Proceedings of the 5th WSEAS Int. Conf. on APPLIED INFORMATICS and COMMUNICATIONS, Malta, September 15-17, 2005 (pp7-15)

Privacy as a Base for Breaching Confidentiality

SABAH S. AL-FEDAGHI
Computer Engineering Department
Kuwait University
P. O. Box 5969 Safat 13050
KUWAIT

Abstract: - Developing principles that address the confidentiality of health information, has presented significant challenges in society, particularly to health care providers. In this context, an important dilemma is whether to breach confidentiality in the case of the risk of harming identifiable individuals. This paper argues that the RIGHT of the third-party person to his/her private information outweighs maintaining patient confidentiality. The private information involved is 'compound' information that identifies several individuals, hence, is 'owned' by all of its proprietors. A systematic approach to confidential private information is introduced based on defining the private information in terms of assertions about its proprietors: those identifiable individuals that are referred to in the assertions. We apply this thesis to the *Tarasoff* case and extend our ethical justification to cover breaching confidentiality in genetic testing.

Key-Words: - Breaching Confidentiality, Privacy, Health Information, Private Information Ethics

1 Introduction[1]

Developing principles that address the confidentiality of health information has presented significant challenges in society, especially to health care providers and the public. 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 (HIPAA) have heightened awareness of ethical dilemmas related to this issue. Furthermore, the increasing use of information technology in health care and advancements in health research, have contributed to the importance of studying the ethical, legal, and policy issues associated with privacy and confidentiality rights.

The foremost of these rights is the information confidentiality in the 'health care provider-patient' relationship, which is seen as central to the maintenance of their mutual trust. It described as "one of the most fundamental ethical obligations owed by a doctor to his patient" [21]. A breach of confidentiality is a disclosure, without consent or legal justification, of information that the health care provider has learned within the provider-patient relationship. Typically, professional ethical guidelines maintain that patient confidentiality is a moral duty.

In this context, the dilemma is whether to breach confidentiality in the case of the risk of harming identifiable individuals or to society at large. The consequentialist stance considers the duty of confidentiality as not being absolute. According to the General Medical Council [20], "Disclosure of personal information without consent *may* be justified in the public interest where failure to do so may expose the patient or others to *risk of death or serious harm*. Where the patient or others are exposed to a risk *so serious* that it outweighs the patient's privacy interest, you should *seek consent* to disclosure where *practicable*... You should generally *inform the patient* before disclosing the information." However it is unclear what constitutes a 'serious harm' that outweighs the obligation of confidentiality. The circumstances in which a breach of confidentiality might be justified are contested within the domains of law and professional codes of conduct. These circumstances include avoidance of danger to others, protection of vulnerable persons, medical research, prevention of crime, etc.

On the other hand, the deontological stance towards this issue always demands patient confidentiality regardless of the circumstances. "Breaching confidentiality causes harms that are not commensurate with the possible benefits gained ... excusing breaches of confidence on the grounds of superior moral values introduces arbitrariness and ethical unreliability into the medical context" [23].

[1] A preliminary version of this paper was presented in the *Fourth Workshop on the Economics of Information Security*, Harvard University, Cambridge, MA, June 3-5, 2005, under the title: *Privacy as a Base for Confidentiality* (Rump Session: http://infosecon.net/workshop/schedule.php).

There are legal cases where the court accepted a doctor's right to maintain confidentiality even when it involved the identification of a potential murderer (QB 967, 2 WLR 992). "This may lead one to think that doctors owe no legal duty to break their patients' confidentiality, except when they are specifically required to do so by law" [11].

We advocate that breaching of confidentiality in these situations is a moral act based on the person's right to his/her private information. Our argument is not based on the utilitarian ethic, which suggests that the confidentiality duty can be overridden when the utility of disclosure outweighs the utility of confidentiality. Rather, we show that the privacy RIGHT of the third-party person to his/her private information outweighs the patient's confidentiality obligation. The confidential information involved is information that identifies several individuals. This 'compound' private information is 'owned' by its proprietors just as private information that identifies a single individual is 'owned' by that individual.

This paper is organized into four sections. First, in section 2, we review a new definition of information privacy given [1]. Section 3 addresses the issue of confidentiality of patient's private information. We apply our thesis regarding the breaching of confidentiality to one of the landmark cases in this area, which is the *Tarasoff* case. In section 4, we utilize our ethical justification for breaching confidentiality in the area of genetic testing.

