Open Access

The Ethics of Information: What is Valued Most

Sabah Al-Fedaghi*

Computer Engineering Department, Kuwait University, Kuwait

Abstract: In response to rising public awareness of information privacy, principles addressing the privacy of information have evolved and converged around a set of basic principles such as, for example, the Code of Fair Information Practice. Legislative developments such as the 1995 European Union's enactment of the Data Privacy Directive and the U.S. Health Insurance Portability and Accountability Act of 1996 have heightened awareness of ethical dilemmas related to this issue. Nevertheless, these and similar privacy-related efforts need to build firmer ground for the ethics of handling personal information. Why distinguish personal information from other types of information? Is it possible to narrowly define personal information in order to provide a workable object of study? Is there a coherent field of study of the ethics of handling personal information? Is personal information privacy different from other kinds of privacy? In this context, the goal of this paper is to focus the study of personal information on its relationship to privacy and ethics.

INTRODUCTION

Privacy is a widely discussed concept. According to Solove [1], various conceptualizations of privacy view privacy as the right to be let alone, limited access to the self, secrecy, control over personal information, personhood, and intimacy. We will review the first four conceptualizations because of their relevance to our discussion.

Originally, the definition of privacy as "the right to be let alone" arose mainly from concerns about expanding communication and new media technologies in the United States in 19th century [2]. The notion of privacy as being let alone has been criticized for failing to provide a balanced view that includes other important notions, such as free speech [1]. In addition, according to Allen [3], "If privacy simply meant 'being let alone,' any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom."

Limited access is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention" [4] that "entitles one to exclude others from (a) watching, (b) utilizing, (c) invading (intruding upon, or in other ways affecting) his private realm" [5]. Solove [1] criticizes some aspects of this conceptualization of privacy. For example, he objects to considering a person stranded on a deserted island as a person in complete privacy.

Secrecy refers to concealment of information to protect it from others who collect it against the wishes of the person to whom the information pertains [6]. According to Solove [1], "The conception of privacy as concealing information about the self forms the foundation for what is known as the constitutional right to information privacy…an offshoot of the Supreme Court's substantive due process 'right to privacy' cases, such as *Griswold v. Connecticut* and *Roe v. Wade*." The conception of privacy as secrecy (absolutely no disclosure) has been criticized for being too restrictive, since some information can be private even if it is shared with some people, as in criticisms of a boss shared with a coworker [7]. According to Solove [1], "[we] often expect privacy even when in public. Not all activities we deem as private occur behind the curtain. The book we read, the product we buy, the people we associate—these are often not viewed as secrets, but we nonetheless view them as private matters."

One conceptualization of privacy considers it the right to control personal affairs. This concept has roots in the principle of individual liberty. Liberty implies the ability to control our own lives in terms of work, religion, beliefs, and property, among other things. Historically, the "right" to control our property is a significant indicator of liberty. An owner can use, misuse, give away his or her property; similarly, privacy is a personal thing "owned" by individuals, and they "control" it. Informational privacy is "the right to exercise some measure of control over information about oneself" [8]. Control of one's own privacy involves freedom to relinquish that privacy, thus becoming "privacy-less," as one has freedom to give up his/her property, thus becoming property-less. In this case, privacy is analogous to "ownership," which usually is defined as "legal right of possession." "Legal right of possession" means "the right to exercise some measure of control over one's own property." In the case of ownership, the control is over property; however, in the case of privacy, the nature of what one controls is not clear. With regard to informational privacy, control of personal information refers to being free to do whatever one wants with his or her personal information, such that this right does not interfere with the comparable rights of others. This "definition" is criticized by many as not appropriate, since people manifest their freedom though voluntarily disclosing information about themselves, thus relinquishing their own privacy. In addition, according to Solove [1], "control-over-information" is "too

*Address correspondence to this author at the Computer Engineering Department, Kuwait University, Kuwait; E-mail: sabah@eng.kuniv.edu.kw

narrow a conception, for it excludes those aspects of privacy that are not informational, … the theory is too vague because [it] often fails to define the types of information over which individuals should have control."

Several types of privacy have been distinguished in the literature, including "physical privacy," privacy of personal behavior, privacy of personal communications, and privacy of personal data [9, 10]. In this paper we focus on information privacy. Information privacy refers to information proximity. According to Clarke [9], it is "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." It involves personal information such as credit data, medical and government records, etc. Personal information is said to denote information about identifiable individuals in accessible form [11]. It means "any information concerning a natural person which, because of name, number, symbol, mark, or other identifier, can be used to identify that natural person" [12]. Canadian privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA) defines personal information as "information about an identifiable individual" [13]. Many such "definitions" exist for personal or private information. They are usually closely linked with the notions of identification and de-identification. According to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) [14], "individually identifiable health information" refers to "health information that identifies the individual or can reasonably be used to identify the individual." Under the HIPAA Privacy Rule, one aspect of "de-identification" is that the health data not include eighteen identifiers of persons that could be used alone or in combination with other information to identify the subject. These identifiers include names, telephone numbers, fax numbers, email addresses, social security numbers, and URLs. The EU Data Protection Directive [15] extensively uses the terms "person-identification" and "identifiable/non-identifiable data." The P3P Specification Working Group specifies "identified data" as "information in a record or profile that can reasonably be tied to an individual" [16]. These descriptions of "personal information" are very general. We claim that our new formalism provides a systematic foundation for defining personal information and its related notions.

