The frequent need to provide private data and the numerous requests for divulging additional personal information online has many people concerned. Users feel that they cannot trust the information requestors and collectors [5, 6] due to the potential risks to their privacy and personal information. The information flow is still unevenly distributed in information systems and related system processes. Users are expected to provide a wealth of their own personal information with little to no information being returned from the requestors and collectors. Users would like to be, and should be, informed on why it is being collected, how it will be used and by whom, and how long it is going to be stored for [7, 8]. These requests, and more frequently demands, have been known for sometime, resulting in a number of ways being suggested to address these privacy issues [17]. Approaches to the problem have included legal and regulatory methods, technical solutions, introduction of standards and certifications, and social, ethical and organizational controls [8, 9, 10, 11, 12, 15].

To date it seems that the most effective way of ensuring the preservation of privacy is through the use of privacy laws and regulations (see [13] for an international survey of privacy laws and developments). However, currently it is mainly the chance of breaching the privacy laws that is driving organizations to review their systems for privacy compliance. The organizational privacy fear is well stated in a recent security magazine article: 'What you don't know about privacy can hurt you' [14]. It goes on to state that the current number of privacy laws and bills is far too large for a single person, or role, within an organization to manage. Current privacy laws, while less than perfect, must still be adhered to. That is, '… both the public and private sectors require comprehensive and proactive privacy solutions' [16]. **We propose that the best privacy solutions should encompass a combination of all of the types of privacy methods.** Further, in order to achieve these goals and legal compliance, privacy issues need to be addressed at the enterprise-wide framework level. For the best chance of a privacy compliant system, privacy must be considered at the very early planning stages of a system development life cycle [18, 19]. This paper follows and expands this line of thought through the **proposal of the Privacy Protecting – Systems Development Life Cycle (PP-SDLC). We identify inadequacies in current information system privacy solutions and applications. From there we argue that for comprehensive privacy protection, all phases of the system development life cycle (SDLC) need to incorporate privacy components.** As has been noted, 'designers and builders of such systems frequently tend to treat privacy either as a secondary consideration or as an issue for future exploration' [11]. The results of such approaches are information systems that do not provide adequate information privacy.

We claim that building information systems that have strong privacy design principles, integrated and maintained throughout the systems life cycle will help instil user trust in the systems. Through the use of PP-SDLC users will be able to gain control and get the necessary information and feedback on their personally information and PII [19]. Additional inspiration for this research was due to a similar evolution with IT security and its incorporation into the SDLC [20, 21, 23, 24]. It has been shown that the inclusion of IT security in the SDLC normally produces a more effective security system and potential cost savings [22]. We feel that the same results are achievable for privacy, with its inclusion in all stages of the SDLC. With the **additional benefits of systems that are adaptable to the dynamic nature and changing landscape of privacy laws and regulations.** Our privacy enhanced system development approach is also guided by recent work and establishment of the Common Criteria (CC) [25]. The CC is a set of functional and assurance security requirements for evaluation of information systems [25, 26]. Brief mention of privacy principles are made in the FPR class. The class covers privacy concepts of anonymity, pseudonymity, unlinkability and unobservability. Another class deals with life cycle support (ALC). It has been identified that there is currently no 'Internationally accepted engineering

standards and methodologies for privacy'. **Through our proposed PP-SDLC we would hope to make a useful contribution to a revised Common Criterion with a more comprehensive coverage of privacy.** Other privacy related contributions to the Common Criteria are also being undertaken [27, 28].

The remainder of the paper provides background information that aids in understanding our proposed Privacy Protecting System Development Life Cycle. The details of our proposed PP-SDLC are presented along with discussion of suggested privacy related additions to the Common Criteria that are currently missing. Specifically, section 2 provides a more detailed examination of related research areas and concepts such as the SDLC and IT Security. It highlights where these current areas provide inadequate privacy protection. Section 3 provides deeper analyses of Information Privacy and inadequacies in current system design and development approaches to privacy protection. The Common Criteria and its treatment of privacy are also covered in this section. Section 4 defines and provides details of our proposed PP-SDLC solution. The conclusion is provided in Section 5 followed by a list of references.

2 Relevant Concepts and Related Research

2.1 Systems Development Life Cycle - SDLC

Privacy protection needs to be integrated into the development life cycle of all information systems [29]. **It is when the decisions are being discussed and made about data usage and system design that privacy needs serious consideration.** Both security and privacy are not just vertical 'silos' or components in systems architects. They are horizontal as well and therefore impact all aspects of system design, including the applications, technologies, data, and networks [30]. However, like privacy and security, definitions and approaches to the Systems Development Life Cycle are as equally diverse. The number of different approaches to the development life cycle each has their own merits and drawbacks. NIST SP 800-34 defines the SDLC as "the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation." [31]. That is, there is primarily five phases that make up the traditional or default standard of the SDLC. The phases are initiation, development/acquisition, implementation, operations/maintenance, and disposal. Other models include fountain, spiral, build and fix, rapid prototyping, incremental, and synchronize and stabilize. Regardless of the model, their focus is on the business processes, the functional requirements, and the economic and technical feasibility for information systems [21]. They ensure that the system is developed in accordance with the stated requirements, works effectively, is cost effective, and is maintainable [21]. We contend that in each model there is either no consideration for privacy, or where considered it is of a limited nature and ineffective.