2 Private Information

Defining private or personal information is a problematic issue. "Privacy means different things to different people, including the scholars who study it, and raises different concerns at different levels" [26]. Privacy is usually said to be a culturally defined notion. Wacks defines it as "those facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or confidential and therefore to want to withhold or at least to restrict their circulation" [27]. Several types of privacy have been distinguished in literature including physical privacy and informational privacy [28] [29]. Recent results have defined 'private information' in terms of true linguistic assertion that refers to an identifiable individual. An ontological definition of private information can be developed from linguistic assertions in order to identify the basic units [1] [2].

The linguistic forms of information or linguistic assertions provide us with the basic components of informational privacy. Simply, assertions about individuals are private assertions. Consequently, linguistic assertions are categorized according to the number of their referents as follows:

(i) Zero (privacy) assertion: An assertion that has no referent signifying a single individual (e.g., *Spare part ax123 is in store 5*).

(ii) Atomic assertion: An assertion that has a single referent signifying a single individual (e.g., *John W. Smith is twenty years old*).

(iii) Compound assertion: An assertion that has several referents signifying two or more individuals (e.g., *John W. Smith and Mary K. Jones are in love*).

In (ii) the referent refers to a single individual (person). The compound assertion in (iii) embeds two atomic assertions *John W. Smith is in love* and *Mary K. Jones is in love*.

The *proprietary* of private information as defined above, is conferred only to its subject. Private information is also related to those who possess it. A single piece of atomic private information may have many possessors; where its *proprietor* may or may not be among them. Atomic assertions can be possessed by any entity including non-individuals (e.g., companies, government agencies, etc.) Individuals (persons) can have private information of other individuals. Companies and government agencies can possess a great deal of private information about individuals. Possession of atomic private information is materialized either as a result of direct possession of atomic private information or as a result of possession of compound private information. In law, the term 'possession' is used to indicate having, holding, or detention of property. It is different from the notion of ownership. "Ownership" implies rightful (legal) or wrongful (illegal) ownership. Historically, rights to property were legally extended gradually to intangible possessions such as processes of the mind, works of literature and art, good will, trade secrets, and trademarks [14]. Both in the past and the present, private property has facilitated means to protect individual privacy and freedom [9]. However, even in the 19th century it was argued that, "the notion of privacy is altogether distinct from that of property" [10].

We identify the relationship between individuals and their own atomic private information through the notion of *proprietorship*. Proprietorship of private information is different from the concepts of possession, ownership, and copyrighting. Any

atomic private information of an individual is *proprietary* private information of 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. '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 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).

The atomic private information of an individual is his/her proprietary information, while others (e.g., other individuals, companies) can only possess a copy of it. Compound private information is proprietary information of its referents: all donors of pieces of atomic private information that are embedded in the compound private information.

2.1 Compound Private Information

Atomic private information of an individual can be embedded in compound private information: a combination of pieces of atomic private information of several individuals. Two or more individuals have the same piece of compound private information because it embeds atomic private information from these individuals. But it is not possible that they have identical atomic private information simply because they have different identities.

Compound private information is not a collection of atomic private information; and it is not a "putting-together" connection. A compound assertion is not only privacy-reducible to a set of atomic assertions, but it is more than that. It is a "bind" that not only contains atomic assertions, but also asserts something about its own assertions.

Is compound private information privacy-replaceable by its embedded set of atomic private components? Reducing a compound assertion to a set of atomic assertions refers to isolating the privacy aspects of the compound assertion. This means that, if we remove the atomic assertion concerning a certain individual from the compound assertion, then the remaining part will not be a "purely" privacy-related assertion with respect to the individual involved. The 'protection' of atomic private information applies naturally to the corresponding compound information. Suppose we have the compound private information, *John saw Mary's uncle, Jim*. The privacy-reducibility process produces the following three atomic private assertions: *John saw someone's uncle*, *Mary has an uncle*, and *Jim is an uncle of someone*. Additionally, we can introduce the zero-information meta-assertion: *The three assertions form a single piece of compound private information*, from which it is possible, in principle, to reconstruct the original compound assertion. The methodology of syntactical construction is not of central concern here.