According to the Computer Professionals for Social Responsibility [17], "Our *personal information* has become a commodity, it is used to predict behavior both for national security and for marketing and other purposes." USACM Policy Recommendations state that

> Well-publicized instances of *personal data* exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. *Personal data* … needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties… We urge public and private policy makers to embrace the following recommendations when developing systems that make use of *personal information* [18].

From this and many other similar declarations, we realize that *personal information* is a significant notion that deserves more in-depth examination. In this context, the goal of this paper is to focus the study of personal information on its relationship to privacy and ethics.

According to Froehlich (2004), issues in information ethics were raised as early as 1980, and the field of information ethics "has evolved over the years into a multi-threaded phenomenon, in part, stimulated by the convergence of many disciplines on issues associated with the Internet." Mathiesen (2004) suggests that "information ethics can provide an important conceptual framework with which to understand a multitude of ethical issues that are arising due to new information technologies."

In response to rising public awareness of information privacy, principles addressing the privacy of information have evolved and converged around a set of basic principles such as, for example, the Code of Fair Information Practice. Legislative developments such as the 1995 European Union's enactment of the Data Privacy Directive [15] and the U.S. Health Insurance Portability and Accountability Act of 1996 [14], have heightened awareness of ethical dilemmas related to this issue.

Nevertheless, these and similar privacy-related efforts need to build firmer ground for the ethics of handling personal information. Why distinguish personal information from other types of information? Is it possible to narrowly define personal information in order to provide a workable object of study? Is there a coherent field of study of the ethics of handling personal information? Is personal information privacy different from other kinds of privacy?

EXTENDING MORAL STATUS FROM HUMANS TO INFORMATION ABOUT HUMANS

Both in traditional and current views on morality, the human being occupies the center moral stage as both moral agent and patient. It has always been recognized that human beings are "privileged" entities. They occupy a special place between angels and all nonhuman animals [19]. Most ethical theories enshrine valuing of the person as a core moral principle.

The most comprehensive arguments for such a thesis are applicable to the information sphere ontology that encompasses all informational entities. Accordingly, in the information sphere, a sister thesis to the claim of "recognize that human beings are privileged entities" appropriates first-class moral status to personal information compared with nonpersonal information. In the traditional sense, ontology provides a base for ethics regardless of whether such a base is nature, utility, reason, and so forth. Ontology presents a comprehensive conception of the world to provide a stage for ethical enquiry.

Consider an ontological world model based on triadic categories. Categories are a basic system of classification. In this triadic conceptualization, an ontological world model includes three categories: subjective (e.g., feelings, experiences), objective (physical universe), and intersubjective (e.g., collective ideas). Such a model appears in many works such as Popper and Eccles' (1997) "three world model" and Peirce's categorization of *Firstness*, *Secondness*, and *Thirdness*. Human beings are the only type of entity that is "complete" in terms of "entity-ness" in every category, as shown in Fig. (**1**). The entity of human beings contains all aspects

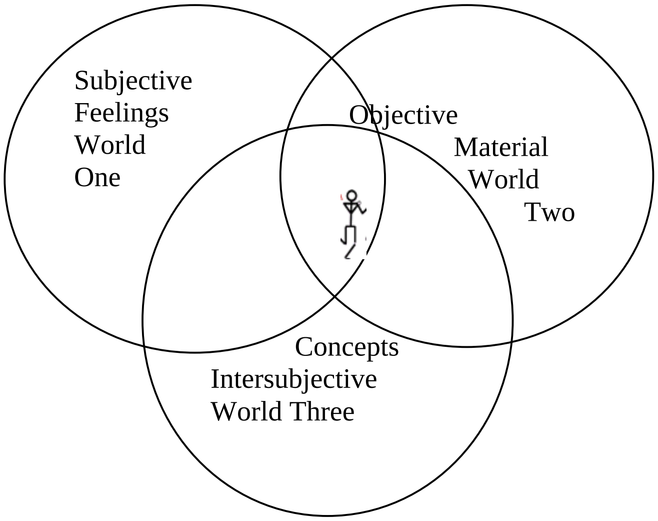

Fig. (1). The human being is the only type of entity that is "complete" in terms of "entity-ness" in every category.

of diverse categories functioning in agreement with each other. If we accept the belief that each category is ontologically irreducible to the others, we see that human beings are unique in terms of obeying multi-category principles, some of which are never applied to any other type of entity. Having a unique ontological category denied to all other entities is ontologically a very important aspect: it not only confers special status on this entity but also grants genuine diversity that is not present in other types of entities.

Many moral theories presuppose different types of moral *agents* (humans, robots) and moral *patients* (humans, animals). A moral agent is one who performs an ethically grounded act (right or wrong). Most theories also consider only rational beings (practically, people) capable of being moral agents. A moral patient is the recipient of a moral act. The human being as a moral patient is judged the most privileged object of moral concern. According to some of these moral theories, human beings are ends, while other beings are means [20]. Even when non-human beings are counted among moral patients, they are conferred second-class moral status.