In this paper and for the discussion of our proposals we have chosen a waterfall model hybrid to build our privacy features into. While dated and not as useful as it once was it does cover all of the key components required for delivering an information system. The waterfall model uses a linear sequence of stages/phases in which the output of each stage/phase becomes the input for the next. In the most commonly used modern waterfall model, the five phases are those listed above. The main noticeable difference in current SDLC models is a greater emphasis on the disposal phase. Partially driven by security and privacy concerns, proper disposal of the information system at the end of the life cycle has become increasingly important. However, the primary tasks in each of the phases remain more or less the same and are summarized in Table 1. Most organizations will use the general SDLC we are using here or will have developed a tailored SDLC that meets their specific needs [22]. This is driven by the evolving complexity of advanced and large information systems which require more complex SDLC models [24]. Due to the waterfall models liner nature and clear separation of phases it makes it easier for the integration and consideration of privacy

components. Each phase can be both analysed in an independent isolated context and also from a whole system perspective for a more complete privacy solution.

SDLC Phase	Tasks within Phase
Initiation	Need for system established and purpose of system is documented.
Development/Acquisition	Design, program, develop, or purchase system.
Implementation	Test and certification of system. Install/field system.
Operations/Maintenance	System performs its work. Enhancements are programmed and tested. Hardware and/or software is added or replaced.
Disposal	Resolve disposition (move, sanitize, dispose, archive, etc.) of information, software, and hardware.

Table 1: The five phases and primary phase tasks of the modern (waterfall) SDLC.

2.2 Information Technology Security

The National Institute of Standards and Technology (NIST) stated in a special publication that "… including security early in the information system development life cycle (SDLC) will usually result in less expensive and more effective security than adding it to an operational system." [20]. We propose that a similar approach to privacy provides the same type of benefits in addition to a host of others. Potential privacy benefits include the development of internationally accepted engineering standards and methodologies, organizations ability to differentiate products based on different privacy characteristics , creation of a mechanism for exercising appropriate due diligence and due care with respect to privacy, and lastly it satisfies a clear demand for better privacy protection approaches [27]. Often open to misinterpretation it should be made clear that security is not the same as privacy and vice-versa. Rather security is a foundation to privacy [28]. That is, while data security is essential to the achievement of privacy protection, security does not mean privacy [19]. Security is concerned with authentication, integrity, confidentiality, and non-repudiation aspects of data. Where as privacy can be viewed as being concerned about identity, linkability, and observability [31]. What is undeniable though is that privacy and security are very closely related and interdependent. Therefore, the steps taken to integrate security into the Systems Development Life Cycle should be by no means the final ones. **Privacy needs to be integrated into the life cycle along similar principles and from what we are aware has not been attempted. This paper and our current research plans to addresses these issue and provide the necessary solutions and methodologies for better privacy protection**.

There has been a fair amount of recent work done to date on implementing security in the SDLC. Two of the most detailed works [21, 22] have both used a 5 phase waterfall model approach for the SDLC. This is because of its simplicity and being an appropriate platform for discussion. Both works again highlight the economical benefits of security inclusion in the SDLC among a number of other advantages. It is stated in [21] that "The inclusion of security controls and measures during the process helps to ensure that: safeguards are part of the design, the developmental and/or acquisition costs include security, and progress can be tracked.". It should also be noted that throughout a particular SDLC the number and types of appropriate security controls may vary [22]. Additionally, the types of security controls will be influenced by the relative maturity of an organization's security architecture. Therefore in a similar line of thought, privacy controls will also be affected not only by an organization's security architecture but also their approach to privacy. Some organizations may even have their own privacy architectures already in place. This highlights another potential need and gives a distinct purpose to our work. In most cases an organizations approach and solutions to privacy are still in their infancy and by no means adequate, effective, or complete. **A privacy**

protecting system development life cycle, also integrating security principles, would provide organizations with the necessary architectural design tools to address privacy.

As the complete analysis and discussion of the implementation of (IT) security is beyond the scope of this paper, readers are directed to [20, 21, 22, 23, 24] for a more detailed coverage of that topic area. For immediate paper reference though the key security considerations for IT security in the SDLC is reproduced below from [22] in table 2.

	Initiation	Acquisition / Development	Implementation	Operations / Maintenance	Disposition
SDLC	Needs Determination: - Perception of a need. - Linkage of a need to mission and performance objectives. - Assessment of alternatives to capital assets. - Preparing for investment review and budgeting.	- Functional Statement of Need. - Market Research. - Feasibility Study. - Requirements Analysis. - Cost-Benefits Analysis. - Software Conversion Study. - Cost Analysis. - Risk Management Plan. - Acquisition Planning.	- Installation. - Inspection. - Acceptance Testing. - Initial User Training. - Documentation	- Performance Measurement. - Contract Modification. - Operations. - Maintenance.	- Appropriateness of disposal. - Exchange and sale. - Internal organization screening. - Transfer and donation. - Contract closeout.
Security Considerations	- Security Categorization. - Preliminary Risk Assessment.	- Risk Assessment. - Security Functional Requirements Analysis. - Cost considerations and Reporting. - Security Planning. - Security Control Development. - Developmental security Test and Evaluation. - Other planning components.	- Inspection and Acceptance. - System Integration. - Security Certification. - Security Accreditation.	- Configuration Management and Control. - Continuous Monitoring.	- Information Preservation. - Media Sanitization. - Hardware and Software Disposal.