2.2 Sensitive Private Information

We have defined every piece of information that includes an identifiable person as private information. The private information can be sensitive or non-sensitive, but both of these types are encompassed by the given definition: they refer to identifiable individuals. It seems that privacy "should come, in law as in life, too much less ... [than] all information about oneself" [25]. Here we can introduce the notion of 'sensitive' private information. However, while identifiability is a strict measure of what private information is, 'sensitivity' is a notion that is hard to pin down. It is "context dependent and thus global measures of sensitivity cannot be adopted" [18]. It is difficult to specify what sensitive information is. In general, sensitive information is a category of private information that would typically include particular types of information such as racial or ethnic origin, political opinion, membership of a political association, sexual preferences or practices, criminal record, health information, etc. These types of information are usually "sensitive" in most contexts. Potentially, sensitive information depends on the context (e.g., culture, situation). Many factors contribute to the level of sensitivity of private data including: identifying information (e.g., social security number), and certain other kinds of information (sex-related information).

Information 'sensitivity' is typically defined in terms of the necessary protection level required for that information. The misuse, or unauthorized access to, or modification of information could adversely affect, or be of risk to the owner of that information. Sensitive information is information that requires protection due to risks that could result from its disclosure, alteration, or destruction. Hence, the level of required security for protecting the data determines the sensitivity of data. For example, since confidentiality implies restriction of access (security), this confidential data is understood to be sensitive data. In this case, the question 'what is sensitive information?' is answerable through identifying its required level of security.

"Sensitivity" in the context of private information refers to a special category of private topics that may disturb people. This characterization of sensitive private information is related to the typical definition where sensitivity of information refers to the impact of disclosing information. We will assume that the private information under consideration is sensitive private information.

3 Confidentiality of Patient's Private Information

From the Hippocratic oath onwards, confidentiality has always been a fundamental obligation in the medical profession. It is also stressed in all ethical codes of health care professional institutions/organizations. Respecting confidentiality builds a relationship of trust and makes patients more willing to share information. The confidentiality of the patient's private information has been protected by many laws. However this information can be disclosed to others in certain situations. This may be accompanied with the claim that the right to privacy is not absolute in nature. Legal and ethical difficulties have risen in this context. An important dilemma is whether to breach confidentiality if others may be at risk of harm from a patient. In this section, we will first examine the notion of confidentiality according to the definition of private information given in the previous section. This concept is applied in the context of the well-known *Tarasoff* case, which involves a conflict between maintaining patient confidentiality vs. the third-party person's right to his/her private information.

3.1 Private Information Ethics

One of the prime concerns in ethics is developing an ethical theory that involves studying moral principles and the interpretation of moral terms. The ethical philosophical investigation is applicable to all human activity and by no means confined to application in any one area. Applied ethics concern with applying the principles of general ethics in a given specific field of human realms.

Private Information Ethics (PIE) concerns with the "moral consideration" of private information because private information's 'wellbeing' is manifestation of proprietors' welfare. Moral consideration of being a piece of private information 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 private information is considered to have an intrinsic moral value in addition to its instrumental value. This intrinsic moral status comes from the intrinsic moral status of its proprietor. Or more accurately, the "moral considerability" of private information by agents stems from the proprietor's right for 'privacy'. Consequently, in the private information ethics studies, many of the classical ethical issues includes private information confidentiality, private information trust, private information lying [2], etc.

3.2 Confidentiality

Confidentiality involves sharing of information with the expectation that it will not be revealed to third parties, or that it will be revealed under restricted circumstances [12]. It implies controlling access to information and its release according to a certain implicit or explicit agreement. Confidentiality is said to be central to the maintenance of trust. In PIE, 'private information trust' is valuing of a trustee to be (a) a reliable, and (b) worthy; hence a decision is taken to disclose/withhold private information. 'Reliability' in (a) is a risk-based utilitarian decision that the trustee *measures up* to the instrumental value of private information. 'Worthiness' in (b) refers to a subjective judgment that the trustee measures up the intrinsic value of the private information.

Definition: Confidential information is information that is disclosed with an explicit or implicit agreement that it will not be revealed to a third party without the consent of its owner(s).

In the private information context anonymity and confidentiality coincide. This is not necessary outside this context. According to Pearson [5], "Reducing the risk of disclosing the identity of individual records are more accurately defined as a concern with protecting their anonymity; not their confidentiality, as it is frequently asserted."