According to Duncan [21], "We need to be (1) guided by an ethics of information, and (2) cognizant of special problems raised by computer and communications technology.… lack of relevant ethical guidance suggests the need for a new framework for consideration of privacy and information issues." "Information Ethics" (IE) can provide an important conceptual framework within which to understand a multitude of ethical issues that are emerging as a result of new information technologies [22]. According to Floridi [10], information ethics refers to the philosophical foundation that provides the basis for the moral principles that will then guide the problem-solving procedures in computer ethics. In information ethics, all objects are "information objects" and *all information objects have inherent moral value*. In view of Floridi's thesis, we can claim that information about humans is also a privileged entity in the world of information. Information ethics claims that personal information is "a constitutive part of a me-hood" [10]. Besides this claim, personal information is the only type of informational entity that is "complete" in terms of "informational entity-ness" in every category. Thus, personal information is unique in terms of obeying informational multi-category principles, some of which are never applied to any other type of information.

THE INFOSPHERE

As a philosophical foundation, the information sphere is said to denote the entire informational environment constituted by all informational entities and their properties, interactions, processes, and mutual relations [10]. It is a conceptualization of "our ontology in informational terms" used to base information ethics on the concept of information, as its basic phenomenon is recognized to have an intrinsic moral value [10, 23].

The informational ontology can be conceptualized as epistemic constructs in a manner similar to reality ontology mentioned previously. For example, *the state of affairs* in reality: that a brick hit John occurs at the ontological level, while the information *A brick hit John* as a linguistic construct represents that state of affairs in the information sphere. Informational ontology refers to categories of words of language as they emerge in language sentences and correspond to entities in reality. For example: *John loves his horse* is a linguistic sentence (hence, in informational ontology) that informs about the state of affairs that John loves his horse in the real world (ordinary ontology).

The information sphere provides counterpart triadic categories to the ontological world model based on triadic categories The infosphere provides counterpart triadic categories of Fig. (**1**) as shown in Fig. (**2**). Such a characteristic is a very important aspect: a unique informational category that no other information can have. As in ontology, this is the source of valuing of personal information that confers special status on this type of information.

The special status of personal information in the information sphere is based on the claim that personal information is a constitutive part of the human being, a privi-

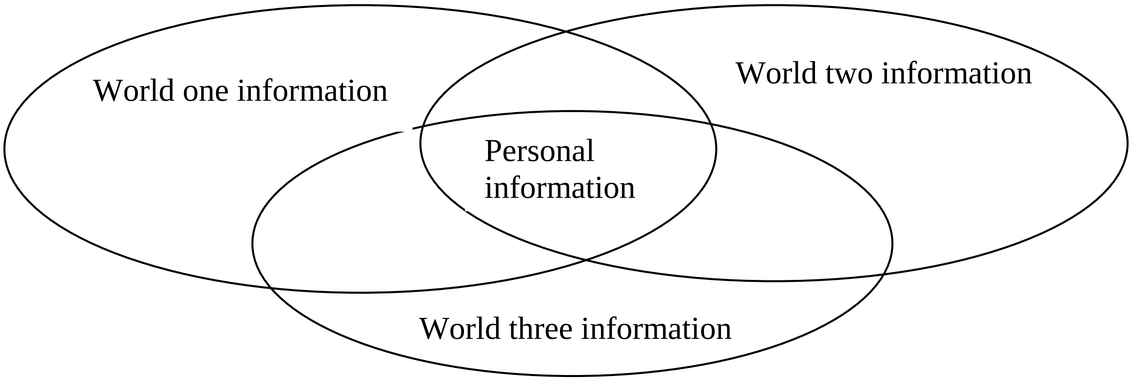

Fig. (2). Triadic categories of the Infosphere.

leged entity. Additionally, personal information is ontologically unique (meta) information in the information sphere since it is about the unique human's objective material existence, subjective feelings, and conceptual constructions.

WHAT IS PERSONAL INFORMATION?

We need a workable definition of personal information. Here, without loss of generality, we limit our definition to linguistic information.

Entities in the world are classified as persons and non-persons. In the information sphere, information is also classified as personal information and non-personal information.

Different types of information of interest in this paper are shown in Fig. (**3**).

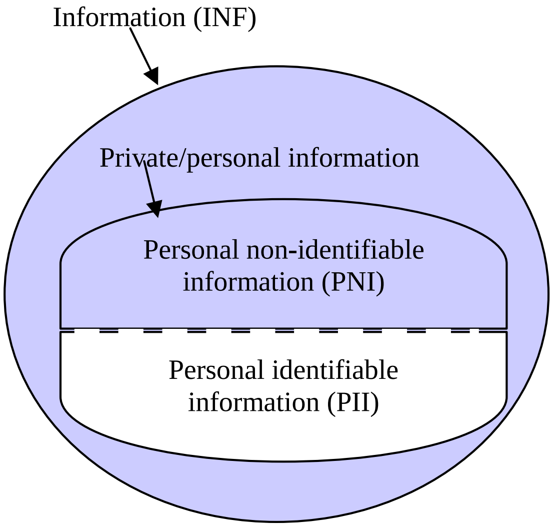
Information (INF)
Private/personal information
Personal non-identifiable information (PNI)
Personal identifiable information (PII)

Fig. (3). Types of information.

Personal information is a subcategory of information related to persons. It is of two types:

1. Personal non-identifiable information, as in the case of ownership of information (e.g., my file).
2. Personal identifiable information (PII): information about a specific person in which the unique identification of that person in embedded.

This paper is concerned solely with personal identifiable information. It is information *about* singly identifiable persons, called its *proprietors*. To recognize PII, we ask, "What is this piece of information about?" If its *aboutn*ess includes singly identifiable persons, then it is personal information.

As a linguistic expression, PII can be categorized as follows:

1. Atomic PII, where the expression *refers* to a single proprietor.
2. Compound PII, where the expression *refers* to more than one proprietor.