Table 2: IT Security in the SDLC.

3 Privacy and the Common Criteria

3.1 Information Privacy

As mentioned there are a number of ways to define privacy but no single all-encompassing definition. What we do know is that privacy is something that every human being needs at some level and in some degree [17]. As such privacy encompasses a number of inter-related

values, rights, and interests unique to individuals [33]. This in turn has lead to the general understanding that privacy has a number of definitions often referred to as dimensions. The four standard dimensions that are widely accepted and reproduced, as is done hear, are the following (see [1, 33] for more details):

- Privacy of the person: refers to the integrity of an individual's body, and spans issues such as compulsory immunization, blood transfusions, or sampling fluids or tissues.
- Privacy of Personal Behaviour: refers to the rights of privacy relating to such matters as sexual preferences and habits, political activities and religious practises.
- Privacy of Personal Communication: the right to communicate with others without routine monitoring.
- Privacy of Personal Data: also called information privacy, this refers to the right to determine when, how and to what extent you will share personal information about yourself.

In an information systems context and of interest to this paper is that of Information Privacy. Information Privacy is best defined in [2] as '… the claims of individuals that data about themselves should be generally not available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.'. The provision of information privacy normally involves the protection of an individual's personably identifiable information (PII). PII data is information that can identify an individual user, such as name, home address, or e-mail address. PII, similarly to privacy, is also context and environmentally specific. That is, in some circumstances disclosure of certain information may reveal a users identity, while in other situations the same information may not. The onus, often by law, is and should be on system owners to determine when and how to protect PII data in their information systems.

One of the main threats to PII and personal privacy is surveillance. Surveillance is the systematic investigation or monitoring of an individual's activities or communications. Its primary purpose is to collect information about that individual, their activities, or their associates. In some cases this collection is justified, in others it is not. It is this grey area of data collection, use and disclosure that is at the centre of much privacy debate. The views that are gaining most support recently are the idea of limited collection or personal data minimization and what is called separation of duties. The first idea is rather fundamental and can be applied to any information process and system to enhance privacy. By minimizing the amount of personal data needed and collected there is less information being stored that could be misused at a later time. The second concept is more involved and relates to roles or duties carried out by people interacting with an information system. By making only certain kinds of data available to specific system/organizational roles, duties and/or tasks, it ensures that only the entities that should have access to data do have. For example, a specific duty may be responsible for all email communications with system users. Then by the separation of duty principle only that entity assigned to that duty would have access to user email addresses. Then possibly no other duty, role, and/or entity would have access to the email addresses. These two methods also provide increased protection against abuse by privileged system users.

Privacy protection generally comes in four major models [13]. They include Comprehensive Laws, Sectoral Laws, Self-Regulation, and Technologies of Privacy. To complement the privacy protection models the use of privacy policy management tools may be applied. The privacy management tools can be divided into five different instruments [17]. They are:

- Privacy Commitments: a more thorough form of self-regulation.
- Privacy Codes of Practice: codified policies stating commitments to the outside world and binding employees to the stated obligations.
- Privacy Standards: a common measurement or code for objective testing, along with conformity assessment procedures.
- Privacy Seals: The next step after certification to a standard. A commonly used mark or symbol awarded to an entity successful gaining certification and registration.

- Privacy Impact Assessments: A privacy focussed risk assessment tool for decision makers to address legal, moral and ethical issues arising from a proposal.

In an ideal scenario we advise that all of the models and management techniques are used together to ensure comprehensive privacy protection. In most situations this is not the case, often due to poor system design and planning. The results are inadequate privacy protection and systems that are not trusted or able to correctly manage personal information. It is apparent that organizations do not yet have the tools to allow them to fully manage and enforce privacy [12]. Through the use of a Privacy Protecting SDLC it is hoped that these issues will be addressed.

Over time it seems that many privacy policies have come to revolve around a number of key principles. These principles have themselves been primarily found on the Fair Information Practices (FIPs) [36] and the OECD Guidelines for Governing the Protection of Privacy and Transborder Data Flows of Personal Date [35] (also consult our own work on Information System Hippocratic Privacy Principles [37, 38]). In summary they require that all personal information must be:

- Obtained fairly and lawfully;
- Used only for the original specified purpose;
- Adequate, relevant and not to excessive to purpose;
- Accurate and up to date;
- Accessible to the subject;
- Kept secure; and
- Destroyed after its purpose is completed.

Problems still exists with policies based on these principles. They are still focussing on trying to protect the personal data rather than the person [1]. Like technological based privacy management tools, policies and regulations alone are not sufficient. Further, there has been little guidance provided to system developers and operators on how to implement and comply with all the privacy guidelines and rules [5]. What is needed is to ensure that privacy is a central design issue in its own right [8]. We feel that the best way to achieve this is through the incorporation of privacy into all stages of the SDLC.

