Privacy: In pursuit of information security awareness

Duane Boucher
Department of Information Systems
University of Fort Hare
East London, South Africa
dboucher@ufh.ac.za

Stephen Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

***Abstract*—The debate regarding the nature of an individual's privacy rights have increasingly centred on the threats posed by technological advances and the disclosure of personally identifiable information (PII). However, the disclosure of PII is often affected by the degree of privacy appetite of individuals. This is often dependent on their understanding of the efficacy of privacy enabling technologies (PETs) towards the protection of privacy. Therefore, the establishment of policy, regulations, and laws seek to mitigate the instances of unsolicited disclosure of PII, which may arise through ignorance or malice. This is done not only to protect the privacy rights of individuals, but also to ensure that the necessary flow of information required for the provision of goods and services is not impeded. However, the protection of privacy will only occur when the appropriate balance is found between keeping information private and making it public. This balance is dependent on the producers and consumers of information understanding the concept of informational privacy through increased awareness. Therefore, this paper considers the nature of privacy through a brief literature analysis of multi-disciplinary privacy theory and arrives at an appropriate understanding of informational privacy. Pertinent to an understanding of informational privacy is a discussion of the type of information that needs to be protected, namely PII. Thereafter, the fair information practices (FIPs), OECD privacy principles [24] and OECD guidelines for establishing a security culture [27] are discussed. This discussion results in an informational privacy model, which can be utilised to ultimately educate the producers and consumers of information about privacy. Thereby improving security awareness and residually fostering a security culture.**

Keywords—Privacy; Awareness; Personally Identifiable Information.

I. Introduction

Progressive advances in technology and the advents of social media, online gaming, digital tracking and electronic monitoring systems are making it increasingly difficult to keep information about ourselves and our actions private [1]. This is because personally identifiable information (PII) is often solicited towards a given end. The proliferation of ubiquitous computing often raises opposing views about the right to privacy and the benefits that can be realised from information sharing. For individuals there is the expectation that any information collected will be utilized for their own betterment [2] and be kept secure. However, there are those who would illegally access and utilise PII. Although, technology exists to protect PII in the form of Privacy Enhancing Technologies (PETs) such as biometric scanners, they are susceptible to either low-tech (brute force) or high-tech attacks. Technology aside, humans remain the consistent weakness in any given security system. Therefore, it is essential that those (consumers or employees) interacting with systems are aware of the security concerns that would arise if said systems were breached. This can be achieved by educating individuals through training about the information they have under their control in order to mitigate instances of unintentional information disclosure.

Being able to control how and when information about one is shared is only possible by increasing awareness about what it means to keep information private. Therefore, this paper considers the nature of privacy through a brief analysis of multi-disciplinary privacy theory and arrives at an understanding of informational privacy. Pertinent to informational privacy is a discussion of the type of information that needs to be protected, namely PII. Thereafter, the PII Life Cycle, Fair Information Practices (FIPs), and the OECD Privacy Principles [24] are discussed. The OECD guidelines for establishing a security culture [27] is briefly addressed. Finally an informational privacy model is derived for raising awareness, assisting in training, and educating individuals about privacy.

II. NATURE OF PRIVACY

The debate regarding the nature of an individual's privacy rights have increasingly centred on the threats being posed by technological advances [1][3][4]. For Samuel Warren and Louis Brandeis that technological advancement, circa 1890, was the proliferation of the print media and the advent of the portable camera [3]. This was a turnkey moment for privacy, as they argued that the unsolicited capture of an individual's image was to all intents and purposes an invasion of privacy [4], and those individuals and their families have the right to keep their private lives 'secret' [3].

The words 'private' and 'secret' are considered interchangeably, but their focus is fundamentally different. Privacy can simply be described as being able to withhold information about our *Self* from others [5]. Whereas, secrecy refers to a group of people keeping information from others, and if that information is disclosed then it could lead to negative consequences for the parties concerned. Secrecy and confidentiality are often similarly defined [5], because both are an extension of privacy, i.e. privacy must exist before they can be manifested. However, it should be noted that there are instances where confidentiality and secrecy are defined differently, e.g. in military circles, where *confidentiality*, *secret*, and *top secret* each represent an increasing severity in associated damage from information disclosure. Subsequently, to be aware of how one arrives at a point of information disclosure, it is necessary to firstly define 'privacy'.

A. Towards a definition

A finite definition of privacy does not easily present itself [1] [2][4][6]. This arises in part because privacy is multi-disciplinary, and has been discussed in multiple contexts [7]. Whitley supports this view by stating that "the term privacy, therefore, has no inherent definition rather different social groups and disciplines have developed different meanings and interpretations of the concept" [8].

