

2005

Lying about Private Information: An Ethical Justification

Sabah S. Al-Fedaghi
Kuwait University

Follow this and additional works at: <http://scholarworks.lib.csusb.edu/ciima>

 Part of the [Management Information Systems Commons](#)

Recommended Citation

Al-Fedaghi, Sabah S. (2005) "Lying about Private Information: An Ethical Justification," *Communications of the IIMA*: Vol. 5: Iss. 3, Article 5.

Available at: <http://scholarworks.lib.csusb.edu/ciima/vol5/iss3/5>

This Article is brought to you for free and open access by CSUSB ScholarWorks. It has been accepted for inclusion in Communications of the IIMA by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

Lying about Private Information: An Ethical Justification

Sabah S. Al-Fedaghi

Computer Engineering Department, Kuwait University
Tel. (965) 4987412, Fax: (965) 4839461, sabah@eng.kuniv.edu.kw

ABSTRACT

Lying motivated by a fear of misusing private information is a key issue in ethics with many important applications in law, business, politics, and psychology. In this paper, lying is separated according to two types of assertions: lying about non-private information and lying about private information. This distinction is applied to the case of the 'known murderer' in the context of Kant's categorical imperative. The main result of the paper is narrowing the ethical dilemma to a choice between 'a zero private information society' and 'an all-lying-about-private-information society'. We claim that privacy as a universal requirement supports lying about private information in order to avoid harm. This thesis has been applied to a current situation where customers, who are lying about their private information, are met with moral outrage and loss of credibility. Our conclusion is that enterprises have to modify their strategies and consider lying about private information, mainly, as a descriptive non-moral phenomenon that can be handled through primarily non-normative measures.

Key words: Lying, Private Information, Ethics, Privacy, Categorical Imperative.

INTRODUCTION

Lying is described as "the most significantly destructive political act in the Information Age" (Steiner, 1999). Technology has amplified the scope and effects of lying. It is often described as a primary way of living in modern society. Telecommunication technologies have opened up new situations that lead persons to lie. Internet users lie to protect their private or personal information. "Right now, the rate of falsification on Web surveys is extremely high, ... People are lying and vendors don't know what is false [or what is] accurate, so the information is useless" (Thomas, 2002).

Recent writers advocate considering deception as an ineradicable aspect of human nature and lying as an "artificial, deviant, or dispensable feature of life" (Campbell, 2001). To ease ethical anxiety in this lie-ridden atmosphere, several studies (Bok, 1978) have argued for a more discriminate use of lying, e.g., white lies, lies to enemies, lies protecting peers and clients, etc. The underlining position is that lying is acceptable in certain situations. Bok suggested that a justifiable lie should satisfy three requirements: no alternative courses of action, the moral arguments for the lie outweigh the moral arguments against it; and a "reasonable person" with no personal interest in the outcome would approve it.

Still, the basic problem is unsolved: Should we lie in the absence of other alternatives? Recommendations in this context include refusing to answer questions, evasive answers, running away, and so forth. Deontological ethics unyieldingly demand always telling the truth. The maxim that lying is wrong is applied even in non-common sense cases such as telling a murderer the whereabouts of his prey. We will dispute this controversial judgment utilizing the (moral) right of proprietorship (personal ownership) of private information as a moral justification for rejecting a request by non-proprietor (outsider) through the use of falsification – where there are no other means.

Moral outrage over lying about private information is the result of an implied assessment that the decision to release private information is based, primarily, on ethical considerations; and treating such a situation can be accomplished with moral enhancement techniques such as lecturing, moral encouragement, etc. If we show, in terms of Kant's deontological justification method, that lying about private information is morally justifiable when there is no alternatives; then, we have neutralized relying on the psychological feeling of compelling, and the authoritative force to pressure people (e.g., online consumers) to be truthful when submitting proprietary private information. People lie about their private information because their decision does not depend on the ethical code Lying is wrong; rather, mainly on objective elements; e.g., incentives, etc.

The rest of the paper includes four main sections. The first section introduces a new definition of private (personal)

information in terms of atomic linguistic assertions that refer to a single person. Alongside with this definition, it is maintained that there is a special relationship between an atomic private assertion and its proprietor (referent) that is different from such associations as possession and copyrighting. This relationship gives a special “right” to the proprietor of private information. The second section reviews the definition of the notion of lying. The third section presents our argument that disputes the deontological thesis that all lying is immoral. We claim that privacy, as a universal requirement, supports lying about private information in order to avoid harm. In the fourth section, we apply this result to the current situation, where it is reported that lying is a common phenomena in online commerce. Our result points out that enterprises have to modify their strategies and consider lying about private information, mainly, as a descriptive non-moral phenomenon that can be handled through primarily non-normative means.