3.2 The Common Criteria

The CC (Common Criteria) is an international initiative for combining the best aspects of existing criteria for the security evaluation of information technology systems [25]. While it mainly focuses on criteria for the evaluation of IT security consideration is given to privacy in information systems. The function of the included privacy class (FPR) is to provide a user protection against discovery and misuse of identity by other users. The greater function of the Common Criteria is a contribution to the development of an international standard. Version 1.0 was published as early as 1996 after work had started in 1993. Version 2.0 was produced in April of 1998. It became ISO International Standard 15408 in 1999. The CC Project subsequently incorporated the minor changes that had resulted in the ISO process, producing CC version 2.1 in August 1999 [40]. **Its handling and inclusion of privacy is the reason for its inclusion in this paper. It is hoped that our research and work on the PP-SDLC will make a useful contribution to the CC. It is felt that in its current state privacy is not adequately covered with sufficient importance and detail.** Part of its privacy shortcoming is its limited scope of privacy concepts. The CC only deals with the privacy areas of Anonymity, Pseudonymity, Unlikability, and Unobservability referred to in the CC as families.

The four privacy families covered in the CC are clearly insufficient to meet all of the privacy requirements [27]. While the CC deals with the main metrics in privacy of identity, linkability and observability [28], it does not discuss other important privacy considerations such as:

- Accountability

- Identifying purposes
- Inform (prior to consent) and Consent
- Limiting collection, use, disclosure, and retention
- Accuracy and Openness
- Individual Access

Our work is not focussed on trying to directly modify the Common Criteria, but rather the development of a PP-SDLC. Once reviewed and updated it could be integrated into potential improvements and additions to the privacy areas of the Common Criteria. We have found other groups currently working on formal extensions to the Common Criteria. Their work is an aimed at having the CC cover a much broader spectrum of privacy concepts [27, 28]. Their recent contributions have provided valuable additional inspiration for our own research in this area.

4 The PP-SDLC

As discussed in the previous section there are a number of methods for privacy protection and management. However in the past privacy tools have been applied in an ad-hoc way, or in a piecemeal fashion. They have been used to address specific immediate privacy issues with no real long term vision. Treating privacy as a secondary consideration or as an issue for future exploration during system design does not provide an effective level of privacy protection. Addressing small parts of privacy problems resulting from poor design and inadequate privacy tools can only lead to further potential privacy issues. **Privacy should be a fundamental design consideration, and therefore must be integrated into every phase of the Systems Development Life Cycle**. This section details our novel solution to this problem, and it has been termed the Privacy Protecting – Systems Development Life Cycle (PP-SDLC). It aims to incorporate all models of privacy protection into an Information System. This includes accommodating the ever changing landscape of Comprehensive and Sectoral Privacy Laws. Secondly, it will include the ability for continual Self-Regulation, Certification and Seals of the system and processes. Thirdly, it will allow ongoing use and integration of the latest Technologies of Privacy that are available at system design, implementation and maintenance time. **The core of the idea is to incorporate the most promising privacy research results and tools, including our own unique contributions and ideas, into a systems design methodology, structured as a privacy protecting SDLC.**

4.1 Privacy Design Principles and Concepts

Before any system can be designed or initiated the key privacy principles and design methodologies need to be identified. Many of the current privacy regulations and guidelines are based on the on the Fair Information Practices (FIPs) [36] and the OECD Guidelines for Governing the Protection of Privacy and Transborder Data Flows of Personal Date [35]. These principles have been listed in section 3.1 and will not be reproduced here. However, it has been identified that these principles are not enough, as they focus on data protection rather than personal privacy. Therefore more recent research has found a number of more promising approaches to privacy protection that should be used to compliment the foundation principles. The most significant of these is the idea of personal data minimization. That is, in designing an information system, at every stage of the system processes the designer should look for ways to minimize the need for, the collection of, and use of personal data, especially PII. Our own work [37, 38] also can make a useful contribution in the use of anonymity in the system for personal information where ever possible. So in addition to data minimization practises, designers should also, where ever possible, keep all data transactions anonymous. The idea here is that anonymous transactions could not and should not be traceable back to an individual. Better personal identity protection is achieved by systems designed for personal data minimization and anonymous data maximization. **We term this privacy design**

principle the 'PDM-ADM Design Rule'. From what we are aware, we are the first to couple these two concepts into one privacy design principle for use in Information Systems.

Another useful privacy design principle that has been previously proposed is what we refer to as the Four Privacy C's [5]. That is '… system designers will be well served if they consider the dimensions of comprehension, consciousness, control, and consent when building privacy-enhanced systems.' [5]. They are privacy design dimensions that mainly deal with the handling of PII data, a special 'set' of personal information. Each of these dimensions is reproduced in Appendix A from [5]. In summary format however they are as follows:

- Comprehension: to understand or know about the privacy aspects of the system.
- Consciousness: to be aware or informed by the system of what is happening.
- Control: the ability to manipulate or be empowered with ownership over your own personal data.
- Consent: to agree to what is done with your personal data.

Along similar lines of thought but presented is a slightly different perspective is the ideas of feedback and control [8]. Control is defined as 'Empowering people to stipulate what information they project and who can get hold of it' [8]. Feedback is defined as 'Informing people when and what information about them is being captured and to whom the information is being made available' [8]. The similarities between the two schemes are obvious with Feedback in the second approach corresponding to Comprehension and Consciousness in the first. Similarly, control in the second encompasses control and consent in the first. The second approach does take the concept further and states that '… systems must be explicitly designed to provide feedback and control … ' [8] for at least a number of user and system behaviours. Those perceived behaviours are as follows:

- Capture: What kind of information is being picked up?
- Construction: What happens to the information?
- Accessibility: Is information public, available to particular groups, certain persons only, or just oneself?
- Purpose: To what uses is information put?