Westin defined privacy as, "the claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [9]. Altman supported this view of privacy by stating that "privacy is a central regulatory process by which a person (or group) makes himself more or less accessible and open to others" [10].

Margulis stated that "privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimise vulnerability" [11]. Margulis continues to state that the control of transactions and the access to information regarding the individual usually revolves around how much individuals are willing, or regulated to share of themselves [11].

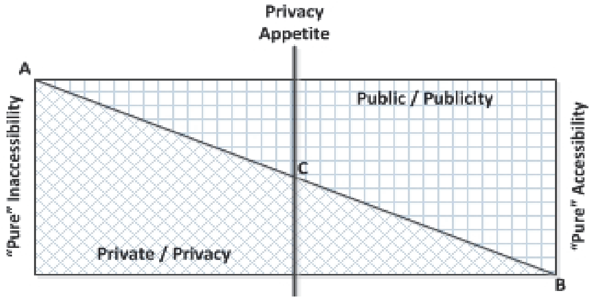

Figure 1. Privacy/Public Continuum (own compilation)

The degree of accessibility forgone by an individual determines the privacy appetite of said individual. Figure 1, depicts the constant flux between that information which should be private, and accessible to the public. Striving for a condition of "pure" inaccessibility (A) would mean that information was only known to the individual and no other. This is increasingly difficult in our modern technologically pervasive lives. For example, individuals are increasingly encouraged to utilise Facebook's "Like" feature in popular media. In doing so individuals share their details with that community of *Like*-minded individuals, and once your information is shared, can it be truly unshared successfully? Therefore, the only way to ensure remaining at point A, is to never make that private information explicit, because once it is written down, it has the potential to be discovered and shared.

Similarly, an individual may deem it inappropriate to allow for "pure" accessibility (B), which instead would allow all their personal information to be shared with the public. This would be equivalent to moving into a glass house, and having no doors on rooms. Effectively passing individuals could enter the house, explore, and leave it at the time of their pleasing with whatever information they have gleaned from what they saw you doing.

Each of the instances (A or B) of purity marks an extremity on the private/public continuum (A-B) [10]. The context and the active elements acting therein and thereon determine vacillation points, and in some instance a point of rest (C) on the continuum, i.e. the degree of sharing. This amplifies the complexity of defining privacy, because no singular rule applies to all contexts, so prescribing universally fixed points and outcomes on the privacy/public continuum is myopic. Consequently, the dichotomy of what constitutes private or public information about a person has resulted in a series of legal interpretations of privacy in order to arrive at some form of governing principles and understanding of the discipline. However, to gain a better awareness into the affect privacy has on the legal perspective, it is important to consider the legal "building blocks" of privacy.

B. "Building blocks" of privacy legislation

An understanding of what constitutes privacy within the legal perspective (and residually as a whole) requires that it is increasingly analysed either from the perspective of *coherence* or *distinctiveness* [12]. Coherence refers to whether there are common characteristics, or traits of privacy concerns. Whereas, distinctiveness refers to whether privacy interests should be defended as privacy issues, or whether they are better defended in terms of other recognised interests, i.e. if privacy is omitted from equation would something significant be lost [13]. Prosser [13] and Thomson [6] favour distinctiveness over coherence, because they argue that the right to privacy is nothing more than a specific grouping of the legal rights that seek to protect privacy.

Prosser proposed that the right to privacy can be simplified into four torts, or harms, of privacy violation [13]. These are the right to be free from...

- ***intrusion*** upon one's seclusion, solitude, or private affairs;
- ***disclosure*** of embarrassing private facts about oneself in public, which would be offensive and objectionable under the '*reasonable expectations of privacy test*[1]' ;
- ***defamation*** of character arising from having "private facts" misrepresented in public; and,
- identity ***appropriation*** or theft for personal gain by others.

Prosser pointed out "that these four types of invasion of privacy may at times be subject to different rules" and applicable interpretations [13]. Corliss provides an explanation of the interrelatedness of Prosser's four privacy harms [12]. Firstly, intrusion and disclosure refer to the invasion of something secret, secluded or private and

[1] Winn [14] provides an indepth discussion on the notion of a 'reasonable expectation of privacy', and the associated 'test' is depended on if 1) you actually expect privacy, and 2) your expectation is one that society as a whole would think is legitimate. Privacy was again reduced to a right, but one that was context specific. This distinction was important, because it implies the privacy of the person, and not the place.

pertaining to the individual; whereas defamation and appropriation do not. Secondly, disclosure and defamation are dependent on publicity; but this is not the case for intrusion, although it is implied for appropriation. Thirdly, defamation represents a falsity or fiction being fabricated; whereas intrusion, disclosure and appropriation do not. Finally, appropriation represents personal gain derivation by another; but this is not a consequence (although it might be a contributing factor) for intrusion, disclosure, and defamation.