PRIVATE INFORMATION DEFINITION

Linguistic forms of information or linguistic assertions provide us with the basic components of privacy (Al-Fedaghi, 2005a; Al-Fedaghi et al., 2005). Simply stated, assertions about individuals are private assertions. Consequently, linguistic assertions are categorized according to the number of their referents as follows:

1. Zero (privacy) assertion: An assertion that has no referent signifying a single individual.
2. Atomic assertion: An assertion that has a single referent signifying a single individual.
3. Compound assertion: An assertion that has several referents signifying individuals.

“Atomic” in this definition refers to the referent of the statement and not the composition of the statement that expresses fact. Linguistically, referents of type individual include the typical proper names, personal pronouns, and definite noun phrases.

Example: *John is shy*, and *John is in love* are examples of atomic (private) assertions because each has one (identifiable) referent. On the other hand, *Spare part ax123 is in store 5*, is a zero (privacy) assertion, because it does not involve any individual (human). *They are in love* is a compound (private) assertion because it has two referents. An atomic assertion is said to be the atomic private information assertion of the sole identifiable individual in the assertion. Compound information is said to be the compound private information of the set of identifiable individuals that it refers to. For simplicity’s sake, we may refer to ‘atomic/compound private information assertions’ as simply ‘private information’.

Possessions and Proprietorship of Private Information

Private information is also related to its possessors. A single piece of atomic private information may have many possessors; while its *proprietor* (i.e., the referent in the private information) may or may not be among them. A *possessor* refers to any entity that knows or stores or owns, ... the information. Individuals can have private information of other individuals and non-individuals, and companies/government agencies can possess a great deal of private information about individuals.

We call the relationship between individuals and their own atomic private information *proprietorship*. Proprietorship of private information is different from the concepts of possession, ownership, and copyrighting. If *p* is a piece of atomic private information of the individual *V*; i.e., *V* is its referent, then *p* is the *proprietary* private information of *V* and *V* is its *proprietor* so every piece of private information has its proprietor. A proprietor of private information may or may not be its possessor and vice versa. Individuals can be proprietors or possessors of private information; however, non-individuals can only be possessors of private information.

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 to others. Proprietorship of private information 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). Also, proprietorship of private information is different from the concept of copyrighting. Atomic private information of *V* is proprietary information of *V*, while others (e.g., other individuals, companies) can only possess it. Compound private information is the proprietary information of its referents: all referents of pieces of atomic private information that are embedded in the compound private information. It is also important to notice the difference between “proprietorship” and “knowing” of private information. ‘Knowing’ here is equivalent to a type of possession of private information. Atomic private information of *V* is proprietary information of *V*, but it is not necessarily “known” by *V* (e.g., secret medical tests of employees). Possession-based “knowing” is not necessarily a cognitive concept. It is possible that a non-individual (for example, a government agency) “knows” atomic private information of *V*. We assume that every piece of information is

“known” by someone, otherwise it is not information. “Knowing” is varied in its scope; thus, at one time, there may be a piece of atomic private information that is “known” only by a limited number of entities; later, it may become “known” by more entities.

Sensitive Private Information

According to our definition of atomic private information, every assertion about an identified individual is his/her atomic private information. Clearly, much of this atomic private information is trivial. Here, we can introduce the notion of sensitive private information. However, while ‘identifiability’ is a strict measure of what is private information, ‘sensitivity’ is a notion that is hard to pin down. It is “context dependent and thus global measures of sensitivity cannot be adopted” (Fule and Roddick, 2004).

There are degrees of sensitivity of private information. For example, one review of a tattoo artist said, "He's getting old and having problems with his eyesight." (Eden, 1995). After the artist hired a lawyer and threatened to sue, the Website changed its wording to, "His eyesight is not what it used to be." "Sensitivity" in the context of private information, refers to a special category of private topics that may disturb people. This description of sensitive private information is related to the typical definition where sensitivity of information refers to the impact of disclosing information. In this paper, we will assume that private information is also sensitive private information.