The general notion of confidentiality is usually applied to private information and non-private information (e.g., government secrets and trade secrets) [13]. Confidentiality of private information implies the protection of other people's private information through controlling the access to information and its release according to a certain established agreement. It is a form of anonymity. Suppose that the information is *John has syphilis*. The anonymized version of such an atomic assertion is *Someone has syphilis*. Certainly, this anonymized

assertion is not confidential information. Similarly, anonymizing *John intends to kill Mary* can be anonymized with respect to John as *Someone intends to kill Mary*. The latter statement is not confidential information assuming it does not identify John uniquely. It is common for journalists to use anonymous informants. The identities of the informants are confidential, but are known to the journalists [22]. Thus, the identity of the proprietor is an integral component of the confidentiality of private information.

Definition: Confidential Private Information (or simply CP information) is private information that is released by its proprietor(s), with an explicit or implicit agreement that it will not be revealed to a third party without the consent of its proprietor(s).

CP information can be classified as atomic and compound CP information. We will argue the following thesis: CP compound information is a proprietorial relationship among all of its proprietors. This implies shared proprietorial rights. They are explicitly or implicitly participants in any type of arrangement concerning their CP information. Thus, any confidentiality agreement involves all proprietors, e.g., their consent is required for revealing this information. Furthermore, this has ethical implications such as when a person receives CP compound information from one of its proprietors, then it is the ethical obligation of that person to inform other proprietors who have the right to know about their private information. In practice, the "strength" of this ethical conduct depends on how valuable the CP information is, similar to the ethical situation when a person finds a lost thing that's owned by someone else. Accordingly, we claim that the health service provider who has CP information, is a possessor of information that belongs to all of its proprietors, thus, any patient-provider confidentiality agreement does not cover this type of information. We next analyze this claim in terms of the known Tarasoff case.

Put in other words, the obligation to maintain confidentiality based on 'worthiness trust' (PIE's trust is a valuing based on reliability and a worthiness) assumes that the trustor is the proprietor. The thesis in this paper is that the trustee has no obligation to maintain confidentiality if the trustor is not the proprietor.

3.3 The *Tarasoff* decision

The facts of the *Tarasoff* case considered by California Supreme Court are as follows. Poddar was an outpatient of a psychiatric hospital. He had depression related to his rejection by Tatiana Tarasoff with whom he had fallen in love. Poddar told Moore, Poddar's Psychologist that he intended to kill Tatiana Tarasoff. Moore informed the campus police and his supervisor of Poddar's intent. The police detained Poddar but after a short detention released him. Two months later, Poddar killed Miss Tarasoff. In civil proceedings, the Tarasoff family accused the therapist of causing wrongful death citing the therapist's failure to warn the Tarasoffs that Poddar was a grave danger to their daughter.

The Californian Supreme Court held that the therapist is liable for his failure to warn the victim. According to the court "When a therapist determines, ... that his patient presents a serious danger of violence to another, he incurs an obligation to use reasonable care to protect the intended victim against such danger. The discharge of this duty may require ... to warn the intended victim or others likely to apprise the victim of the danger, ..." [7]. Also, "... the therapist's obligations to his patient require that he not disclose a confidence unless such disclosure is necessary to avert danger to others, and even then that he does so discreetly, and in a fashion that would preserve the privacy of his patient to the fullest extent compatible with the prevention of the threatened danger." The court limited the *Tarasoff* decision to identified victims. Other courts have also specifically required warning victims only when there is "an overt threat of violence toward a specifically identifiable victim" (Brady v. Hopper, [6]).

The 1976 *Tarasoff* decision by the California Supreme Court has been adopted in many jurisdictions and expanded to include a wide variety of health care practitioners. In a related case, a patient told a mental-health professional that he felt like killing his stepfather. The mental-health professional did not report the threat. Later, the patient killed his stepfather (*Thapar v. Zezulka*, [15]). In a 1999 decision, the Texas Supreme Court held that a mental health care professional does not have a duty to warn third parties of a patient's threats. In reaching its decision, the Supreme Court reasoned that the statute takes precedence over case law. The Texas Legislature had adopted a health and safety code, which did not require a warning to potential victims. We will consider this point in the next section.