A more detailed framework discussing these behaviours along with a set of criteria that is used to design a privacy protecting information system framework in reproduced from [8] in Appendix B. Appendix C in also included that provides an alternate set of privacy design principles that is very complete and covers many of the areas already mentioned. The principles were developed by the Ontario Government of Canada [19]. In turn they were based on principles from the Freedom of Information and Privacy Act (FIPPA), CSA Model Privacy Code, and the Fair Information Practices.

The Accessibility behaviour mentioned in the preceding paragraph also highlights another important proposal in privacy design principles. This approach is often referred to as the separation of duty, in our own research it is coupled with the additional separation of data concept. In this design approach the system data storage is firstly separated by type. For example it could be divided into operational, transactional, auditing, and personal categories. Secondly, system and data access is divided by the duty, tasks and/or roles of system entities (users and/or processes). The objective is to not only to increase system privacy in general but provide improved protection from potential privileged user abuse. Once these separation principles are designed in, the fact should be made transparent. Transparency as a design philosophy can help people ensure that information about them is not used in a way that is contrary to legally permissible purposes. People are comfortable about information collection provided they know that it is happening and what is happening to it [4].

Transparency has become a popular design approach to aid privacy protection. It is mentioned in [17] along with a number of other privacy 'lessons'. Those lessons are listed in [17] and include:

- Learn from experience elsewhere.

- Beware the perception of 'Big Brother'.
- Resist the temptation to identify citizens just for the sake of it.
- Anticipate, rather than react to, privacy events.
- Be Transparent and seek consultation.
- Enhance Trust.
- ***Design Privacy In.***

It is this last lesson that we feel is of most importance and potential benefit. As stated in [17]:

'The most significant challenge for the privacy movement today is less a legal and regulatory one, but more one that ensures that those who build information systems, and negotiate the standards upon which they are developed, are sufficiently conscious of the privacy implications of what they are doing.'

It may be impossible to hope that at every level of a system development life cycle the people involved will have a solid privacy comprehension and appreciation. However, if the standards and methodologies they are following to carry out their work have privacy as one of the central considerations then there is hope for better privacy protection. Another of our contributions will be the fact that individuals involved at all stages of the life cycle will not need to know the intricate privacy laws, regulations, technologies, etc. It will be built in to the procedures they are following and ensure information systems with good privacy protection.

4.2 Privacy Protecting – Systems Development Life Cycle

With so many tools in the privacy "toolbox", each of which are necessary, but none sufficient on its own, we need a set of procedures to integrate them all together. Our main contribution to this problem is the PP-SDLC. This section provides a detailed breakdown of each phase in the SDLC with our corresponding privacy measures that need to be taken in each phase. The result is our PP-SDLC.

4.2.1 Initiation

The initiation phase begins with a determination of need the system along with an initial definition of the problem to be a solved. Once completed, the following privacy tasks and considerations must be performed:

- Perform initial PIA. The PIA is fast becoming one of the most important processes for privacy evaluation. It is designed to guide system owners and developers in assessing privacy through the early stages of development. The one performed at this phase is only a preliminary version for initial system specifications and requirements.
- Perform Data Sensitivity Assessment. This is a review of all information, potential damage, laws and regulations, threats, environmental concerns, security and privacy characteristics, and organizational policy and guidance.
- Perform privacy design principles requirements analysis (Appendix C):
    - Planning, documenting and preliminary proposals and requirements for PII that needs to be collected by the system along with the purposes for its collection.
    - Planning, documenting and preliminary proposals and requirements for PII and personal information uses by the system. This includes system processes, other systems interacting with the new system and using PII and personal information, and system users.
    - Planning, documenting and preliminary proposals and requirements for PII and personal information retention periods and reasons for the lengths of those period.
    - Planning, documenting and preliminary proposals and requirements for security safeguards that will be used to protect PII and personal information.
    - Planning, documenting and preliminary proposals and requirements for entities that will have access to the PII and personal information. This would also involve the early separation of duty/tasks/roles/data in the system.

    - Planning, documenting and preliminary proposals and requirements for system openness or transparency. This in regards to privacy tools and system processes that apply to the management of personal information.
    - Planning, documenting and preliminary proposals and requirements for uses being able to access their personal information.
    - Planning, documenting and preliminary proposals and requirements for keeping PII and personal information up to date and accurate.
- Preliminary evaluation and feasibility review for required Privacy Management Tools. Initial planning for the use of Privacy Management tools and requirements. This includes Laws, Regulations, Code of practice, privacy certifications, technical approaches, etc.
- Perform preliminary Risk Assessment and Privacy Implementation Plan.
- Data Privacy Categorization for the proposed system. After the data in the system has been separated then it can be categorized by the level of privacy and security protection it requires.
- Initial assessment of Privacy requirements Security requirements. This is to see if there are any conflicting interests. If so they need to be addressed and resolved.
- Brief all developers and designers on the values of the Four C's of Privacy Design. That is, the dimensions of comprehension, consciousness, control, and consent.