Bloustein rejected Prosser's simplification of privacy to mere inhuman harms, and thereby distinctiveness [15]. Bloustein rather supports the notion of coherence, because he proposes that each of the four harms identified by Prosser have significant implications for human dignity, or result in dignitary harms. The discussion of privacy as violating dignitary harms is a major theme that has raged in the ongoing privacy debate [12] and often compounds privacy rulings [4].

Thomson supported the notion of distinctiveness in its purest form by rejecting the concept of a right to privacy insofar as she argues that "privacy" in and of itself brings nothing unique to the fore [6]. She substantiates this view by stating that invasions of privacy can be relegated to other more fundamental rights entrenched in law, such as property law, whether that is intellectual or physical property.

However, rather than becoming embroiled in a philosophical, political, or otherwise inherently all consuming discussion of privacy, it might instead be more beneficial to rather consider the actual functioning of privacy [2]. This would involve focusing on the business processes, or workflows, because they are important in understanding privacy and the utility *(value)* associated therewith [16]. To understand the actual functionality of privacy, Introna summarised his discussion of privacy into three broad categories, namely:

- privacy as the right to solitude;
- privacy as the right to control information disclosure about the self; and
- privacy as the right to not be the subject of prejudice, ridicule, defamation, or unsolicited scrutiny [2].

The three identified categories are a hybrid of the torts identified by Prosser [13] and the later extrapolation by Westin [9] into the functionality of privacy, namely: *informational privacy*. The concept of informational privacy is covered in more detail in the next section as it is a tangible component in the later derivation of an informational privacy awareness model.

III. INFORMATIONAL PRIVACY

Prior to embarking on an explanation of informational privacy, it is necessary to ensure a common understanding of the concept of *information*. On the outset, this would seem a simple task, but various disciplines have assigned different meanings to the concept of information. Losee, in his extensive analysis of a definition for information, stated that "a good definition or theory of information both describes factually what occurs or what exists, as well as provides an explanation of events" [17]. Therefore, "information is always informative about something, whether it is considered a component of the output or result of the process" [17].

The Information Systems discipline ascribes to this notion, that there is simultaneously an interaction of elements and forces in action on information. This concept is represented by utilising the standard notation of General Systems Theory, namely: *input → process → output*. This notation is shown on Figure 2, where input==data, process==information and output==knowledge.

The data, i.e. alphanumeric characteristics about a person, place, or thing are input into the system. For the captured or recorded data to become information, then it must be processed, which involves organising, transforming, and presenting it in a way that gives the data meaning [18]. The output is then considered meaningful and useful information, that when utilised creates knowledge. If the information cannot be used in some form of understandable communication, then it should simply be considered as useless information, and therefore not meaningfully processed data [18]. This implies that the data was processed incorrectly, or the means utilised were not suitable for the context.

Once the processing has occurred, the actors in the given context have access to the information in the form of a given output. The output may be represented in soft copy format, e.g. to the screen of an electronic device, or in hard copy format, e.g. printed documentation. The output may also be the automated input to another system. However, once information has been represented as some form of output, it is not always easy to reverse engineer to the original data [17]. This is in part because information is derived within a given context as depicted in Figure 2. Although, information is determined for a given context, it is also influenced by the privacy constraints associated with that context.

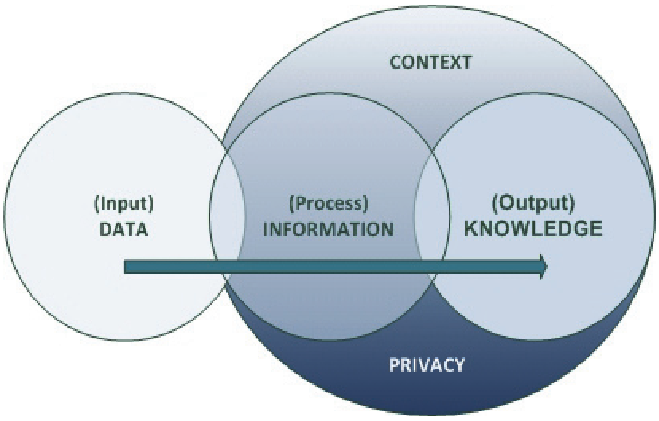

Figure 2. Explaining Information (adapted from [18])

Shedroff believes that information serves as an overlapping point between the producers of information and the consumers of information [18]. The *producers of information* are those individuals from whom data is collected by an organisation in order to process it towards some given end, e.g. a contract. A contract contains information about the organisation's customer, where the customer has the right to determine how, when, where, and why their information will be shared. Therefore, the producers of information (the customers) exert control equally over the data and information spheres, i.e. they can decide how much information about themselves they are willing to share.