3.4 Informational Privacy-based Analysis

In analyzing the Tarasoff case, the assertion *Poddar intends to kill Tarasoff* is clearly a piece of compound private information in Moore's possession. Poddar told it to Moore. Any mental-

health professional is a facilitator of transfer of CP private information from a patient to his/her possession. The whole dilemma started when Moore helped in moving the threat from Poddar to Moore's possession. Since the involved (threat) assertion is compound private information, it is not solely the proprietary private information of Poddar. It is also proprietary private information of Tarasoff. In its atomic form, the "Tarasoff side" of the compound information can be stated as: *Tarasoff is an intended victim of murder* or *There is a plan to kill Tarasoff*. So Moore is no longer dealing with the "private sphere of Poddar" but also with the "private sphere of Tarasoff." Contrast this with Poddar telling Moore that he intends to kill a dog, or cut a tree where the information is proprietary private information of Poddar. In this case, all clichés of confidentially of a patient can be asserted because it does not embed private information of another individual. Consequently, we claim that compound private information should not necessarily be included in the notion of doctor-patient confidentiality.

Typically, the Tarasoff case is viewed as addressing "the conflict in weighing the patient's right to confidentiality and the need for a trusting psychotherapist-patient relationship in therapy against society's right to be protected from a foreseeable, dangerous, and potentially lethal event" [3]. In our approach, the case involves the conflict between the patient's right to confidentiality vs. the third-party person's right to his/her private information.

Ethically, if we apply this dilemma to Kant's imperative, then the maxim under consideration would be: I respect the right of every person to know his/her private information. The 'will' to respect a 'right' seems to overcome any derivative notion such as psychotherapist-patient confidentiality. Confidentiality is a mutual agreement while the right of informational privacy is a "mine-ness" right that refers to the right of a person to his/her own. It is a stronger right than ownership. If someone finds a thing that is owned by an individual, then he/she has the duty to return this thing to the owner. Similarly, a piece of private information missing from its owner should be returned to him/her. Furthermore, in the CP information case, the confidentiality agreement extends implicitly to other proprietors. So in the CP information case, the therapists have the duty of confidentiality to their patients and implicitly to the third parties as well. The 'third party' refers to any proprietor of the CP information besides the patient. The therapists are in possession of personal identifiable information that is also the proprietary information of this third party. Even the disclosure of this (compound) private information (e.g., to a patient's family) requires the consent of this third party as much as it requires the consent of the patient. If the patient does not mention in his/her threat an identifiable person, then no compound private information is involved; hence, any person who becomes a victim of the patient can claim no right to private information. Courts have already confirmed this conclusion and cases have been dismissed on the ground that no evidence was there as an explicit threat to an identifiable person (e.g., *Leonard v. Latrobe Area Hospital*, Pennsylvania; *Thompson v. County of Alameda*, California; *Brady v. Hopper*, Colorado – see [7]).

3.5 Privacy and Safety

In this discussion therapist becomes sufficiently involved to assume some responsibility for the safety not only of the patient himself but also for any third person whom the doctor knows to be threatened by the patient ..." The California supreme court asserted that confidentiality "ends where the public peril begins" [7]. Notice that the therapist in the Tarasoff case did warn the police about the potential danger of Poddar, but did not inform Tarasoff herself. In these cases, matters may involve safety alongside privacy. Privacy-based justification is different from "limitation to the privilege of confidentiality, ... [as in] ... lawyers must keep communications from clients privileged, except if such communication pertains to the execution of a future crime." Typically, disclosure of confidential medical information is based on the utilitarian justification that it is of the public interest where the benefits to society outweigh the patient's interest in keeping the information confidential. A therapist-patient relationship establishes a duty for "the right to privacy" and not for "the sake of safety of the patient and the public" [7] [16]. According to Fleming and Maximov, "... by entering into a doctor-patient relationship, the therapist becomes sufficiently involved to assume some responsibility for the safety not only of the patient himself but also for any third person whom the doctor knows to be threatened by the patient ..." [16]. The California Supreme Court asserted that confidentiality "ends where the public peril begins" [7]. Notice that the therapist in the Tarasoff case did warn the police about the potential danger of Poddar, but did not inform Tarasoff herself. In these cases, matters may involve safety alongside privacy. Privacy-based justification is different from "limitation to the privilege of confidentiality, ... [as in] ... lawyers

must keep communications from clients privileged, except if such communication pertains to the execution of a future crime" [3]. Typically, the disclosure of confidential medical information is based on the utilitarian justification that it is of the public interest where the benefits to society outweigh the patient's interest in keeping the information confidential.