Private Misinformation

Consider the atomic private information; V is *honest*. Suppose that it is a true assertion. Does this imply that V is *dishonest*, is not private information? Can we say that if someone claims that V is *dishonest* then this is not a privacy-related case? Clearly, this is not acceptable. Describing V as honest or dishonest is a privacy-related matter regardless of whether the description is true or not. Atomic misinformation is said to be atomic private misinformation if its *referent* is an identifiable individual. Compound misinformation is said to be compound private misinformation if its referents are a set of identifiable individuals.

Private misinformation usually does not have the same significance as private information. It is not “a constitutive part of a me-hood” or “true self”, unlike private information. However, it is ‘private’ because it includes true identity. All characteristics of private information such as identification, sensitivity, secrecy, and publicity can be applied to any piece of ‘private’ misinformation. Even though it is misinformation, the proprietor may block others from possessing it for fear of being ridiculed, etc. So what is the property that separates private misinformation from private information? The only possible answer is, that what makes private information ‘private’ is its Double Truth. It is true in identifying a person (agreement with referent-part), and it is true as an assertion (i.e., agreement with its discourse). In private assertions (about ourselves), when we assert, we are reflecting ourselves in another form; so, if we are ‘true’, this (linguistic) form is true; otherwise, the resultant information is erroneous and we are ‘false’. We may claim that this is the underlying motivation of many great thinkers for defending truthfulness, to the extent that all lying is prohibited. Non-private information is different in the sense that it reflects abstract notions of morality not ‘us’ as in the case of private information.

DEFINITION OF LYING

Lying is a complex psychological phenomenon. People lie for a variety of reasons such as to avoid conflict, to save face, to please people, etc. Formally, a lie may be described as concealing information or falsifying it. Falsifying implies concealing information. Lying is confined to untrue linguistic expressions in order to exclude other forms of deception. We will limit ourselves to falsification or ‘formal lying’ where one asserts what he/she believes not to be true, or promises what one intends not to do. Thus, to lie is to make assertions that are untrue regardless of the actual situation (discourse) in terms of truth or falsehood. This state is shown in table 1.

Actual situation	The situation as believed by a person	Assertion
-	True	False
-	False	True

Table 1: Lying regardless of the actual situation (discourse).

The nature of intent is an important issue; nevertheless, we concentrate on the act of “intentionally asserting what is false” or intentionally falsifying what is true, and not on the act of “intentionally deceiving someone” (Macintyre, 1994). The immediate objective of this paper is not analyzing the notion of lying; rather, it is relating lying to private

information in a valid way. This context forces us to outline, in a sketchy non-exhaustive manner, some basic issues related to the objective. One important observation here is that in the context of proprietary private information, the actual situation and the believed situation coincide. This state is shown in table 2.

Actual situation	The situation as believed by a person	Assertion
True	True	False
False	False	True

Table 2: For proprietary private information, the actual situation and the believed situation coincide.

This type of falsification of proprietary private information is a lie both at the actual situation level and at the belief level. This type of lying will be called p-type (proprietary private information) lying. It concerns lying that involves the speaker's own private information.

For non-proprietary private information, lying (about others) is the process of producing misinformation that is associated with private information of others (atomic-of-others or compound assertions). This type of lying will be called n-type lying (Non-proprietary private information). Obviously in n-type lying, the actual situation and the belief of the speaker may not coincide. This categorization of private information creates "disunity" of a compound assertion through identification its atomic components, thus, creating moral sub-situations.

Example: Suppose a man "finds himself forced by necessity to borrow money" but is not able to repay the loan. Suppose that the man was asked directly whether he would be able to repay the loan. This is an example of compound private information. Let us denote the man as A and the loan giver as B. B asks A: "Will you able to repay me the loan?" This compound information question embeds the atomic assertions: *A will repay the loan*; *B will be repaid his/her money*. These two atomic assertions cannot be treated separately, as described previously in the discussion on compound private information. So, if A lies, he/she would give misinformation about himself (p-type of lying), about B (n-type of lying) and about their 'compound identity' created by the interaction between them. Hence, the maxim under consideration in front of A is: I give (private) misinformation about myself (p-type), misinformation about B (n-type) and misinformation about the me-B transaction.

This example shows one benefit of our definition of private information. It creates "disunity" of a compound assertion through identifying its atomic components, thus, creating moral sub-situations. It is possible to have a situation where:

P-type only: *A will repay the loan* is misinformation (p-type) while *B is repaid his/her money* is information because B can recover the money by other means such as –say– an insurance company.