2.2.2 Development/Acquisition

- Personal Data Minimization and Personal Data Anonymous Maximization. This is the application of the PDM-ADM Design Rule discussed in section 4.1.
- Perform a formal Risk Assessment. Used to identify threats to and vulnerabilities in the information system.
- Perform a formal PIA.
- A Privacy functional requirements analysis. Used to consider the system privacy environment, including the enterprise information privacy policies and the enterprise privacy architect.
- Privacy assurance requirements analysis. In the future this would hopefully include consultation with the Privacy enhanced Common Criteria. It is used to address the activities and assurances needed to produce the desired level of confidence that the information privacy will work correctly and effectively.
- A privacy plan. Used to address the current and future proposals for information privacy and ensure they are fully documented.
- A study of the privacy controls and privacy management tools. This is to ensure that they are designed, developed, and implemented.
- A privacy test and evaluation plan. This should be developed for the privacy controls that can be evaluated prior to deployment.
- Incorporate Privacy Design Principles into the system (Appendix C).
- Design and develop suitable feedback and control privacy mechanisms into system.

4.2.3 Implementation

- Inspection and Acceptance. This is necessary to ensure that the functionality described in the specifications has been included in the deliverables.
- Obtaining initial user consent on personal information collection, use, disclosure and retention.
- Ensure users informed on systems processes and meaning of them (transparency). Also ensuring users or informed on how to access their personal information and ensure it is up to date and accurate.
- Privacy controls and system are integrated and configured.
- Security safeguards are activated to ensure protection of personal information and PII.
- First stages of gaining privacy commitments, codes, certifications and seals, accreditation, standards compliance and self and/or external regulation compliance.

- Staff privacy training and creation of in-house privacy department or positions if required.
- Ongoing initial testing and evaluation according to documented plans.

4.2.4 Operations/Maintenance

- Completion and ongoing updating of privacy commitments, codes, certifications and seals, accreditation, standards compliance and self and/or external regulation compliance.
- Legislative, legal, regulatory watch for any new privacy requirements.
- Privacy configuration management and control.
- Controls monitored through periodic testing and evaluation, audit logs analysed.
- New information privacy protection methods, controls and management tools evaluated and integrated into system for improved privacy.
- Observing and implementing data retention periods privacy controls.

4.2.5 Disposal

- Information, including personal and PII, retained as necessary. Certain legal and regulatory conditions may require the preservation of certain information.
- Media sanitization and personal information deletion.
- Secure dispose of old software and hardware.
- User feedback on system deactivation and disposal. Inform the users what will happen to their personal information during this phase.

4.2.6 Phase Summary

Consult Appendix D for a tabular summary of the PP-SDLC Privacy Phase Requirements.

5 Conclusion

This paper has presented the idea of the Privacy Protecting – Systems Development Life Cycle (PP – SDLC). In the past privacy has been treated as a secondary consideration or one for future exploration. We have shown that Information Privacy is a system design principle in its own right and of significant importance in all phases of the SDLC. As with current approaches to security, it is more beneficial to include privacy considerations early in the design and development process. Trying to add it at a later stage can be expensive and only serves as an ad-hoc piecemeal solution, rather than a complete system solution. As a result we have information systems that are still inadequate and ineffective in their handling of information privacy. To ensure individuals can make informed decisions about the purposes for which their personal information is collected or disclosed we need to design and develop systems built of privacy design principles. We have detailed a useful number of privacy principles that should be used during information system design.

Another benefit of our PP-SDLC is in its usefulness for system developers and designers. It is impossible to expect that all the people involved in the phases of a SDLC will be proficient with the numerous privacy principles, laws, regulations, codes, and guidelines. What we can expect however is that system developers, designers, and other people involved in the project will know how to follow instructions and methodologies. By using the PP-SDLC the individual does not need to be a privacy expert. Rather, they are guided in good privacy design principles by following those provided in the PP-SDLC. These benefits then flow on the system users and also the organizations owning the system. Pursuing Privacy Seals and Privacy Certifications as recommended in the PP-SDLC increases users confidence in the system, and provides brand recognition and differentiation for competitive advantages. We are hoping that the benefits of the PP-SDLC are clear, and may also be of use for privacy enhancements of the Common Criteria.

References

[1] Clarke, R. (1999), Introduction to Dataveillance and Information Privacy, and Definitions and Terms. *http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.*

[2] Clarke, R. (1998), Internet Privacy Concerns Confirm the Case for Intervention. *ACM 42, 2 (February 1999) 60-67.*

[3] Poneman, L. (2004), Top 5 Privacy Issues for 2005. *Computerworld (December 2004), http://www.computerworld.com/printthis/2004/0,4814,98448,00.html.*

[4] Weitzner, D.J. (2004), Openness as a Privacy Protection Strategy. *Computerworld (Octoberr 2004), http://www.computerworld.com/printthis/2004/0,4814,96827,00.html.*

[5] Patrick, A.S. and Kenny, S. (2003), From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. *Privacy Enhancing Technologies Workshop (PET2003), Dresden, Germany, March, 2003.*

[6] Palen, L. and Dourish, P. (2003), Unpacking "Privacy" for a Networked World. *CHI 2003, April 5-10, 2003, Ft. Lauderdale, Florida, USA.*

[7] Kobsa, A. (2002), Personalized hypermedia and international privacy. *Communications of the ACM, 45(5), 64-67.*

[8] Bellotti, V. and Sellen, A. (1993) Design for Privacy in Ubiquitous Computing Environments. *Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93).*