Our justification for releasing CP information has a deontological base and is not based on evaluating consequences related to "third party safety." Suppose that Poddar told Moore that he intended to set fire to a certain building. This information is not private information of a third party because it does not involve an identifiable individual. The dilemma here concerns confidentiality vs. public safety (consequential) not confidentiality vs. right to private information (deontological). Here, we can touch on the issue of "laws inevitably threaten the benefits that flow to consumers and the economy from responsible information-sharing." According to Cate and Staten, "no privacy law should be enacted unless the harms it addresses are explicitly balanced against the law's interference with the benefits that flow from information-sharing" [8]. By the same type of logic, we can claim that no anti-privacy law should be enacted unless the benefits it addresses are explicitly balanced against the law's interference with the protection of individuals. So Texas Legislature adaptation of health and safety code, which governs the disclosure of communication during the course of mental-health treatment, has an unnecessarily wide scope. The statute permits, but does not require, disclosure, if the professional determines that there is a probability of harm to the patient or others. This should be applied to the non-private harm mentioned above (e.g., setting fire), where such a view can be based on reason and a mature sense of social responsibility [7] [16]. However, the law should specify that when the harm involves an identifiable individual, then he/she has the right to know about this harm, regardless of confidentiality and professional practices. This argument with regard to CP information can be used to counter claims that the patients would be deterred by a lack of confidentiality. It also gives more options at the social policy level. The patients can be informed in advance what kind of confidential information is DEFINITELY not protected by the confidentiality of a therapist-patient relationship. Private information of a third party should not be part of the so-called "negotiated confidentiality." Also CP privacy-based justification can be used to argue that the therapist owes no confidentiality duty to a patient and thus there is no foundation to claims of liability in tort and/or a patient's claim for embarrassment resulting from the disclosure of private information that also belongs to a third party.

One of the interesting options that resulted from this fine discernment of confidentiality is the ability to inform the potential victim without revealing the identity of the source and/or the assailant. For example, Moore could inform Tarasoff that there is a plan to kill her without mentioning Poddar. Here, not revealing the source of the therapist's information becomes an issue that is similar to the issue of news reporters protecting their sources. In the Tarasoff decision, the court "provided therapists greater latitude to "protect" intended victims, rather than to "warn," as the only alternative" [7]. This latitude can be applied to "warning" itself, where informing Tarasoff without mentioning Poddar is a "base-line warning" for the potential victim. Also a privacy-based justification for releasing confidential information in a doctor-patient relationship is a stronger ground than characterizing vague standards such as "a duty to use reasonable cause to protect third parties from becoming victims" [3].

3.6 Informing Proprietors

How can we formulate the therapist-patient confidentiality when it involves other individuals? Does this mean that the therapists must inform the third party about every piece of private information concerning them mentioned by their patients? We propose the following guidelines:

1. It is the right of every individual to access any of his/her private information held by others. This right is relinquished only through the consent of the individual (e.g., employment contracts).
2. A person who has in his/her possession private information has the obligation to inform its proprietor based on "duty of care" that requires everything 'reasonably practicable' (e.g., sensitive private information) to be done to protect the welfare (e.g., health and safety) of others.

This utilization of the notion of "protecting the health and safety of others" here is not in conflict with confidentiality. The patient's right to confidentiality is not an issue in the CP information context. Under the concession that it is the right of every individual to access any of his/her private information (e.g., Tatiana Tarasoff) held by others (e.g., therapists), the concern here is what the "founders/possessors" (e.g., therapists) of this information should do. Analogously, we can ask: Is it the duty of anyone who has found a lost thing to return it to its owner? If we apply the "duty of care" principle, then returning that thing is a duty when it is "worth something" to its proprietor. Similarly,

information such as "someone doesn't like you", "someone thinks that you are a fool", etc. are "worthless" information, and it is not the duty of its possessor to "deliver" it to its proprietor. Some of these statements may also be misinformation or trivial assertions. However, the duty of care requires informing the proprietor of private information whenever this information is related to his/her welfare. Also, clearly, a person does not have the right to his/her private information in certain situations such as those in legal practices where information that refers to third parties is passed between a lawyer and his/her client. The lawyer has no obligation to inform the opponent about what (private) information related to that opponent is discussed with his/her client. However, when the client presents information that may harm a third party (e.g., a plan to kill), then the lawyer would be in the same position as the therapist. In this case the lawyer can disclose the information based on the thesis that it is compound private information and that it does not belong exclusively to the client. Because of this non-exclusivity factor, the level of "sensitivity" of this information is not as critical as when the disclosure is based on harm or public interest.