N-type only: *A will repay the loan* is information but *B is repaid his/her money* is false because B will not get the money – say– A intends to give the money to B's ex-wife.

DEONTOLOGICAL ETHICS DOES NOT APPLY TO PRIVATE INFORMATION

The question, 'Should we lie in the absence of other alternatives?' has always been encountered with the unyieldingly answer of deontological ethics demand for truth. *Lying is wrong*, is almost a universally acceptable normative principle and as such, this act is met with moral outrage and loss of credibility. Lying about private information is considered a type of lying; hence it is judged to be morally wrong. This moral assessment of lying about private information is applied similarly to any person who gives untruthful private information; even when lying is allowed in certain circumstances, these circumstances are, typically, described as being "extreme, rare, great, or at least, special" (Newman, 1865).

Specifically, Kant's reasoning insists that truth telling must be universal. Its basic principle requires taking an action if its maxim is to become a universal law through our will. Our strategy in this paper is to give in to such a stringent demand, while splitting its universality feature by creating conflicting universal laws in sub-domains. The conflict occurs in the world of private information between *willing all-private-information-lies* and *all-private-information-revealing societies*. We claim the following thesis: *The person, who intends to reveal private information, should ask him/herself whether (a) he/she would 'will' that revealing private information should be made a universal law, or (b) he/she would 'will' universal untruthfulness in the context of private information. This is the choice between a 'zero private information society' and an 'all-lying-about-private-information society'. Choosing the second option, we claim that privacy, as a universal requirement, supports lying about private information.*

Kantian Morality

In proposing a criterion of moral obligation Kant argues that categorical oughts are derived from a principle called the Categorical Imperative. Kant's basic categorical imperative (CI) can be stated as follows: *Take an action if its maxim (general principle of conduct) were to become a universal law through your will; i.e. you want others to treat it as a moral law.* In applying the CI, one asks what maxim he/she would be adopting if he/she were to carry out the action. Then he/she asks whether he/she would be willing for the maxim to become a universal law of nature (i.e., be applied by everyone at all times and in all places). If the maxim can be made universal, then the action is a moral action. According to Kant, all categorical imperatives are based on this single basic categorical imperative CI. The difference in formulations of the CI is due to the fact that they are specially formulated with different referents (Bordum, 2002).

One of the major challenges to Kant's reasoning is that since truth telling must be universal, one must (if asked) tell a known murderer the location of his prey. Kant argued that it is indeed one's moral duty to be truthful to a murderer. If he/she is untruthful, then this registers a will to end the practice of telling the truth. The choice in this case, is between helping a murderer and 'killing truth'. Lying is fundamentally wrong, and we cannot rationalize it even when it leads to 'good'. Untruthfulness means willing universal untruthfulness since the net effect is that every one would tell lies. Also, Kant maintained that, if a person performs the correct act, telling the truth, then he/she is not blamable for any outcomes.

Lying and Private Information

We claim that any person who intends to give misinformation should first ask what type of misinformation it is: individual or non-individual; in analogy to a person who intends to kill, he/she first should ask what type of killing it is. Every one agrees that killing a *non-Individual*, such as a poisonous snake, is ethically different from killing an *Individual*. Each of these types of killings has completely different moral settings. Similarly, dealing with non-private information about a non-individual (e.g., The guns are hidden in the farm) has different moral consideration than private information concerning an identifiable individual (e.g., The man you are looking for is hiding in the farm). The analogy here is not between "Killing" and "information" but between categories and sub-categories of the two phenomena. Since subcategorizing is allowed in "killing", then its counterpart is allowed when dealing with information without considering it as a manifestation of a special situation. This notion is known among thinkers. In contrast to Kant, Milton philosophized "If all killing be not murder, nor all taking from another is stealing, why must all untruths be lies?" (Rickaby, 1918; Newman, 1865). Rickaby answered this question by saying that it is: "Because, we say, killing and taking away of goods, deal with rights which are not absolute and unlimited, but become in certain situations void; whereas an untruth turns, not on another's right, but on the exigency of the speaker's own rational nature calling for the concord of the word signifying with the thought signified, and this exigency never varies. Untruth and falsehood are but polite names for a lie" (Rickaby, 1918). According to Grotius, a lie is "injurious to the rights of others" (Grotius, 1925), i.e., it violates the right of the person spoken to.