The relationship between individuals and their own atomic personal information is called *proprietorship*. John is the proprietor of *John is tall*, assuming that *John* is a singly identifiable person. John and Mary are the proprietors of *John loves Mary*.

We claim that proprietorship of PII is different from the concepts of possession, ownership, and copyrighting. The notion of proprietorship here is different from the legal concept of ownership. The "legal owning" of a thing is equated with exclusive possession of this thing with the right to transfer this ownership of the thing to others. Proprietorship of PII is non-transferable in the absolute sense. Others may possess or (legally) own it but they are never its proprietors (i.e., it cannot become their proprietary data). In addition, proprietorship of PII is different from the concept of copyrighting. Atomic PII of a proprietor is proprietary information of that proprietor, while others (e.g., other individuals, companies) can only possess it. Compound PII is proprietary information of its referents: all donors of pieces of atomic PII that are embedded in the compound PII.

Any compound PII is privacy-reducible to a set of atomic PII. For example, *John and Mary are in love* can be privacy-reduced to *John and someone are in love* and *Someone and Mary are in love*. Reducing compound PII to atomic PII refers to isolating the privacy aspects of the compound information to be about a singly identifiable person. It is obvious that privacy-reducibility of compound PII causes a loss of "semantic equivalence," since the identities of the referents in the original information are separated.

Note that these secondary issues, for example, the difference between *proprietorship* and other related notions and the "semantic equivalence" of atomic and compound PII, are peripheral issues that do not have to be settled while fixing our overall conceptual framework of PII privacy and ethics.

Defining PII as "information identifiable to the individual" does not mean that the information is "especially sensitive, private, or embarrassing. Rather, it describes a relationship between the information and a person, namely that the information—whether sensitive or trivial—is somehow identifiable to an individual" [24]. Clearly, much of PII, as defined, is insignificant in terms of privacy. Even though there is no criterion that precisely divides these types of PII, it seems that, in most cases, the difference between them is apparent. Many works in the area of privacy have no difficulty identifying (significant) privacy in domains such as health information or financial information. The "significance" here refers to the threshold of an intrinsic value of the PII.

Notice the broadness of our definition of PII. It involves any amount of information that embeds PII. For example, *John Smith* is PII if *John Smith* refers to a uniquely identifiable person. *John Smith is a physician* is PII since it embeds his identification. A prescription written by John Smith and directed to a pharmacist to dispense a certain medication to an identified patient embeds personal health information about that patient, and it also embeds PII regarding John Smith. In this case, John Smith's "pure" PII is mixed with a larger lot of information. PII may be embedded in a large amount of non-PII. Interestingly, the entire lot still *refers* to a singly identifiable person. The issue of isolating PII such that it includes only information *about* the proprietor is not discussed here; however, extending consideration to any amount of information that embeds PII seems justifiable. Imagine a defamation case involving a pharmaceutical prescription; the consequences involve John Smith, even though his name appears as a minor part of the content of the prescription. It discloses that the physician is treating an identifiable person (patient), and it describes certain types of medicine (e.g., may be as sensitive as morphine). It certainly can be used to harm him, for example, by ridiculing him because of his style of misspelling.

We notice here that it is important to exactly identify the objects of study (personal information), then to apply the definition according to requirement (e.g., rules of PII handling). Permitted and prohibited acts on PII can be specified only after establishing clear criteria defining personal information. As in law, "theft" is first defined, then thefts are (legally) differentiated from one another according to the value of the goods stolen. Specifications such as *John Smith's blood type is A* is PII and *Chef John Smith specializes in cooking fish* is not PII, are arbitrary specifications. Rather, if desired, we declare certain types of uniquely identifiable information such as *Chef John Smith specializes in cooking fish* to be available for, say, legitimate commercial consumer reporting. The actions of John Smith as a uniquely identifiable person provoke generating PII about him.

Does this mean that one's actions always produce PII? Notice that PII is realized in some form (e.g., linguistic). Thus, observing that Chef John specializes in cooking fish becomes PII when it is generated as spoken or printed materials. PII is "data," that is, a representation suitable for communication, interpretation, or processing, that refers (reference = meaning) to a uniquely identifiable human being. *Mary observed that Chef John specializes in cooking fish* is compound PII if it is generated in some form. A book embeds PII about its author because it embeds the PII *Author X wrote this book*. It does not embed PII when it is anonymized. Data is specifically *about* someone if it embeds his/her unique identity.

PERSONAL IDENTIFIABLE INFORMATION ETHICS

Privacy has always been promoted as a human trait. It is a broad concept that crosses first, second, and third worlds, exemplified by privacy in thought, body, and social relationships, respectively. In the infosphere, information exists about the proprietor: his/her thoughts, his/her body, and his/her relationships with other persons. Privacy and information are entangled in PII. Personal identifiable information is more "valuable" than non-PII because of its privacy aspect. It has an intrinsic value because it is "a human matter," just as privacy is a human trait. Does this mean that scientific information on how to make a nuclear bomb has less intrinsic moral value than the PII, *John is left handed*? No, it means *John is left handed* has a higher moral value than the scientific fact that *There exists someone who is left handed*. It is important to compare equal amounts of information when we decide the status of each type of information.