[9] Schwartz, P.M. (1999), Privacy and Democracy in Cyberspace. *52 VAND. L. REV. 1609, 1610-11 (1999).*

[10] Schwartz, P.M. (2000), Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices. *Wisconsin Law Review, 2000.*

[11] Patil, S. and Kobsa, A. (2004), Preserving Privacy in Awareness Systems. *Wissen in Aktion 2004.*

[12] Powers, C.S., Ashley, P., and Schunter, M. (2002), Privacy Promises, Access Control, and Privacy Management. *Third International Symposium on Electronic Commerce (ISEC'02), October 18 - 19, 2002 , Research Triangle Park, North Carolina.*

[13] Privacy and Human Rights 2003 – An International Survey of Privacy Laws and Developments. *Electronic Privacy Information Centre and Privacy International.*

[14] Aftab, P. (2004), The Privacy Lawyer: What You Don't Know About Privacy Can Hurt You. *Information Week – Security, July, 2004. http://www.informationweek.com/shared/printableArticleSrc.jhtml?articleID=22104468.*

[15] Goldberg, I. (2002), Privacy-enhancing technologies for the Internet, II: Five years later. *PET2002, San Francisco, CA, USA 14 - 15 April 2002.*

[16] SRA International, Privacy Protection. *http://www.sra.com/services/index.asp?id=590.*

[17] Bennett, C.J. (2001), What Government Should Know about Privacy: A foundation Paper. *Information Technology Executive Leadership Council's Privacy Conference, June 19, 2001.*

[18] Office of the Ontario Information and Privacy Commissioner and the United States Department of Justice (2000), Privacy Design Principles for an Integrated Justice System – Working Paper. *http://www.ojp.usdoj.gov/archive/topics/integratedjustice/pdpapril.htm*

[19] Government of Ontario (2000), Privacy Design Principles – Personal Information. *23 May, 2000. http://www.gov.on.ca/MBS/english/fip/pub/pdp.html.*

[20] NIST Special Publication Executive Summary 800-64 (2003), SP 800-64 Security Considerations in the Information Systems Development Life Cycle. *NIST October 2003. http://www.iwar.org.uk/comsec/resources/security-life-cycle/.*

[21] Wlosinski, L.G. (2002), Implementing Information Technology (IT) Security in the SDLC – A 'How To' Approach. *SANS Institute 2003, part of the GIAC practical repository.*

[22] NIST Special Publication 800-64 (2004), Security Consideration in the Information Systems Development Life Cycle. *Rev. 1 June 2004 NIST Special Publication 800-64.*

[23] NIH SDLC (2002), NIH SDLC IT Security Activities Matrix. *CIT 2002, http://wwwoirm.nih.gov/security/nih-sdlc.html.*

[24] NIST CSD – Computer Security Division (2004), Info Security in the SDLC. *Computer Security Resource Centre (CSRC), August 30, 2004.*

[25] Common Criteria (2004), Common Criteria for Information Technology Evaluation. *January 2004, http:// www.commoncriteria.org.*

[26] Malnick, K. (2003), Common Criteria Evaluations for the Biometrics Industry. *2003 West Virginia High Technology Consortium Foundation.*

[27] Zatychec, P. (2004), Testing and Evaluation of Privacy Enhancing Technologies using the Common Criteria. *EWA-Canada Ltd.*

[28] Hope-Tindal, P. (2003), Privacy and the Common Criteria. *15th Annual CSE ITS Symposium, May 14, 2003.*

[29] Office of the Chief Information Officer (2002), SBA Privacy Impact Assessment for Fixed Assets Accountability System. *Freedom of Information/Privacy Acts Office Washington DC, USA.*

[30] Hope-Tindal, P. (2001), Managing Privacy and Security Risks Through Architecture Design: An Enterprise Privacy View. *Data Privacy Partners, November, 2001.*

[31] Friedman, M. and Wlosinski, L. (2003), Integrating Security into the Systems Development Life Cycle (SDLC). *Centre for Information Technology, May 22, 2003.*

[32] IBM Research Report (2003), Views of Privacy: Business Drivers, Strategy, and Directions. *IBM Research Division, September 22, 2003.*

[33] Ontario Management Board Secretariat (2001), Privacy Impact Assessment Guidelines. *http://www.gov.on.ca/mbs/english/fip/pia/pia.html.*

[34] Hes, R. and Borking, J. (2000), Privacy-Enhancing Technologies: The path to anonymity. *Registratiekamer, The Hague, August 2000.*

[35] Baker, S.A. (1999), Privacy, Anonymity and the Attack on Authentication Technologies. *Steptoe and Johnson, Washington, DC, USA.*

[36] U.S. Department of Labour (2002), U.S. Department of Labour E-Government Strategic Plan – Security and Privacy. *http://www.dol.gov.*

[36a] Federal Trade Commission (FTC) (2003), Fair Information Practise Principles. *Federal Trade Commission Online Privacy, http://www.ftc.gov/reports/privacy3/fairinfo.htm.*

[37] Skinner, G. and Chang. E (2004), Hippocratic Policies in Computer Based Collaborations. *PHCRC 2004, Newcastle Australia, 2004.*