We can see here how important our claim of the right of a proprietor to his/her private information is. We will disentangle private information from non-private information in order to reach to the conclusion that lying about private information has a different ethical base from lying about non-private information. Instead of basing the concept of lying on the right of "the person spoken to", we claim "lying" is a right that can be exercised by the private information proprietor. Hence lying, like killing, "deals with rights which are not absolute and unlimited." As will be discussed later, we don't provide a blank check to lie about private information. Also, Rickaby objects to considering the hearer's right as violated by a *simple* lie if the *right* carries the obligation of restitution. There is no notion of such an obligation in the proprietor's right's argument.

To a lesser degree, we claim the right of a possessor of private information to lie to its non-proprietor. Admittedly, this possessor's right is not based on as strong argument as the proprietor's right.

Kant also separates individuals from non-individual, when he provides his other formulated principle: the 'human integrity' principle. It says: *In every case, treat your own person or that of another, as an end in itself and never merely as a means to an end.* According to Korsgaard "the different formulations [of CI] give different answers to the question of whether if, by lying, someone may prevent a would-be murderer from implementing her or his intentions, that person may do so" (Korsgaard, 1986). From this, it is concluded that different formulations of CI narrow the restrictions imposed by the universalizability requirement (Macintyre, 1984). In our case, we claim that the 'human integrity' principle implies that dealing with "information of/about an identified human being" (private information) is tantamount to dealing with the human being him/herself.

Consider the act of lying that involves an identified Individual. The situation is restricted to the following circumstances: Somebody asks a person to reveal private information about an individual. So that person who intends to reveal this private information, should ask him/herself whether he/she would 'will' that: revealing private information should be made a universal law. We can easily imagine a world in which individuals always reveal their private information when queried. Therefore, this maxim is logical and everyone can abide by it without causing a logical impossibility. Would a rational being 'will' this maxim to become a universal law where in every case, a rational being would believe that the morally correct action is to reveal his/her or others private information? Even the most vigorous anti-privacy position does not agree with such a zero-privacy society. We claim that the act under consideration (telling a known murderer the location of his prey) or n-type of lying is not a moral act. This view was known in the non-private information context, where it is claimed that there is no duty to tell the murderer the information because "to tell the truth is a duty only towards a person who has a right to the truth" (Constant's view - Macintyre, 1984). Of course, Kant did reply lucidly to such a claim. Nevertheless, the claim is stronger in the private information situation. We interpret the 'right' here as the right to private information. So the CI and common sense, agree that the moral action is not revealing the private information of the prey.

Also, the proposed solution, lying or giving misinformation, is permitted when a non-proprietor inquires about private information that is not his/hers. Kant allows exceptions as long as they can be consistently universalized. Kant's constraint states that "any principle that warrants us in lying in certain circumstances, as to a would-be murderer, must be either one and the same principle that forbids us to lie in every other case or at the very least a principle that cannot generate possible inconsistency with that primary principle. The permitted or required lie must not be understood as an ad hoc exception, since, for reasons that Kant makes admirably clear, there cannot be such exceptions to genuine moral rules. And the principle that permits or requires a lie must not be some independent principle, potentially in conflict with the principle forbidding lying, since, for reasons that Kant also makes clear, our moral principles must be a consistent set, consistent to this degree that they do not, in any situation that has occurred or will occur or may occur, prescribe incompatible actions, so that one or the other has to be modified in an ad hoc way" (Macintyre, 1984). We claim that the privacy-base justification given previously satisfies all these requirements.

APPLICATION: THE CONSUMERS LYING PROBLEM

Consumer privacy is a mounting concern for e-commerce services that have been burdened with the problem of how to balance collecting private information with consumers' anxiety about their information privacy. According to a researcher at IBM's Privacy Research Institute, "consumers are not willing to give up their good data because of privacy concerns, and in the process, they are basically lying" (Wolverton, 2002). In August 2000, it was found that about a quarter of Internet users (24%) provided a fake name or personal information in order to avoid giving real information about themselves (Pew, 2000). In contrast, encryption email is used by 9 per cent and anonymizing software is utilized by 5 per cent of the respondents. According to one of the report writers, these users "assume the industry is out to exploit their information. (Lying) is the best way to fight back" (Charny, 2000). This report provoked some business executives to argue that "lying when releasing personal information should be made illegal and punishable by law" (Viseu et al., 2004; Charny, 2000). It is, also, reported that "one in five Americans engage in privacy protection behavior, like lying when they fill out forms, ... , or simply not seeking care at all to avoid having their health records released" (Nelson, 2000).