The employees of an organisation are considered the *consumers of information*, because they need to be able to make decisions about their business based on the information they hold about their customers. They make these decisions based on the knowledge gained from applying useful information. This has been accumulated from their previous experiences, or from conducting data mining on the information derived from their customer's data. However, all employees in an organisation do not automatically have access to all information about a customer, and are restricted in how the information can be shared with others. Therefore, the consumers of information exert limited and authorised control over the information sphere, but complete control over the knowledge sphere.

The key element here is the control of the information by the producers of information who will ultimately decide how much privacy they are willing to forego. Westin argued that privacy is not purely the notion put forward by Warren and Brandeis for the "right to be let alone" [9], i.e. free of nuisance. He believed that privacy should primarily be seen as the control of information, which in social contexts is expressed by an individual's right to withhold themselves from interaction with others. Westin's concept of informational privacy is depicted in Figure 3, and is briefly described below.

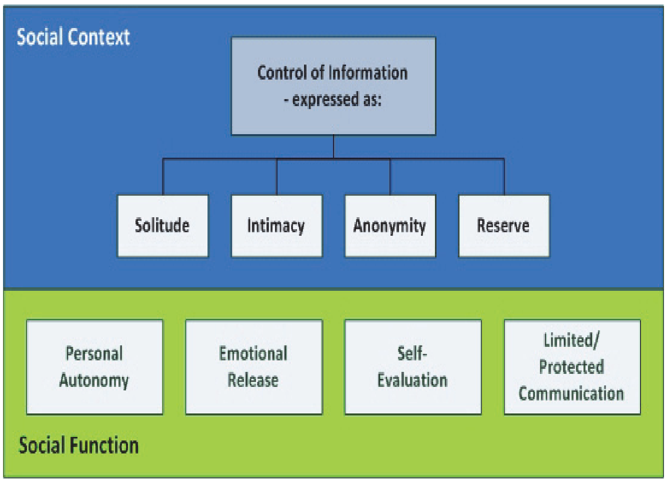

Figure 3. Westin's Informational Privacy (own compilation)

Westin's informational privacy is concerned with the amount of control an individual exerts on their information to keep it private, as opposed to their degree of social participation, i.e. how much they are willing to make public [9]. The amount of control that an individual exerts on their information is determined by the social context in which they find themselves. *Solitude* refers to that individual who does not want to share any information with another. They are in a state of absolute privacy, or pure inaccessibility (as depicted earlier in Figure 1). *Reserve* implies that individuals decide to keep certain information private from everyone else, i.e. information that is not shared for fear of repercussions. *Intimacy* is concerned with the control individuals exert on the information they are willing to disclose to others. Intimacy and reserve sound very similar, but reserve is concerned with the amount of control exerted on keeping information private, whereas intimacy is concerned with the control associated with sharing information, or making it public. *Anonymity* is concerned with controlling what information is associated with the individual, i.e. information, which is in the public domain cannot be traced back to the individual.

Westin explained that the justification for the control of information originates from four distinct social functions, which individuals must address in their lives [9]. These are represented in the bottom half of Figure 2. *Personal autonomy* is fundamental to the individual maintaining their individuality by being the owner of their own decisions. This means that the individual must decide what information to withhold or share without experiencing a threat to the Self. *Emotional release* is indicative of the individual being able to manage the sharing of that information which is construed as inappropriate by the greater society. *Self-evaluation* is where the individual evaluates the information they are receiving from the world, and how their ideas may be interpreted against accepted societal norms. Finally, *limited and protected communications* is concerned with whom individuals feel they can share their information, i.e. who do they trust.

Individuals have a relative amount of control over their information. However, their greatest threat to the control of information arises from how much of their information enters the public domain. The anonymity of an individual is always at risk, because the vast flows of digital information make it increasingly easier to identify the individual from who the information originated.

Losee raised a valid point in identifying the difficulty in reverse engineering information to the original data, but he did not discount it from actually occurring [17]. Technological tools, such as search algorithms have increased the ability to mine and access the data from which information was derived. It is therefore imperative that the nature of PII is understood if information disclosure is to be mitigated through privacy awareness.

IV. PERSONALLY IDENTIFIABLE INFORMATION

Information about individuals is becoming increasingly more accessible with advances in technology [1][19]. This accessibility occurs not only from the digitisation of paper-based records, but also from information generated from the storage of biological data about individuals [20][21]. Once this information is collected and stored in central databases, it could be utilised towards a number of ends [21]. The retention of information and the access thereto is of great importance, especially when considering who may have access to that information. Therefore, it is necessary to clearly define what is meant by PII, and how, if at all, we can control its disclosure.