[38] Skinner, G. and Chang. E (2004), Shield Privacy Hippocratic Security Method for Virtual Community. *IECON2004, The 30th Annual Conference of the IEEE Industrial Electronics Society, Nov 2-6. 2004 Korea.*

[39] Clarke, R. (1999), Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. *http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.*

[40] NIST Security Division (2004), Common Criteria for IT Security Evaluation. *July 28, 2004, http://csrc.nist.gov/cc/index.html.*

[41] Clarke, R. (2003), Privacy Impact Assessments. *http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html.*

[42] Radack, S. (2003), Security Considerations in the Information System Development Life Cycle. *http://www.itl.nist.gov/lab/bulletns/bltndec03.htm.*

Appendix A – The Four C's of Privacy Requirements

The table below is reproduced from a list of requirements provided in reference [5]:

Patrick, A.S. and Kenny, S. (2003), From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. *Privacy Enhancing Technologies Workshop (PET2003), Dresden, Germany, March, 2003.*

Category	Requirements
Comprehension	• Comprehend how PII is handled. • Know who is processing PII and for what purpose. • Understand the limits of processing transparency. • Understand the limitations on objecting to processing. • Be truly informed when giving consent to processing. • Comprehend when a contract is being formed and its implications. • Understand data processing rights and limitations.
Consciousness	• Be aware of transparency options. • Be informed when PII is being processed. • Be aware of what happens to PII when retention periods expire. • Be conscious of rights to examine and modify PII. • Be aware when information may be collected automatically.
Control	• Control how PII is handled. • Be able to object to processing.

	• Control how long PII is stored. • Be able to exercise the rights to examine and correct PII.
Consent	• Give informed agreement to the processing of PII. • Give explicit permission for a Controller to perform services being contracted for. • Give specific, unambiguous consent to the processing of sensitive data. • Give special consent when information will not be editable. • Agree to the automatic collection and processing of information.

Table 4: Essential HCI Privacy Requirements

Appendix B – Privacy Feedback and Control Framework Design Factors

The tables below are reproduced from a list of requirements provided in reference [8]:

Bellotti, V. and Sellen, A. (1993) Design for Privacy in Ubiquitous Computing Environments. *Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93).*

	Feedback About	Control Over
Capture	When and what information about me gets into the system.	When and what not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
Accessibility	Which people and what software have access to the information about me and what information they see or use.	Who an what has access to what information about me. I can set automatic default behaviours and permissions.
Purpose	What people want information about me. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is feasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal use.

Table 5: Feedback and Control for user and system behaviours.

Privacy Criteria	Description
Trustworthiness	Systems must be technically reliable and instil confidence in users.
Appropriate Timing	Feedback should be provided at a time when control is most likely to be required and effective.
Perceptibility	Feedback should be noticeable.
Unobtrusiveness	Feedback should not distract or annoy.
Minimal Intrusiveness	Feedback should not involve information which compromises the privacy of others.
Fail-safety	In cases where users omit to take explicit action to protect their privacy, the system should minimise information capture, construction and access.
Flexibility	What counts as private varies according to context and interpersonal relationships. This mechanisms of control over user and system behaviours may need to be tailored to some extent by the individuals concerned.

Table 6: Privacy Design Criteria for Feedback and Control.

Appendix C – Privacy Design Principles

The information provided below is reproduced from reference [190:

Government of Ontario (2000), Privacy Design Principles – Personal Information. *23 May, 2000. http://www.gov.on.ca/MBS/english/fip/pub/pdp.html.*

1. Accountability.
2. Identifying Purpose for Collecting Personal Information.
3. Limits for Collecting Personal Information.
4. Obtaining Consent.
5. Limits for Using, Disclosing, and Retaining Personal Information.
6. Keeping Personal Information Accurate.
7. Safeguarding Personal Information.
8. Openness.
9. Persons will have access to their personal information.
10. Challenging Compliance.

Appendix D - PP-SDLC Privacy Phase Requirements

	Initiation	**Acquisition / Development**	**Implementation**	**Operations / Maintenance**	**Disposition**
Privacy Considerations	- Initial PIA. - Data Sensitivity Assessment. - Privacy Design Principles Requirements Analysis. - Privacy Management Tools evaluation and feasibility study. - Preliminary Risk Assessment and Privacy Plan. - Data Privacy Categorization. - Privacy and Security Trade-Off Resolution. - Privacy Training for involved individuals (4 C's).	- PDM-ADM Design Rule. - Risk Assessment. - PIA. - Privacy Functional Requirements Analysis. - Privacy Assurance Requirements Analysis. - Privacy Plan. - Study of privacy controls and management tools. - Privacy test and evaluation plan. - Integrate Privacy Design Principles. - Feedback and Control.	- Inspection and Acceptance. - User consent. - Inform users. - Privacy controls and system are integrated and configured. - Security safeguards are activated. - First stages of gaining privacy certification, accreditation, regulation, etc. - Staff privacy training and creation of in-house privacy department or positions if required. - Test and evaluation.	- Completion and ongoing privacy certification, accreditation, regulation, etc. - Monitoring for new privacy requirements. - Privacy configuration management and control. - New privacy techniques evaluated ad integrated. - Personal Data Retention. Periodic testing, auditing, and evaluation.	- Information preservation. - Media sanitization. - Disposal of hardware and software. - User feedback.

Table 3: The PP-SDLC Privacy Phase Requirements