Personal identifiable information privacy is a property of PII that makes it significant. Personal identifiable information ethics (PIE) is the ethics of creating, collecting, processing, and disclosing personal information [25]. PIE recognizes PII itself to have an intrinsic moral value. It is concerned with the "moral consideration" of PII because PII's "well-being" is a manifestation of the proprietor's welfare. This means that valuing PII is based on valuing a human being. Moral consideration of its being a piece of PII means that, before acting on such information, it ought to have at least the consideration of "being private," in addition to other considerations (e.g., its significance/insignificance). PIE is based on the notion that *PII privacy* is applicable only to humans and that moral action concerns information about an identified human being. For example, animals have no concern about personal information privacy, e.g., about handling of their individually identifiable information. Enterprises (e.g., companies, agencies) have concerns about their reputation and confidentiality; if we want to call this enterprise information privacy, this would be different from PIE.

PII is considered to have a higher intrinsic moral value than non- PII. From the privacy side, the moral worth of PII is based on the assumption that the proper "beneficiary" of moral action is the proprietor of the PII. Thus, the intrinsic moral status of PII comes from the intrinsic moral status of its proprietor. To be more accurate, the "moral considerability" of PII by agents stems from proprietors' right to privacy.

The person's role as patient comes about indirectly through having proprietary PII (PII about the person him/herself) affected by an agent's activities on his/her PII. Consider the act of possessing PII that is not one's own, against the proprietor's will, whose consent is not unreasonably withheld. What is wrong with such an act is not the possession of information, hardly valued in itself as an anonymized piece of information, but the possession of information with a particular quality—namely, that of being not the proprietary information of the possessor. Thus, the proprietor of the possessed information is the patient at whom the act is aimed and whom it affects. The sensitivity of the PII is incidental, whether it is information of minor significance or vital health information, and it does not affect the fundamental character of the act as morally wrong. Thus, possession of PII—against the proprietor's will—amounts, morally, to theft, where what is wrong is not acting on the stolen thing, but taking the thing that is not one's own.

If someone asks me (say, I am your neighbor) what color car you drive and I tell them the answer without getting your explicit permission, I may have technically transgressed your PII privacy. Notice that such a judgment is made in the context of PII privacy. On the other hand, the act of hiring a private detective to unearth private details of your life that I then sell to a tabloid transgresses not only your PII privacy but also other types of privacy, such as your physical privacy and communication privacy. In the former case (asking about car color), the only patient is your PII, while the latter case involves you (directly) as a patient in addition to your PII.

According to PIE, a human being, as a PII entity, has intrinsic value that ought to regulate a moral action affecting it. Information about the human-information entity (proprietary PII) has intrinsic value because it is a constitutive part of that entity. A fundamental premise in PIE, adopted from IE, is that *proprietary PII about an individual is a constitutive part of the individual*. The implication here is that PII has value because a person values it as he/she values aspects or parts of his/herself.

PII ethical principles regulate the behavior of any agent. Individuals have proprietary rights to their PII. Agents have the duty to treat PII, when it is put in the role of patient, as an informational manifestation of its proprietor. Generally, any action on a piece of PII is evaluated in terms of its contribution to the welfare of the PII environment, which implies the welfare of proprietors. This welfare seems to have some universality feature with the development of agreed-on PII protection principles and privacy protection rules.

How can PIE be interpreted to mean that protecting PII privacy of non-criminals has the side effect of protecting criminals? "Protecting the personal information privacy of non-criminals does have the side effect of protecting criminals" is a contradictory statement, because the premise assumes PII privacy of non-criminals, while the conclusion is a judgment about the PII of criminals. What is meant is that whenever it is not possible to distinguish criminals from non-criminals, then PII privacy protects criminals.

PII privacy assumes that the significance of PII is based on the non-retribution (non-fear of punishment) desire of the *proprietor* to control PII [26]. That is, the proprietor values his/her PII *per se*, not as an instrument against others, similar to the way a human being values his/her body parts (e.g., hand) *per se*, not as tools against others. A paralyzed person's hand is intrinsically valuable to him because it is a constitutive part of him. No one has the right to act on it without his/her permission. Certainly, a murderer cannot claim respect for his/her body when others try to incarcerate him/her. Proprietorship of PII is based on the same principle. Criminal (personal) information (e.g., *John is an arsonist*) does not have the significance awarded to PII. Criminals cannot claim this value for their PII because the significance of this information is based on secrecy (not privacy), an instrumental value to protect them from punishment. They use PII secrecy as a tool against others.

Notice the contrast between our "identification" of privacy-related information and the typical definition of (informational) privacy as "control over personal information." As in the case of PII, the notion of "control" is too wide to limit the personal identifiable information to only privacy-related states of affairs. However, the notion of (informational) privacy as "control" permits such typical claims as *privacy protects criminal*s, which mixes privacy with secrecy. In contrast, the notion of (informational) privacy as privacy-significant PII does not lend itself to anti-privacy arguments that an individual's control of personal information can be used to cover criminal activities.

Privacy-significance means sensitive PII [27]. Clearly, much of this PII is insignificant in terms of privacy. We further categorize PII into two types:

1 Significant PII such as *John is caught urinating on tape*. This information is clearly of privacy significance from John's point of view.

2 Insignificant PII such as *Madonna won her right to use the domain name madonna.com*. It is newsworthy information, and Madonna would not consider release of (e.g., publishing) such information an intrusion on her claim for informational privacy.

