PRIVACY AS A BASE FOR CONFIDENTIALITY

Sabah S. Al-Fedaghi
Computer Engineering Department
Kuwait University
sabah@eng.kuniv.edu.kw

Keywords: Confidentiality, Information, Privacy.

ABSTRACT

Privacy and information technology are inextricably tied to society's ethical and legal issues. In this paper we propose to base confidentiality of private information on the consent of all proprietors of that information. Informational privacy can be used to justify the breach of professional obligation for confidentiality in cases involving third parties, instead of relying on the *ad hoc* notion of safety, which requires determining "standards of the profession." A systematic approach to confidential private information is introduced based on defining private information in terms of assertions about its proprietors, those identifiable individuals that are referred to in the assertions. A discernment of the confidentiality of private information is developed based on the notion of transferring private information by its possessor to a third party. Of special interest in this study is the compound private information that embeds references to a third party. We claim that this type of private information "belongs" to its referents including the third party. This concept is applied in the context of the well-known *Tarasoff* case, which involves a conflict between a patient's right to confidentiality vs. the third party's right to his/her private information.

Introduction

This paper introduces a privacy-based justification for a breach of confidentiality of private information. Legal right to confidentiality can be established based on the claim of right to privacy. 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 distinction of types of private information needs a new definition of private information that will be reviewed in the next section.

Currently, technology has been accompanied by growing concerns over ethical and legal issues related to the loss of private confidential information. "Professionals in computer science, law and business point to privacy and security as the stumbling blocks of electronic commerce" (Camp et al., 2001). Confidentiality of private information is an important notion in the professional dealings of lawyers, psychiatrists, clergy, etc. Successful professional relationships depend on the client's trust in the confidentiality of his/her private information. Studies have shown that there is a positive correlation between trust in privacy practices and the willingness customers to engage in commercial activities (Swire, 2003).

We distinguish between confidentiality and secrecy. Confidentiality involves sharing of information while secrecy is a type of blocking that makes information unavailable. "Confidential" information generally refers to any information that is kept in confidence such that its revelation requires the consent of its owner. It implies protection of other people's secrets through the control of access to information and its release according to certain agreements. Financial statements, trade secrets, technical formulas, models, business plans, etc. are some types of confidential information. We shall distinguish between these types of non-private confidential information and private confidential information. Private (personal) information refers to any identifiable personal information. For example, *the treasure is buried in the park* is not private information because it involves a treasure, not a person, but it is certainly a secret. Some secrets are "private secrets" while others have nothing to do with privacy. While all private affairs (e.g., information, actions, etc.) are "personal" affairs applicable only to humans, not all secrets are 'personal'. Since, secrecy does not contradict "some level of sharing" then privacy always has the ingredient of secrecy.

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" (Acquisti., 2004). 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" (Wacks, 1989). Several types of privacy have been distinguished in literature including physical privacy and informational privacy (Clarke, 1999) (Floridi, 1998). 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 (Al-Fedaghi, 2005(a) and 2005(b)) (Al-Fedaghi et al., 2005). This definition will be briefly summarized next. An ontological definition of private information is important because it clarifies the structure of our perception regarding the notion of informational privacy, i.e., what are the entities that reflect informational privacy

and what are their categories? In this case, a private information model can be formulated as a conception of sub-concepts (of private information) and the relationship among these sub-concepts. Private information in this definition does not mean sensitive information, as in the case where personal property does not mean valuable personal property.

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*.

In this conception, linguistic assertions are limited in their possible extension to human beings. They become 'private' assertions when 'coupled' with specific individuals through the mechanism of identification. For example, The Swedish Data Act (Palme, 1998) "regards every single storage of any piece of information about a person as a personal information base. For example, if person A sends an e-mail to person B, this is a personal information base, since the persons A and B are specified. If the text mentions a third person, then the letter becomes a personal information base for that person, too."

If an assertion is true, then it is said to be information otherwise it is said to be misinformation. Consequently, there are zero information, atomic information, and compound information according to the number of referents in the underlining atomic assertion. *Atomic* information becomes *private* if it refers to identifiable individuals. Similarly, compound information becomes private if it refers to identifiable individuals.

Possession of Private Information

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 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 (Edgar, 2003). Both in the past and present, private property has facilitated means to protect individual privacy and freedom (Cate, 1997). However, even in the 19th century it was argued that, "the notion of privacy is altogether distinct from that of property" (Chlopecki, 1992),

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. A corollary to this is that every piece of atomic private information is a proprietary datum of its referent. Proprietorship of atomic private information denotes the fact that the individual is the "host" of the atomic private information. He has always the "original copy" of the information and others can only possess a copy of it. This is what makes the information "private" no matter how many copies are made and how long the chain of copying is.