How do we handle this problem and encourage a customer to enter real private data? In addition to the legal aspects that are related to private information acquisition, the problem is, usually, handled by relying on:

Normative means: Normative principles are generalized operational terms of human conduct. By 'normative', we refer to a morality-based criterion. "Release truthful private information because lying is wrong" is a normative principle that appeals to inner virtues. Normative system, in this context, means the presence of moral force that presses on as an "action-guide" for "norms" (standards of right and wrong) that specify what ought to be done when releasing private information. This moral force utilizes normative means such moral outrage, loss of credibility, expressions of support for truth, etc. A normative-based environment carries the force of normative assertions such as: 'everyone ought to be truthful when releasing his/her private information because it is moral'. This paper advocates – based on the thesis that lying about private information is morally justifiable– that the normative value-laden means is not the right approach to encourage customers to enter real private data.

Procedural and technical solutions: Enterprises – to gain customers trust – have publicized privacy policies that claim fair information practices. Also, there has been a substantial increase in privacy-related projects such as standard initiatives (e.g., P3P) and, security and credentials trust negotiation research. For example, one attempt in

this direction is developing software that randomizes private information before transmitting it to the requester in order to encourage a customer to enter real data. According to the developers, "Lying" has been instituted "by making it happen scientifically", where "software will do a better job of coming up with a random value for age than (a customer) would" (Wolverton, 2002). In database research, lying can be used to preserve confidential information, even under inferences made by a (malicious) user (Biskup et al., 2001). The technique goes further by avoiding the detection of lying. These methods obviously don't rely on normative means.

Our solution involves applying the thesis that lying about private information is morally acceptable in the arena of online services. We claim that falsifying information –when you have to– about private information is not a lie; that is, customers have no ethical duty to tell the truth about private information to service providers. We consider that the condition of "having private information" justifies being untruthful. We concentrate on the proprietor's right to lie about his/her private information. Hiding private information (e.g., thought) is a natural state of humanity. Every person conceals an infinite stock of his/her private information (e.g., thought) and doesn't tell the whole truth and nothing but the truth, except in limited contexts. Hiding private information involves using several tools including misrepresenting oneself and lying about our private affairs – when needed. Note that this is not a consequentialist position. Furthermore, using lying to conceal proprietary (own) private information is a passive act, where some information is withheld. It fits in what we call passive privacy (Al-Fedaghi, 2005b). Passive Privacy means freedom "from" being subjected to others' activities with regard to private affairs. In this context lying about private information is simply an evasion to avoid privacy intrusion.

A Model

As it is mentioned previously, people lie for a variety of reasons; here, we construct our model such that lying is used to conceal private information. It is, also, assumed that a negative consequence (e.g., denying an available service) results, if private information is not provided. Note the following representative case (Lewis, 2003): "By purchasing a ticket, or completing a registration form so that you are able to access a purchase page for a ticket, to a concert, game or other event on the Site, you consent (i.e., you opt-in) to us sharing your personal information with ... ("Event Partners"). We cannot offer you a separate opportunity to opt-out, or not to consent, to our sharing of your personal information with them." So a "lie" in this case, is a tool to hide private information with no prime intention to deceive, rather an attempt to evade and avoid, and it contains no act to assert, only to report what is false. Also, it is assumed that other factors related to the situation are satisfied, e.g., the supplier of private information has satisfied all costs involved in providing the service. This model is designed specifically for a private information collection environment, where a person is required to release his/her private information beyond a certain limit set by the individual him/herself.

The OECD Guidelines on the protection of privacy and the EU's data protection directive limit the collection of personal data to data that is relevant for the purpose. The limit may be specified in terms of the sensitivity of the data and in terms of the amount of data collected. Both concepts are not well defined. Typically, a requester declares the limit as "what we need to know in order to achieve our goal of providing superior quality and value" (P&G, 2005).

Assume that the proprietor (supplier) does not want to release the requested private information; hence in response to such a request for private information, he/she can lie. We assume that the information under discussion is atomic private information. Atomic private information has two components: identity and identity-less components. For example, *John is 30 years old*, has the identity: *John*, and the identity-less component: *is 30 years old*. Consequently, lying about this atomic private information would involve:

1. Using a fictitious identity: Here we draw a line between a deliberate deception and crafted nondisclosure of private information. We exclude the option of using other people's identities because is not essential for protecting private identity
2. Using false identity-less information (assuming identity is known)
3. Using fictitious identity and false identity-less information

In the context of our model, we can claim the following proposition.