A. Defining Personally Identifiable Information

Narayanan and Schmatikov argue that "for a concept that is as pervasive in both legal and technological discourse on data privacy, PII is surprisingly difficult to define" [22]. The Protection of Personal Information (Popi) Bill of 2009, currently under debate within the South African legislature, defines personal information quite extensively as "meaning information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b) information relating to the education or the medical, financial, criminal or employment history of the person;
c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
d) the blood type or any other biometric (biological) information of the person;
e) the personal opinions, views or preferences of the person;
f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g) the views or opinions of another individual about the person; and
h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person".

The Popi Bill[2] although all-encompassing of privacy rights does provide for exclusions. These are instances when the privacy of the individual may be in conflict with what is considered necessary for the collective (public) good or legal recourse. These exclusions aside, the individual has significant control over where, when, and how their personal information is shared. This includes those instances during its life cycle when the individual / data owner / subject are not proximate to said information [23]. However, it is imperative that there is an understanding of the life cycle of personally identifiable information in order to mitigate instances of information disclosure.

B. *Personally Identifiable Information Life Cycle*

The International Security, Trust & Privacy Alliance (ISTPA) provide a common vocabulary and toolkit for dealing with privacy policy development [23]. This initial framework provided a description of the elements involved in the sharing of PII. An overview of these various elements and their interactions, which provide the basic requirement for the management of PII, are depicted in Figure 4. The titles of "Personal Information Preferences", "Consistency", and "Use of Personal Information" are all associated with the expectant proper handling of PII. If PII is properly handled then it is the expectation, that privacy management can be realised.

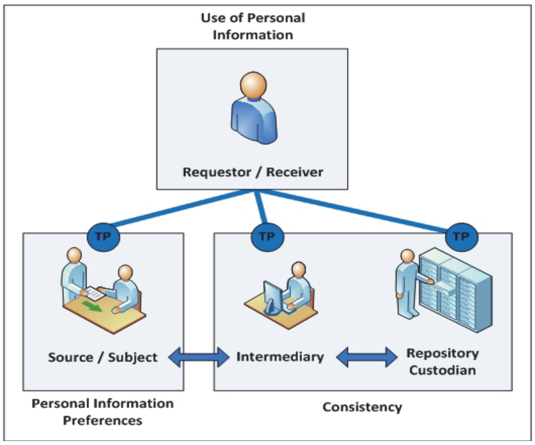

Figure 4. PII Life Cycle (adapted from [23])

Figure 4 is briefly described using an example of the flow of PII within the context of an application for a mobile phone contract. The client (*source / subject*) has a consultation with a sales agent *(receiver / requestor)* at the business premise. At the time of the consultation the client specifies how their PII can be shared, i.e. they indicate whether it can be used for marketing purposes or shared with third parties. The "TP" in the figure refers to a touch point or point of interaction, i.e. a point in the life cycle at which an individual, institution or other recognised entity can either request information, or be the recipient of information. The sharing of the client's PII can only occur within the constraints of the preferences stipulated by said client. The sales agent may pass the information onto an administrative clerk (*intermediary*) who then either captures the information electronically, or provides the record to a clerk for filing. Alternatively, the sales agent can electronically record the clients PII directly into a repository. Electronic- or paper-based filing represents the notion of the *repository custodian*. From the initial handover to the intermediary and then onto the repository custodian, there has to be consistency in data management, data security, and data usage.

As depicted in Figure 4, there can be requests for information regarding the client. This may be information that needs to be sent to support staff. In all instances, the client is deemed, although removed from the proximity of their personal information, to be in control of their privacy. The double arrows thus indicating, that the client may at any time request (legal requirements notwithstanding) that certain information is removed or added to their existing record.

The overriding assumption is then that the control by an individual over their PII is largely governed by the degree of privacy they are willing to waiver, i.e. the amount of consent afforded the person holding their records. However, the ease of duplication of digital records also raises concerns regarding

[2] The two Information Bills currently (circa 2011) under review in the South African Legislature are the ***Protection of Information (POI) Bill***, and the ***Protection of Personal Information (Popi) Bill.*** The similarity of the names is cause for confusion, because the POI Bill deals with the degree of control the State has over information shared (transparency) with the public, and the Popi Bill originated to address the European Union requirements for the protection of trans-border information flow for its citizens and its companies trading with South Africa. South Africa is a laggard in the adoption of some form of all-encompassing Privacy Act to manage all areas of informational flow within the borders of South Africa.

the control and accessibility thereof, and the importance of consent [1].