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). As mentioned previously, the notion of possession may not coincide with the notion of ownership. Also, proprietorship of private information is different from the concept of copyrighting. Copyrighting refers to the right of ownership to exclude any other person from reproducing, preparing derivative works, distributing, performing, displaying, or using the work covered by copyright for a specific period of time (Lectric Law Library, 2003).

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.

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.

Atomic private information is the 'source' of privacy. Compound private information is "private" because it embeds atomic private information. Also, the concept of proprietorship is applied to compound private information, which represents "sharing of proprietorship" but not necessarily shared possession or 'knowing'. Some, or all proprietors, of compound private information may not "know" it.

Compound private information is not a collection of atomic private information; and it is not "putting-together" connection. A compound assertion is 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*, *Jim is an uncle of someone*. Additionally, we can introduce the zero-

information meta-assertion: *The three assertions form one 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. In database modeling, there are three (private information) databases of John, Mary and Jim, with one (non-private information) database that includes "pointers" that link the three private facts (Al-Fedaghi et al., 2005).

Atomic assertions are "pure" private information, while compound information is not exclusive proprietary information of the individual. The latter is shared privacy, thus its control is shared among its proprietors.

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" (Gerety, 1977). 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" (Fule and Roddick, 2004). 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), certain 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.

Additionally, "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. Consider the case of the Public Access to Court Electronic Records (Olsen, 2001), where the public is able to download and print court case files deemed to be "sensitive-but-not-confidential" by the courts. They include such information as "social security numbers, credit card numbers or medical information"; the public can also unearth personal filings such as divorce or bankruptcy cases." Privacy-rights advocates recommended that the system electronically remove such personal information from public court filings that are available online.

We will assume that the private information under consideration is sensitive private information.

Confidentiality

In this paper, we apply the definition of private information as reviewed above, to the notion of 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 (Marx, 2001). It is a form of anonymity. For example, it is common for journalists to use anonymous informants. The identities of the informants are confidential, but are known to the journalists (Kling et al., 1999). The notion of confidentiality is usually applied to private information, government secrets and trade secrets (Coleman, 1993). Confidentiality of private information implies the protection of other people's private information through controlling the access to information and its release according to certain established agreement. The confidentiality of private information is an important aspect of privacy.

Legally, the notions of unavailability to the public, 'secrecy' and/or 'sensitivity' are necessary qualifications for data to be qualified as confidential information. This unavailability to the public may be identified in terms of beliefs of the proprietor of the information with regards to: (Coleman, 1993)

(a) Sensitivity: Expectation of harm from the release (or taking advantage by others) of the information.

(b) Secrecy: Unavailability of information, i.e., not already available in the public domain.

Reasonableness of these beliefs and the usage and practices of dealing with this type of information are also taken into considerations. There are many other legal aspects of confidentiality of information as in the professional cases of information between lawyer and client, doctor and patient, etc.

Confidentiality implies controlling access to information and its release according to certain agreed on implicit or explicit agreement.

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).

Next we apply this definition to 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:

> *When a person receives CP compound information from one of its proprietors, then it is the obligation of that person to inform other proprietors who have the right to know about their private information. Furthermore, these other proprietors are implicitly participants in the confidentiality agreement, i.e., their consent is required for revealing this information. After all, a breach of confidentiality includes any unauthorized disclosure of confidential information; and "authorizing" the disclosure requires the consent of all proprietors of the compound private information.*

Application: The *Tarasoff* decision

From the Hippocratic oath onward, 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. Confidentiality of 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 as in the famous *Tarasoff* case.

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. Moore, as Poddar's Psychologist was told by Poddar 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,..." (Buckner & Firestone, 2000). 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 do 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, (Moore, 1983)).

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, (Enoch, 1998)). 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.

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, then 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 cat 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." (Stern, 2003). In our approach, the case involves the conflict between the patient's right to confidentiality vs. the third party'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 party as well. They 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 patient's family) requires the consent of this third party as much as it does 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 (Buckner & Firestone, 2000)).

Privacy and Safety

In this discussion 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" (Fleming & Maximov, 1974), (Buckner & Firestone, 2000). According to Fleming and Maximov (1974) "... 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 ..." The California supreme court asserted that confidentiality "ends where the public peril begins" (Buckner & Firestone, 2000). 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.