4 Application to Genetic Testing

Our methodology can be applied to situations where the third person is implicitly identified such as, when an HIV infected patient tells that he/she still sleeps with his/her spouse, or when a person tells of his/her violent activities towards his/her child, etc. Name, number, symbol, mark, pointing or other identifiers can identify uniquely a natural person. We will apply our previous results for breaching confidentiality in the following case summarized from Leung [19].

Andrew is diagnosed with hepatolenticular degeneration. His doctor also acts as the general practitioner for his 21-year-old brother, Martin, and his 20-year-old sister, Alison. As Wilson's disease is autosomal recessive in inheritance, both Martin and Alison have a 1 in 4 risk of having the disease. The disease is treatable in the presymptomatic stage. Although the doctor carefully explained to Andrew the importance of Martin and Alison receiving early counseling and testing, Andrew refused to inform them about his recent diagnosis. According to Leung, this case may be applied to cases of information on genes that increase susceptibility to breast cancer. A recent survey in the United States showed that over 56% of women felt that written consent should be required for immediate family to receive information on genes that increase susceptibility to breast cancer.

In discussing this case, Mariman [17] claims that breaking Doctor's duty of confidentiality would not only bring conflict with Andrew, it would also harm the position of a general practitioner since such an action would have a negative impact on relationship with other patients. In the end, it could do more harm than good. Therefore, the best decision is to respect the duty of confidentiality and take no action. Mariman advices to obtain a written statement from Andrew that can be used in the future to prove that he claimed his right of confidentiality.

Weijer [24] based on consequential position, advocates that "the physician has a duty to breach the patient's right to confidentiality if there is an imminent risk of serious and preventable harm to an identified other"[24]. The key term in such a statement is "identified other", i.e., in our terminology, proprietary private information of third party. According to Weijer, "Many will argue on these grounds that Andrew's right to confidentiality should be breached given the risks posed by Wilson's disease to his siblings and the fact that treatment may prevent this harm. I think this is the right answer, but the wrong reasons are given for it. A blind eye is turned to the dissimilarities between cases about genetic information and the Tarasoff case." We claim the same ethical position based on deontological justifications. The CP information in this case is *Andrew's disease implies, with high probability, that the Martin and Alison having the disease*. Martin and Alison have rights to such a fact because it contains their proprietary private information. It is the doctor's duty to respect such a right because he/she is no longer dealing with Martin's private information.

5 Conclusion

We have applied our definition of private information to the concept of private information confidentiality. This application is not only important by itself, but also can be useful in ethics, law, and computer science. This paper has shown that breaching of confidentiality in the case of information involving a third-party person is morally justified. In both the Tarasoff case and the genetic testing case, breaching of confidentiality can be based on the right of this third-party person to his/her proprietary private information.

References:

[1] Al-Fedaghi, S., How to Calculate the Information Privacy, *Proceedings of the Third Annual Conference on Privacy, Security and Trust*, October 12-14, 2005, St. Andrews, New Brunswick, Canada.

[2] Al-Fedaghi, S. S., Lying about Private Information: an Ethical Justification, *16th Annual Conference International Information Management Association (IIMA)*, September 22 –24, 2005, Dublin, Ireland.

[3] Stern, Edward, Tarasoff cases weight patients' confidentiality rights with society's protection needs, *MassPsy.comm*, 2001 (July). http://www.masspsy.com/columnists/stern_0107.html

[4] Olsen, Stefanie, Privacy advocates question Net access to court docs, *ZD Net*, 2001, http://zdnet.com.com/2100-11-527611.html?legacy=zdnn).