We can theorize about how to decide about the privacy-based sensitivity of PII in different ways. Consider the PII *A brick hit John*. To measure its privacy relatedness, we look at its corresponding informational level. Ridiculing John by spreading "A brick hit John" on the network may have privacy significance. The proprietor John in *A brick hit John* does not originally consider it of privacy significance. When he is hit by the brick, privacy is not an issue. It becomes privacy-significant for him afterward, when someone uses it to ridicule him.

WHAT TYPES OF ACTS OPERATE ON PII?

Identifying the type of objects of study provides the opportunity to specify possible types of operations on these objects. PII is a type of information. Information is a flowthing. A flowthing refers to types of a thing that flows, hence, is received, processed, created, released, and communicated. Fig. (**4**) shows the state transition diagram of information flow and includes five states: received, processed, created, disclosed, and communicated.

This flow is applied to PII; thus, the generic operations (also called stages of PII system) that can be performed on PII are receiving, processing, creation, disclosing, and communication. Each operation denotes an act on PII, and the arrows in the figure show possible flow of PII among stages of acting on PII.

Fig. (**4**) shows a circulation system of PII analogous to the model of circulation of water among its various compartments in the environment. New PII is *created* by proprietors or non-proprietors (e.g., medical diagnostics by physicians).

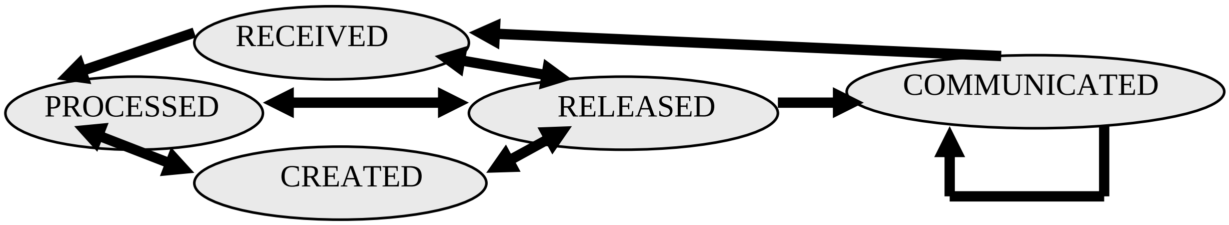

Fig. (4). Transition states of information.

As soon as it enters the system though collection by someone, it can enter many possible paths of flow. The PII can be used immediately, and it can be stored for a long or short period. It can be processed to change its form in order to extract embedded information, or mined to create new information. It can be transferred to another agent, or even returned to its proprietor. Meanwhile, it can be duplicated, thus producing copies that circulate independently in the system among different stages. It or any of its copies can be destroyed, anonymized, or encrypted. A piece of PII may have the history: released by proprietor, collected by agent 1, stored, processed (duplicated), released to agent 2, collected by agent 2, processed, mined, utilized (in conjunction with other persons' personal information) to create new PII, stored, etc.

Each of the five stages may include sub-stages such as storage and "use." "Use" refers to going outside the circulation system to any utilization of PII. For example, PII such as address can be used to deliver customer purchase (action). "Customer purchase" is a type of use of PII. In contrast, receiving, processing, creating, disclosing, and communicating are not *uses* of PII; rather, they are *states* of PII.

The collecting stage is the information acquisition stage that accepts information from external suppliers and injects it into the circulation system. It includes the possibility of using the collected (raw) personal information; thus, *use* in the figure is information exit from the system (e.g., customer address used in "product delivery"). It also includes the possibility of storing the collected information. At the collecting stage, we have to consider that the information may be collected from two sources: (1) a proprietor, or (2) a third party (non-proprietor). Notice the arrow between the collecting and communication stages in Fig. (**4**).

The processing stage involves acting on (e.g., anonymizing, data mining, summarizing, recording, organizing, adapting or altering, retrieving, consulting, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying, translating) PII. The processing is performed on acquired information from the collecting stage or the creating stage (see Fig. **4**). In actual processing, information is modified in form or content. Data mining is a type of processing that may generate new information. An example of generation of new information is the categorization of other persons' PII to generate the new PII that *John is a risk*. Other types of processing that do not generate new information, but only change the appearance of PII, include comparing, compressing, translating, and deleting. The "destruction" of PII is a type of process performed "when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form" (OECD, 1980). Disposing of information can occur in any stage of the flow model.

The disclosing stage involves releasing PII to insiders or outsiders. PII disclosure is performed on acquired information from a proprietor or from collected, created, or processed information. The disclosure depends on the communicating stage that transfers the information from the disclosing agent to the collecting one, which can be the same agent, another agent, or the proprietor him/herself.

APPLICATION: SECURITY AND ASSESSMENT SYSTEMS

In general, the term "security" refers to the well-being of information and infrastructures where the possibility of threat to information and services is minimized. Similarly, PII security is a state of well-being of PII in which the possibility of mishandling is minimized. Establishing a PII security strategy aims to achieve compliance with regulations, provide a foundation for communications and shared understanding (e.g., technical vs. non-technical), and expose vulnerabilities in the operational environment. Security strategy usually starts with policy development according to facilities (e.g., physical hardware, network, etc.), and access specifications according to users (e.g., administrator, guests), data, and media (host, devices).

The flow model provides a conceptual framework for defining and designing security strategy for PII handling in a manner similar to applying network and systems management processes to monitor intrusion detection, configure firewalls, etc. Of course, general security systems are concerned with breaches of personal information stored in networked computers; nevertheless, explicit design of a PII security system is necessary in order to ensure compliance with requirements based on statutes and regulations. Furthermore, PII exhibits unique characteristics (e.g., anonymity) that can be exploited by the designers. For example, access to a piece of PII that has been approved by a general security system is not necessarily an appropriate handling of PII. Access control systems usually do not control information propagation.