Associated with consent is the individual's right to either *opt-in* or *opt-out* of providing information. To opt-in means that the individual agrees to the sharing of their information in some specific manner through participation, i.e. they provide consent. To opt-out means that the individual has to specifically state that they no longer want to participate. For example, an individual may send a text message containing the word 'STOP', to avoid future contact for marketing-related purposes. They are in effect rescinding the use of their information, or reducing the degree of their privacy appetite. There is more support for the notion of opt-out by those wanting to increase the adoption of new technologies. This stance is supported because individuals don't typically understand their privacy rights when first making use of new technologies. Those often offering these technologies, such as social media sites will initially have default settings which favour greater accessibility over privacy concerns.

The next section considers the various privacy principles arising out of the Fair Information Practices (FIPs). A better understanding of these will assist in raising security awareness amongst consumers and employees about the various aspects associated with privacy.

V. PRIVACY PRINCIPLES

The origin of the FIPs was a set of privacy principles that sought to provide a code of action to address how an individual's private information should be protected [24]. These were initially contained in the HEW[3] Report [24], which outlined the following five principles, namely:

1. There must be no personal data record-keeping systems whose very existence is secret **[Notice/Awareness]**.
2. There must be a way for a person to find out what information about the person is recorded and how it is used **[Choice/Consent]**.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent **[Access/Participation]**.
4. There must be a way for a person to correct or amend a record of identifiable information about the person **[Integrity/Security]**.
5. Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of data **[Enforcement/Redress]**.

The information practices associated with each of the five principles above are represented by the words contained in the square bracketed items. The Organisation for Economic Cooperation and Development (OECD) provided a common privacy framework [24] that stipulated eight privacy principles that needed to be in place in order to safeguard the automated processing of data across countries borders, namely:

1. *Collection Limitation Principle* – stipulates that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. *Data Quality Principle* – stipulates that personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. *Purpose Specification Principle* - The purpose for which personal data are collected should be specified not later than at the time of data collection and subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. *Use Limitation Principle* – stipulates that personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: a) with the consent of the data subject; or, b) by the authority of law.
5. *Security Safeguards Principle* – stipulates that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. *Openness Principle* – stipulates that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. *Individual Participation Principle* – stipulates that an individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him .. i) within a reasonable time .. ii) at a charge, if any, that is not excessive .. iii) in a reasonable manner and .. iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.
8. *Accountability Principle* – stipulates that a data controller should be accountable for complying with measures which give effect to the principles stated above.

The OECD privacy principles formed part of the European Commission (EC) Data Protection Directive (Directive 95/46/EC), and are integrated into various privacy legislation throughout the European Union (EU). The differences in countries approaches to sharing data meant that in some

[3] The full name for the report is the U.S. Department of Health, Education and Welfare (HEW), Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens.

instances *Safe Harbour Principles* needed to be established to deal with those trading parties outside the EU. The Safe Harbour Principles provide a means for companies trading from countries that do not have established, or that possess significantly different concepts of privacy legislation, to be allowed to trade (or share sensitive information) with each other [24].

The ISTPA [25] conducted an in-depth analysis of 12 privacy instruments, "and by carefully reviewing their provisions, identified the privacy principles and practices that are common to all". These were grouped into a "composite requirement", which are represented in Table 1. Furthermore, they reviewed the terminology associated with each, and determined what they called a "restructured requirement", which are also represented in Table 1 [25].

Table 1. ISTPA Privacy Requirements Summary [25]

Composite Requirement	Restructured Requirement
Notice and Awareness	Openness Disclosure Notice
Choice and Consent	Collection Limitations Use Limitations Consent Accountability
Access (by the Subject)	Access (Not Correction)
Information Quality	Data Quality Security / Safeguards
Update and Correction	Correction (not Access)
Enforcement and Recourse	Enforcement

The requirements listed above are evidenced in many regulatory documents worldwide, which need to consider the privacy rights of individuals. However, many individuals still have little awareness of their privacy rights. Therefore, security cultures need to be cultivated to protect individuals and computer networks [26].

VI. CULTIVATING A SECURITY CULTURE

The OECD [27] provides nine general security principles that are considered to cumulatively foster a security culture on a given computer network. The keystone security principle is *awareness,* which is described as existing when all participants are aware of the need for security and their role in enhancing security [27]. It also forms the starting point of a learning continuum, which sees the recipient of the security information moving from *awareness*, to *understanding*, to *training*, and then *education* [28].