Proposition: In this model, lying in order to avoid disclosure of proprietary private information is morally acceptable.

Justification: We have shown in the analysis of the ethical dilemma of 'known murderer' in the context of Kant's Categorical Imperative that privacy as a universal requirement supports lying about private information in order to

avoid harm. Specifically, lying or giving misinformation is ethically permitted when a non-proprietor inquires about private information that is not his/her. The situation that we are modeling here is a restrictive version of the situation of 'known murderer' because the requested private information is proprietary information, i.e., the (potential) supplier of information is its proprietor.

Consequences

Based on this proposition, expecting people to release their private information by relying on the ethical principle that lying is immoral behavior is a fruitless effort. By its nature, ethical decision-making is determined within the individual and is free from external considerations. Enterprises (and society, in general) can influence the factors, which contribute to the process of ethical decision-making by such methods as preaching, persuasion, education, etc. More importantly, ethical decisions can be influenced through certain types of responses such as showing moral outrage, discrediting, lecturing, moral enhancement, etc. Through current assessment of the customers lying problem, we observe outcries to fight against lying about private information. The assumption is that lying/not lying about private information is basically an ethical decision i.e., what is good or bad? Such normative methods aim at producing 'attitudes' and its results are hard to test.

In contrast, persuading a person to invest his/her money is approached through presenting the enterprise investment policy, financial practices, financial reputation, alliances, ownerships, etc. This methodology is followed because it is understood that the decision is a non-normative (objective) decision. Our thesis that lying about private information is a morally justifiable action, implies that a decision to 'lie or not to lie' in this context, is predominantly a non-normative decision. If a person is requested to release certain private information, his/her decision does not depend on the ethical principle *Lying is wrong*, rather, it relies primarily on objective elements that can be presented by the requester. Currently, there is confusion between *Lying is wrong* and *Lying about your own private information is wrong – when needed*. The former is a moral principle that is stringently championed by many people, while the later assertion can be challenged under the same ontological justifications of the former. Consequently, an enterprise should orient its policy toward non-normative means instead of ethical-based techniques of persuasion.

Non-normative actions imply that decision-making, which resulted in producing such an action, is based on risk analysis associated with external factors with respect to the decision maker. Private information is defined as a true assertion; thus, the two basic ingredients of private information are: identification and truth. It is generally acknowledged that there are risks to telling the truth; hence, it is obvious that the combination of telling the truth and revealing identity is riskier. Private information is the conjunction of these two types of risks. Furthermore, trust can be enhanced among participants in the activity of private information collection, if well-defined non-normative methods of exchanging private information are used instead of social/ethical notions. Simply stated, the private information "market" ought to rely on well-defined market means to build trust and credibility. In an organization, the private information acquisition method should be oriented such that it depends on facts not on the hope that the customer believes that *Lying is wrong*. Every piece of private information should be analyzed in terms of its sensitivity (probability that the customer would consider it not necessary), its market value (can be dispensed with), its cost (how much we are willing to 'pay' for it), etc.

Lying and Society

Reconciling the well being of the individual with the good of society is one of the most persistent problems in ethics. Lying is socially objectionable because of the harm that is inflicted upon the social fabric of the society, which is sustained by mutual trust and credibility. Typically, those who advocate such an objection are consequentialists who allow certain types of lying to prevent some greater harm. We don't argue against such a thesis as we have argued against the deontological ethics. It is possible that "lying when releasing personal information" could be made "illegal and punishable by law" if it conflicts with a social value that is deemed to be more valuable. The law, in this case, would not be created based on the deontological principle: *Lying is wrong*.

CONCLUSION

We claim that dividing lying-based state of affairs into private and non-private information types eliminates moral difficulties that produce a non-common sense conclusion in situations that involve identifiable individuals. Using deontological justification methods, we have shown lying about private information – when needed– to be a morally justifiable state of affairs. Such a theoretical justification sheds light on known phenomena like customers lying about their private information in online services. Our ethical analysis have neutralized relying on psychological

feeling of compulsion, and authoritative force to pressure consumers to be truthful when submitting proprietary private information. Instead, it is important to distinguish between predominantly normative and descriptive aspect. In the later, the focus is on portraying the symptom in order to select the option with the highest utility.