The PII security system may enforce additional constraints such as approval of *type of usage* of PII (e.g., OECD Data Quality Principle), requiring knowledge of the proprietor before releasing PII (e.g., OECD Collection Limitation Principle), etc. Accordingly, a PII security system may overrule a network and systems security policy. In addition, the PII security system involves end-to-end information flow including manual handling of PII.

Table 1. Types of PII Risks

Stage	Examples of Risks
Creating	Creation of false PII, creation of slander, notification failure Destruction of stored data, unauthorized access to stored data
Creating	Unauthorized use of raw data, risky use
Processing	Unauthorized processing of PII, inadequate processing (e.g., wrong results), illegal modification, refusal to grant access Unauthorized access to processed data, destruction of processed data Unauthorized use of processed data Unauthorized mining of PII
Collecting	Misplacement of collected data, inadequate collecting techniques, illegal collecting techniques, false information, policy declaration failure, refusal to give information
Collecting	Destruction of collected data, illegal entry of data
Collecting	Misuse of collected data
Disclosing	Unauthorized disclosure, unauthorized dissemination, falsification
Communicating	Unprotected communication channel
Communicating	Inadequate authentication
Communicating	Inadequate Non-Repudiation

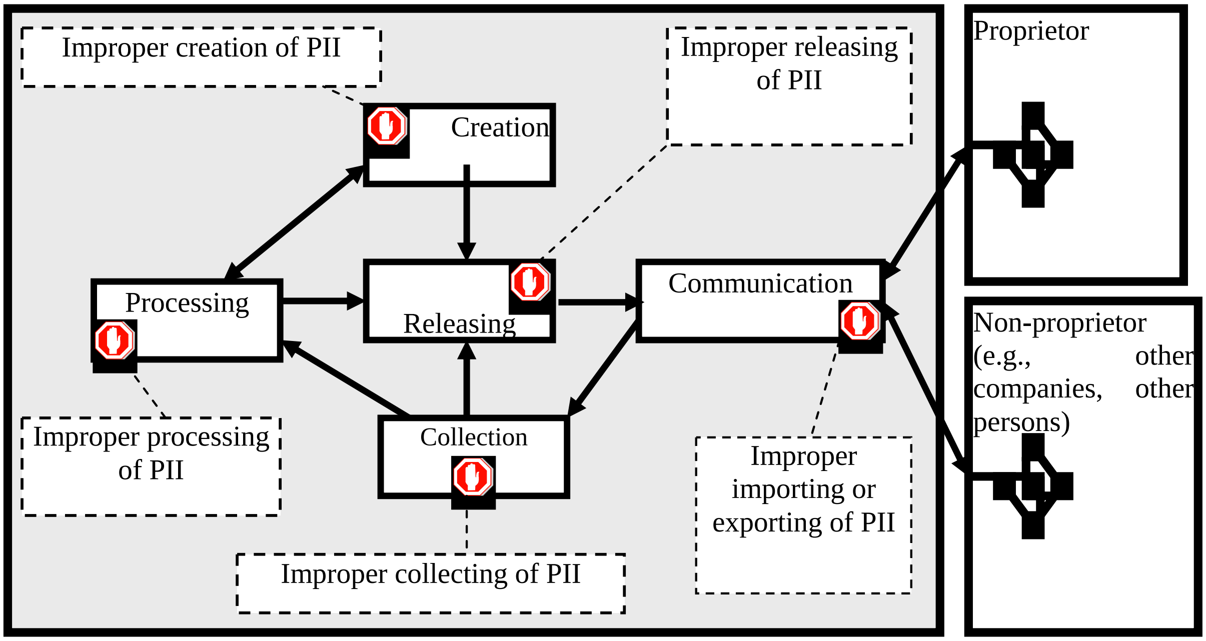
Improper creation of PII
Improper releasing of PII
Creation
Proprietor
Processing
Releasing
Communication
Non-proprietor (e.g., other companies, other persons)
Improper processing of PII
Collection
Improper importing or exporting of PII
Improper collecting of PII

Fig. (5). The PII flow model provides a complete map for the specification of security rules for PII handling.

We view a PII security strategy as including three basic components:

- Security problems/needs, including threats and risks to PII in terms of type and scale. An information flow–based model of threats deals only with informational threats such as authorized release, gathering, processing, creation, and transferring of PII.
- Security conceptual model based on information flow
- Security policies comprising rules for determining PII handling

The conceptual model serves at the level between security problems/needs and the solution that meets those needs, including development of information security policies. The conceptual model sketches the big picture of policies integrated into the organization through identification of critical sectors, connection origins, destinations, and control points along the five stages of the information flow. Development of a high-level map is similar to development of a network map before security features such as dial-in policy and password policy are drawn in.

Consider a Typical PII Specification Such the OECD Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data

We observe that the flow model raises several issues with regard to this principle. For example, does "loss or unauthorized access" cover raw, processed, mined, or newly created data? In real life, there is a tendency to consider raw data unimportant (data vs. information), while greater value is placed on decision-related information (e.g., *John is a bad risk*). Table **1** shows possible types of these risks. It is possible to further divide these risks according to sub-stages of the flow model.