Awareness occurs in the presence of a passive recipient, where information is shared for informative purposes. The existing security policies, and/or a security topic of relevance are communicated to the staff in the organisation at this time. The second step requires understanding, which involves the recipient of the information becoming familiar with a given security topic. The third step, training, sees an individual becoming an active participant in the learning process. Finally, education refers to the ability of the recipient to internalise the information and actively interrogate it for greater insight. The learning continuum is not necessarily linear, but iterative, because new information may require retraining in a specific area. The McCumber INFOSEC Model highlights the importance of the training and education of staff as a crucial countermeasure against breeches in information security [28]. This assists greatly in developing a security culture within an organisation.

There are many benefits that can be derived from having a successful security culture [29]. One of these is the potential to mitigate instances of PII disclosure by raising informational privacy awareness amongst individuals [26].

VII. INFORMATIONAL PRIVACY MODEL

The discussion of privacy has led to the derivation of the informational privacy model shown in Figure 5. It is a combination of Figure 4, and the various privacy principles detailed in this paper. The goal of the model in this paper is to provide a graphical representation of privacy. Its initial purpose is to raise awareness of the various elements of privacy amongst recipients, thereafter, it can be utilised as a means of training and education. The application of the model for training and education purposes will be dependent on the business context, and the relevant regulatory requirements, which may exist in the given industry sector.

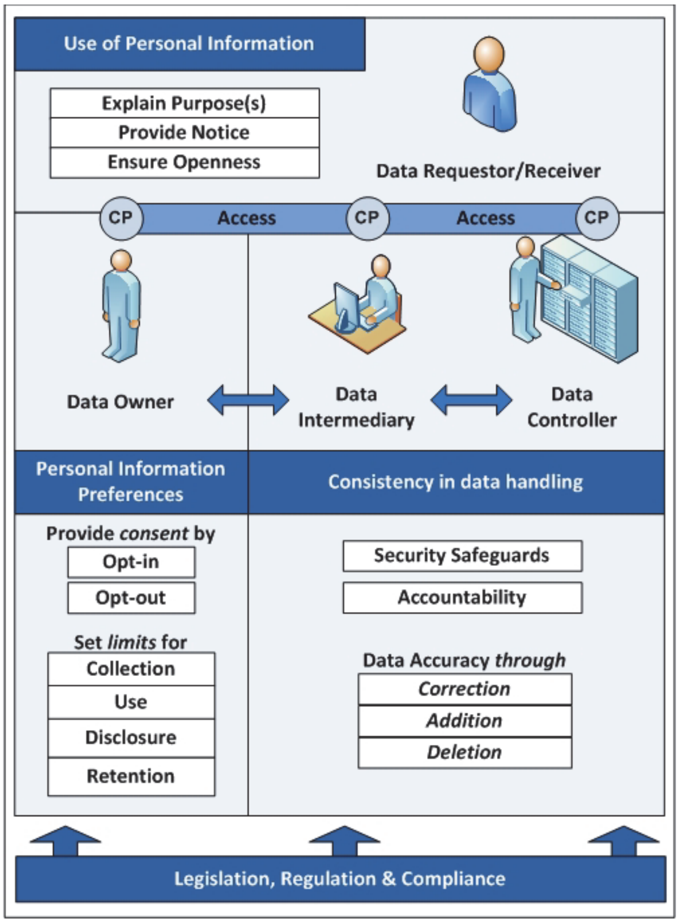

Figure 5. Informational Privacy Model (original creation)

The model consists of four primary parts, namely: the *personal information preferences* of the data owner; the *use of personal information* by the data requestor/receiver; the *consistency in data handling* carried out by the data intermediary and the data controller; and *legislation, regulation, & compliance* for a given industry sector. The various actors (data owner, data requestor/receiver, data intermediary, and data controller) access information through various contact points (CP). These actors interact and have control over information in varying responsibilities. However, the data owner has continuous access to their information in order to control how much of it is kept private or made public. This will to a large extent be governed by the legislative or regulatory requirements for compliance in a given sector, e.g. the banking sector. Not all aspects may be present in every sector, but this model provides those trying to educate individuals about information privacy concerns with a starting point for increased security awareness and more specifically, privacy awareness.

VIII. CONCLUSION

The instances of security breaches and the resultant losses of PII are increasingly reported in the popular press. These breaches arise largely from the increased digital interactions of the producers and consumers of information. The mitigation of unintentional information disclosure can be greatly aided by an increased awareness of individual privacy rights and how to control them.

The exploration of the nature of privacy resulted in the development of an informational privacy model. It provides a graphical representation of the myriad of privacy concepts to better aid in developing awareness for a security culture amongst the producers and consumers of information.

REFERENCES

[1] H. Nissenbaum. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, California: Stanford University Press, 2010.

[2] L.D. Introna. “Privacy and the Computer: Why we need privacy in the Information Society”. Metaphilosophy , vol 28, no. 3, 1997, pp.259-275.