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 & 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" (Cate & Staten, 2001). 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 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 (Fleming & Maximov, 1974) (Buckner & Firestone, 2000). 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. Also, it 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" (Buckner & Firestone, 2000). 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" (Stern, 2003).

Privacy vs. Common Good

According to Etzioni, "rights" leaves no room for compromise (Etzioni, 1999). This characterization is taken as a rationalization to reduce the reliance on right-based justifications. He claimed that concern for privacy rights has obstructed advancing the notion

of common good, as in such actions as releasing medical and criminal records and electronic monitoring in certain situations. We show next that, in our conceptualization of information privacy, the opposite is true: concern for (informational) privacy rights advances the common good as a reason for breaching confidentiality.

Private information, as defined in this paper, has linguistic embodiment in terms of written or spoken assertions. There is a potentially infinite stock of private information about every individual. Others attach some of this information to the individual (social security number, passport number, name, etc); some information is generated by the individual him/herself (*I hate this*, *I feel this*, etc). So a logical step in analyzing the relationship between a proprietor and his/her information is to identify the "source" of this information in preparation of examining any right-based claims. Figure 1 exhibits such a relationship.

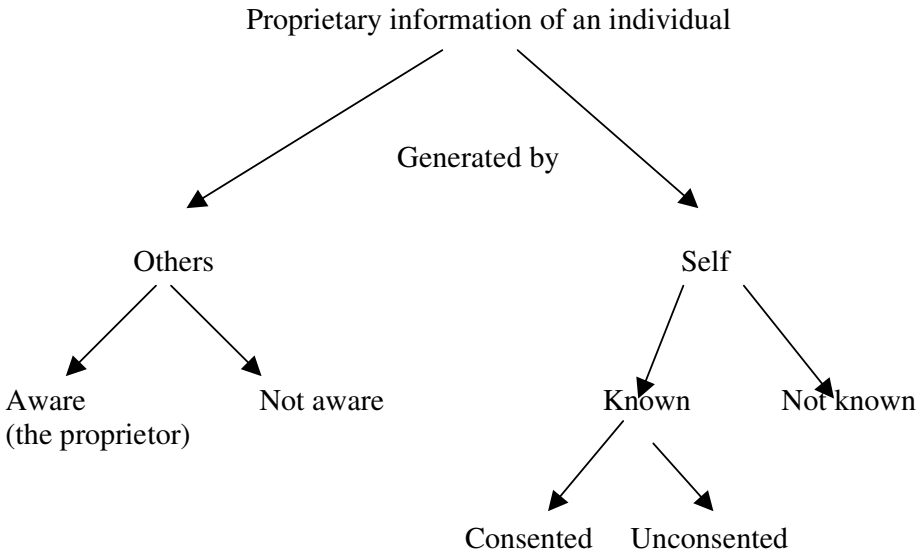

Figure 1: Taxonomy of proprietary information of an individual according to source of generation.

Information that is generated by others includes names, numbers, attributes given to the individual by others (e.g., government). He/she may or may not be aware of this proprietary information. For example, in backbiting, say, *John is greedy*; the assertion is private because it embeds the identifier John. He may or may not be aware of this backbiting by others. Also, information may be generated by the individual him/herself as exemplified by personal diaries and personal blogs. Many types of private information can be associated with different kinds of rights to do a variety of actions on private information. The following is a sample of these types and kinds of information, rights, and actions:

(1) Rights to information generated by others with the awareness of the individual: rights to block (e.g., Web site data about a visitor activity), rights to give/withhold (e-commerce), rights to correct/update (government personal records), rights to erase (commercial databases), etc.

(2) Rights to information generated by others without the awareness of the individual: rights to block (e.g., employer secret medical testing), rights to be aware (government personal records), rights not to be used to harm the proprietor, rights to be protected, etc.

(3) Rights to information generated by the proprietor and consented to others: Copyrights, rights not to be misused, rights to confidentiality, rights to be protected, etc.

(4) Rights to information generated by the proprietor and unconsented to others: rights to be done legally, rights to be protected, etc.
(5) Rights to information generated by the proprietor and not known by others: rights to diary -like information, rights to not incriminate oneself, etc.

In the Tarasoff case, the assertion *Poddar intends to kill Tarasoff* is analyzed in terms of its atomic assertions and the taxonomy of figure 1 as shown in table 1.

Poddar proprietary information *I intend to kill someone*	Tarasoff proprietary information *Tarasoff is an intended victim of murder*
Self Known Consented	Others (Poddar) Not Aware

Table 1: Analysis of the Tarasoff case according to figure 1.