The PII flow framework can be used to identify sources of information security problems; see Fig. (**5**). Such a map can be utilized in designing PII security and assessment systems. Further research would develop metrics to assess inherent risks of flow as defined in the flow model.

CONCLUSION

This paper studies personal identifiable information (PII) and its relationship to privacy and ethics. A workable definition of PII is introduced based on semantic reference to uniquely identifiable persons. The attachment of PII to an identifiable human being makes it the most valued type of information. The claim of this paper is that PII has an intrinsic moral value, because it reflects moral value conferred upon its proprietor as a human being. PII value may be significant or insignificant; nevertheless, it deserves moral consideration awarded to any piece of a human being.

REFERENCES

[1] Solove DJ. Conceptualizing privacy. Calif L Rev 2002; 90: 1087.

[2] Warren S, Brandeis L. The right to privacy. Harv L Rev 1890; 4: 193.

[3] Allen A. Uneasy access: privacy for women in a free society. Totowa, NJ: Rowan and Littlefield 1988.

[4] Bok S. Secrets: on the ethics of concealment and revelation. New York: Vintage Books 1989.

[5] Van den Haag E. On Privacy. In: Pennock RJ, Chapman JW, (Eds.) Nomos XIII: Privacy. New York: Atherton 1971.

[6] Posner RA. The economics of justice. Cambridge, MA: Harvard University Press 1981.

[7] Simmel A. Privacy is not an isolated freedom. In Nomos XIII: Privacy. In: Pennock RJ, Chapman JW, (Eds.), New York: Atherton 1971.

[8] Westin AF. Privacy and Freedom. Atheneum; 1967.

[9] Clarke R. Introduction to Dataveillance and Informational privacy, and Definitions of Terms; 1999. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

[10] Floridi L. Information Ethics: On the Philosophical Foundation of Computer Ethics. ETHICOMP98 The Fourth International Conference on Ethical Issues of Information Technology 1998. http://www.wolfson.ox.ac.uk/~floridi/ie.htm.

[11] Wacks R. Privacy in Cyberspace. In: Birks P. (Eds.), Privacy and Loyalty, Oxford, NY, Clarendon Press: 1997, pp. 91-112.

[12] Department of Motor Vehicles. Privacy and Security Notice. Internet Office, New York State, 2002, http://www.nydmv.state.ny.us/securitylocal.htm

[13] PIPEDA. PIPEDA Overview – What; 2004, http://privacy-forbusiness.ic.gc.ca/epic/internet/inpfbcee.nsf/en/hc00005e.html

[14] HIPAA. Glossary of Common Terms, Health Insurance Portability and Accountability Act of 1996. http://healthcare.partners.org/phsirb/hipaaglos.htm#g3

[15] EU Directive 1995/46/EC. On the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official J Eur Commun 1995. No. L 281, 23.11.

[16] P3P. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. http://www.w3.org/TR/2005/WD-P3P11-20050104/Overview.html#def_identity

[17] CPSR. Electronic Privacy Principles. Accessed March, 27, 2007. http://www.cpsr.org/issues/privacy/epp

[18] USACM. Policy Recommendations on Privacy. June 2006. http://www.acm.org/usacm/Issues/Privacy.htm

[19] Robert JS, Baylis F. Crossing species boundaries, In Shannon TA, Eds. Genetics: Science, Ethics and Public Policy: A Reader, 131-45. Readings in Bioethics. Lanham, MD: Rowman & Littlefield Publishers; 2005. http://books.google.com.kw/books? id=Oz1tJrSVamsC&pg=PA23&lpg=PA23&dq=ethics+%22privileged%22++morality+human+animal&source=bl&ots=rv81Pmn300&sig=kkMwFoyP5k_WlUqZOkV47vugZ9s&hl=en&ei=8jUEStm2CoisjAec3L2VCw&sa=X&oi=book_result&ct=result&resnum=10

[20] Cavalieri P. Are human rights human? LOGOS 4, 2 SPRING 2005. http://www.logosjournal.com/issue_4.2/cavalieri.htm

[21] Duncan GT. Ethics, mediating of disputes, and protecting privacy on the information highway. Proceedings of the AAAS Conference on Ethical, Legal and Technological Aspects of Network Use and Abuse. he Conference on Ethical, Legal and Technological Aspects of Network Use and Abuse October 7-9, 1994. www.aaas.org/spp/egii/opeds/DUNCAN.HTM

[22] Mathiesen, K. "What is information ethics?" Comput Soc Magn 2004; 32(8).

[23] Floridi L. An Interpretation of Informational Privacy and of its Moral Value. 7th Computer Ethics:Philosophical Enquiries Conference 2005. http://www.anvendtetikk.ntnu.no/pres/floridiabstract.pdf

[24] Kang J. Information privacy in cyberspace transactions. 50 Stanford Law Review 1998; 1193: 1212-20.

[25] Al-Fedaghi S. Crossing Privacy, Information, and Ethics. 17th International Conference Information Resources Management Association 2006a; May 21-24.

[26] Al-Fedaghi S. How Would Aristotle Define Privacy? The First International Conference on Legal, Security and Privacy Issues in IT 2006b; Hamburg, Germany.

[27] Al-Fedaghi S. How Sensitive is Your Personal Information? The 22nd ACM Symposium on Applied Computing 2007; March 11-15, Seoul, Korea.

Received: April 10, 2009 Revised: September 2, 2009 Accepted: September 3, 2009

© Sabah Al-Fedaghi; Licensee *Bentham Open*.

This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.