[3] S.D. Warren & L.D. Brandeis. “The Right to Privacy”. The Harvard Law Review, vol 4, no. 5, 1890, pp.193-220.

[4] D.J. Solove. Understanding Privacy. Cambridge, Massachusetts: Harvard University Press, 2008.

[5] M.E. Whitman & H.J. Mattord. Principles of Information Security, 3rd ed. Boston: Course Technology, 2009.

[6] J.J. Thomson. “The Right to Privacy”. Philosophy and Public Affairs, vol 4, no.4, 1975, pp.295-314.

[7] F. Schoeman. “Privacy: philosophical dimensions of the literature”. In F. D. Schoeman (Ed.), Philosophical Dimensions of Privacy: an anthology. Cambridge, UK: Cambridge University Press, 2007, pp.1-33.

[8] E.A. Whitley. “Informational privacy, consent and the ‘control’ of personal data”. Information Security Technical Report, vol. 14, 2009, pp.154-155, 2009.

[9] A.F. Westin. Privacy and Freedom. New York: Atheneum Publishers, 1967.

[10] C. Nippert-Eng. Islands of Privacy. Chicago: University of Chicago Press, 2010.

[11] S.T. Margulis. “Privacy and Psychology”. From the proccedings of Contours of Privacy: Normative, Psychological and Social Perspectives. Ottawa, Canada, 2005, pp.1-26.

[12] M. Corliss. The Use of Information: How new technology is changing discussions of privacy. UMI Number: 1475484 . Ann Arbor, MI: UMI Dissertation Publishing, 23 April 2010.

[13] W.L. Prosser. “Privacy (a legal analysis)”, 1960. In F. D. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology. Cambridge, UK: Cambridge University Press, 2007, pp. 104-155.

[14] P. Winn. Katz and the Origin of the "Reasonable Expectation of Privacy" Test, 29 October 2008. Retrieved September 5, 2010, from Social Science Research Network: http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=1291870.

[15] E.J. Bloustein. “Privacy as an aspect of human dignity: an answer to Dean Prosser”, 1964. In F. D. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology. Cambridge, UK: Cambridge University Press, 2007, pp. 156-202.

[16] A. Barth. Design and Analysis of Privacy Policies. Dissertation, Stanford University, Department of Computer Science, 2008. Unpublished.

[17] R.M. Losee. “A Discipline Independent Definition of Information”. Journal of the American Society for Information Science , vol. 48, no. 3, 1997, pp. 254-269.

[18] N. Shedroff. Information interaction design: a unified field theory of design. In R. Jacobson (Ed.), *Information Design* (pp. 267-292). Cambridge, MA: MIT Press, 1999.

[19] C.J. Bennett & C.D. Raab. The Governance of Privacy - Policy Instruments in Global Perspective. Cambridge, MA: MIT Press, 2006.

[20] M. Crompton. “Biometrics and Privacy - The End of The World as We Know It or The White Knight of Privacy?”, 2003. Retrieved September 20, 2010, from Australian Government - Office of the Privacy Commissioner: http://www.privacy.gov.au/materials/types/download/8518/6407

[21] C Rosen. “Liberty, Privacy, and DNA Databases”, Spring 2003. Retrieved September 20, 2010, from The New Atlantis - A Journal of Technology and Society: http://www.thenewatlantis.com/docLib/TNA01-Rosen.pdf

[22] A. Narayanan & V. Schmatikov. “Myths and Fallacies of ‘Personally Identifiable Information’. Communications of the ACM, vol. 53, no. 8, June 2010, pp. 24-26.

[23] ISTPA. Privacy Framework V1.1, October, 2002. Retrieved September 20, 2010, from International Security, Trust & Privacy Alliance: http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf

[24] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980. Retrieved April 27, 2011, from Organisation for Economic Co-operation and Development: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines

[25] ISTPA. Analysis of Privacy Principles: Making Privacy Operational, May 2007. Retrieved September 20, 2010, from International Security, Trust & Privacy Alliance:

http://www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf

[26] R. Herold. Managing an Information Security and Awareness and Training Program. 2ed. New York: CRC Press, 2011.

[27] OECD. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002. Retrieved April 27, 2011, from Organisation for Economic Co-operation and Development: http://www.oecd.org/dataoecd/16/22/15582260.pdf

[28] V. Maconachy, C.D. Schou, D. Ragsdale, & D. Welch. “A Model for Information Assurance: An Integrated Approach”. Proceedings of the 2001 Workshop on Information Assurance and Security, United States Military Academy, West Point, N.Y. 5-6 June 2001, pp. 306-310.

[29] E.C. Johnson. “Security awareness: switch to a better programme”. Network Security, February 2006.