REFERENCES

- Al-Fedaghi, S., Fiedler G., and Thalheim B. (2005). Privacy Enhanced Information Systems. *Proceedings of the 15th European-Japanese Conference on Information Modelling And Knowledge Bases*, Tallinn, Estonia, 165-182.
- Al-Fedaghi, S. S., (2005a). How to Calculate the Information Privacy. *Proceedings of the Third Annual Conference on Privacy, Security and Trust*, October 12-14, St. Andrews , New Brunswick, Canada.
- Al-Fedaghi, S. S., (2005b). The 'Right to Let Alone' and Private Information. *Proceedings of the 7th International Conference on Enterprise Information Systems*, Miami (USA), 98-107.
- Biskup J., & Bonatti, P.A. (2001). Lying versus refusal for known potential secrets. *Data and Knowledge Engineering*, 38(2),199-222.
- Bordum, A. (2002). The Categorical Imperative Analyzing Immanuel Kant's Grounding for A Metaphysics of Morals. MPP Working Paper No. 4/2002. Retrieved June 10, 2005, from http://www.tannerlectures.utah.edu/lectures/macintyre_1994.pdf
- Campbell, J. (2001). *The Liar's Tale: A History of Falsehood*, New York: W. W. Norton.
- Charny B. (2000). Protect your Internet privacy ... by lying, ZDNet News. Retrieved June 10, 2005, from http://membrane.com/security/java_and_cookies/notes/consumers_lying.html
- Grotius, Hugo (1925). On the Law of War and Peace. Translated by F. Kelsey, Indianapolis: Bobbs-Merrill.
- Korsgaard, C. (1986). The Right to Lie: Kant on Dealing with Evil. *Philosophy and Public Affairs* 15, no. 4.
- Lewis H. G. (2003). Firm Commitments and Other Lies. Articles, PRIMEDIA Business Magazines & Media Inc. Retrieved June 16, 2005, from http://www.findarticles.com/p/articles/mi_m3815/is_12_15/ai_108325265
- Macintyre, A. (1994). Truthfulness, Lies, and Moral Philosophers: What Can We Learn from Mill and Kant? Retrieved June 7, 2005, from http://www.tannerlectures.utah.edu/lectures/macintyre_1994.pdf
- Nelson J. (2000) The Senate Committees on Health Services and Economic Development examine privacy issues at the State Capitol. Texas Senate News, May 15, 2000. Retrieved June 7, 2005, from <http://www.senate.state.tx.us/75r/Senate/Archives/Arch00/p051500a.htm>
- Newman, J. (1865). Apologia pro Vita Sua, Works of John Henry Newman. Retrieved June 7, 2005, from <http://www.newmanreader.org/works/apologia65/noteg.html>
- Pew (2000) Internet and American Life Project released Trust and Privacy Online: Why Americans Want to Rewrite the Rules. Retrieved June 7, 2005, from http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf
- P&G (2005), Global Privacy Policy, Retrieved June 10, 2005, from http://www.pg.com/company/our_commitment/privacy_policy/privacy_policy.jhtml
- Rickaby, J. (1918). Moral Philosophy: Ethics, Deontology and Natural Law. Longmans, Green & Co., London. Retrieved June 12, 2005, from <http://www.nd.edu/Departments/Maritain/etext/moral.htm>
- Steiner, C. (1999). TRANSACTIONAL ANALYSIS IN THE INFORMATION AGE. *The ITAA Conference*, San Francisco, August 1999. Retrieved June 12, 2005, from <http://www.emotional-literacy.com/tainfo.htm>
- Thomas, R. (2002). Random privacy. *Plus Magazine*, September, Retrieved June 12, 2005, from http://plus.maths.org/issue21/news/random_privacy/

Viseu A., Clement A., & Aspinall J. (2004) Situating Privacy Online: Complex Perceptions and Everyday Practices. *Information, Communication & Society*, Volume 7, Number 1 / March 2004, 92 – 114. June 12, 2005, from <http://72.14.207.104/search?q=cache:8GEITgj2iPkJ:aoir.org/members/papers3/viseu.pdf+%22personal+information+should+be+made+illegal+and+punishable+by+law%22&hl=en>

Wolverton, T. (2002) IBM serves scrambled data for privacy. ZDNet, May 31. Retrieved June 15, 2005, from <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2868650,00.html>