[5] Pearson, R. W., THE CONFIDENTIALITY AND EXTENDED USE OF FEDERAL STATISTICS, *Proceedings of the Survey Research Methods Section, American Statistical Association*, 1986, http://www.amstat.org/sections/srms/Proceedings/y1986.html

[6] Moore, John P., *Brady v. Hopper*, District Court of Colorado, 570 F. Supp. 1333, 1983, http://www.law.umkc.edu/faculty/projects/ftrials/hinckley/civil.htm

[7] Buckner, Fillmore and Marvin Firestone. Where the Public Peril Begins: 25 Years After TARASOFF, *The Journal of Legal Medicine*, 21: 2, 2000, pp. 187- 222. http://cyber.law.harvard.edu/torts01/syllabus/readings/buckner.html

[8] Cate, F. H. and Michael E. Staten. The Value of Information-Sharing, Copyright National Retail Federation, 2001. http://www.bbbonline.org/UnderstandingPrivacy/library/whitepapers/valueofinfosharing.pdf

[9] Cate, F. H., 1997. *Privacy in the Information Age*, Brookings Inst. Press, Washington, D. C., 1997.

[10] Chlopecki, M. The Property Rights Origins of Privacy Rights, *The Freeman*, a publication of The Foundation for Economic Education, Inc., August, 1992, Vol. 42, No. 8. www.libertyhaven.com/personalfreedomissues/freespeechorcivilliberties/privacyrights.html

[11] Chutpaitoon, N., *CONFIDENTIALITY: THE DOCTOR' S PUBLIC DUTY*, Edinburgh: University of Edinburgh, 2003. 26 p. (T E22073).

[12] Marx, G. T., Identity and Anonymity: Some Conceptual Distinctions and Issues for Research, In J. Caplan and J. Torpey, *Documenting Individual Identity*, Princeton University Press, 2001.

[13] Coleman, A., Protecting Confidential Information, In: Reed C. (Editor), *Computer Law*, 2nd Edition, (Blackstone Press, Limited, London), 1993, pp. 173-202.

[14] Edgar, S. L., Computers and Privacy. In M. E. Winston & R. D. Edelbach (Eds), *Society, ethics, and Technology*, Belmont, CA, Wadsworth, 2003, pp. 205-222.

[15] Enoch, Craig T., *Renu K. Thapar v. Lyndall Zezulka*, THE SUPREME COURT OF TEXAS, No. 97-1208, 1998. http://caselaw.lp.findlaw.com/data2/texasstatecases/sc/971208o.htm

[16] Fleming, John G. and Bruce Maximov, The Patient or His Victim: The Therapist's Dilemma, 62, *CALIFORNIA LAW REVIEW*, 1974, pp. 1025-1068.

[17] Mariman, E C M**,** Act to resolve conflict, *BMJ*, 2000 (9 December); 321.

[18] Fule, Peter and John Roddick, Detecting Privacy and Ethical Sensitivity in Data Mining Results, *Twenty-Seventh Australasian Computer Science Conference (ACSC2004)*, 2004, Dunedin, New Zealand.

[19] Leung, Wai-Ching, 2000. Results of genetic testing: when confidentiality conflicts with a duty to warn relatives, *BMJ*, 2000 (9 December); 321:1464-1466.

[20] GMC, guidance on confidentiality, 2003, http://www.gmc-uk.org/standards/default.htm

[21] Kennedy I., and Grubb, A.. *Medical law*, 3rd ed. London: Butterworths, 2000.

[22] Kling R.; Ya-ching Lee, Al Teich, Mark S. Frankel, Assessing Anonymous Communication on the Internet: Policy Deliberations, *Information Society* 15(2), 1999, pp. 71-77. http://www.indiana.edu/~tisj/readers/full-text/15-2%20kling.pdf

[23] Kottow, M. H., Medical confidentiality: an intransient and absolute obligation. *Journal of Medical Ethics*, 1986;12: 117–22.

[24] Weijer, C., Family duty is more important than rights, *BMJ*, 2000 (9 December); 321.

[25] Gerety, Tom, Redefining Privacy, Harvard Civil Rights—*Civil Liberties Law Review*, 12, no. 2, 1977, pp. 236.

[26] Acquisti, Alessandro. Security of Personal Information and Privacy: Technological Solutions and Economic Incentives. In: J. Camp and R. Lewis (eds.), *The Economics of Information Security*, Kluwer, 2004.

[27] Wacks R., *Personal information: Privacy and Law*, Oxford University Press, Oxford, 1989.

[28] Floridi, di Luciano, 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

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