Tarasoff's claim of rights to her proprietary information is justified by the fact that others generated it (in terms of linguistic embodiment) without her awareness. We may claim that this is analogous to using "part of a me-hood", to apply Floridi's terminology, such as DNA without the person's awareness. Interestingly, affirming this right strengthens advancing the common good of the public through overruling the claim of confidentially. Consequently, rights to privacy do not necessarily shield anti-social activities.

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 found a 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.

Conclusion

We have introduced in this paper a refinement of the concept of informational privacy and have applied it to an actual case. We claim that this approach leads to a systemization of the study of the relationship between the notion of privacy and other notions. Specifically, 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 exhibits the general methodology of applying privacy in several fields such as ethics, law, and computer science.

References

Al-Fedaghi, S., 2005(a). The 'Right to Let Alone' and Private Information, Proceedings of the 7th International Conference on Enterprise Information Systems, Miami (USA).

Al-Fedaghi, S., 2005(b). A Systematic Approach to Anonymity. In 3rd International Workshop on Security in Information Systems WOSIS-2005, Miami, May, 2005.

Al-Fedaghi S., Fiedler G., and and B. Thalheim B., 2005. Privacy Enhanced Information Systems, Proceedings of The 15th European-Japanese Conference on Information Modelling And Knowledge Bases: Tallinn, Estonia.

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

Amitai Etzioni, 1999. The Limits of Privacy, by Amitai Etzioni. New York: Basic Books, 1999

Boltuc, Piotr, 2003 (access date). Is There an Inherent Moral Value in the Second-Person Relationship?, in: Abbarno John (ed.), Inherent and Instrumental Value, (Rodopi Press, Takoma Park, MD, USA (in print)). http://www.uis.edu/philosophy/Document%20in%20Microsoft%20Internet%20Explorer.doc

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

Camp L. Jean, Helen Nissenbaum, and Cathleen McGrath. 2001.Trust: A Collision of Paradigms Proceedings of Financial Cryptography, Lecture Notes in Computer Science, Springer-Verlag (Berlin, Germany) Fall 2001. http://www.ljean.com/files/Trust.pdf

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

Cate, F. H., 1997. Privacy in the Information Age. (Brookings Inst. Press, Washington, D. C.

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

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

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

Edgar, S. L., 2003. Computers and privacy. In M. E. Winston & R. D. Edelbach (Eds), Society, ethics, and Technology, (Belmont, CA, Wadsworth), pp. 205-222.
Enoch, Craig T., 1998. Renu K. Thapar v. Lyndall Zezulka, THE SUPREME COURT OF TEXAS, No. 97-1208. http://caselaw.lp.findlaw.com/data2/texasstatecases/sc/971208o.htm
Fleming, John G. and Bruce Maximov, 1974. The Patient or His Victim: The Therapist's Dilemma, 62 CALIFORNIA LAW REVIEW, pp. 1025-1068.
Floridi, di Luciano, 1998. Information Ethics: On the Philosophical Foundation of Computer Ethics, ETHICOMP98 The Fourth International Conference on Ethical Issues of Information Technology, http://www.wolfson.ox.ac.uk/~floridi/ie.htm
Fule, Peter and John Roddick 2004. Detecting Privacy and Ethical Sensitivity in Data Mining Results, Twenty-Seventh Australasian Computer Science Conference (ACSC2004), Dunedin, New Zealand.
Gerety, Tom, 1977. Redefining Privacy, Harvard Civil Rights—Civil Liberties Law Review 12, no. 2: 236.
Kling R.; Ya-ching Lee, Al Teich, Mark S. Frankel, 1999. Assessing Anonymous Communication on the Internet: Policy Deliberations, Information Society 15(2), pp. 71-77. http://www.indiana.edu/~tisj/readers/full-text/15-2%20kling.pdf
Lectric Law Library's Legal Lexicon On Copyright, 2003 (access date). http://www.lectlaw.com/def/c132.htm
Marx, G. T., 2001. Identity and Anonymity: Some Conceptual Distinctions and Issues for Research, In J. Caplan and J. Torpey, Documenting Individual Identity (Princeton University Press, 2001).
Moore, John P., 1983. Brady v. Hopper, District Court of Colorado, 570 F. Supp. 1333. See also: http://www.law.umkc.edu/faculty/projects/ftrials/hinckley/civil.htm
Palme, Joseph, 1998. Critical Review of the Swedish Data Act. http://dsv.su.se/jpalme/society/data-act-analysis.html
Olsen, Stefanie, 2001. Privacy advocates question Net access to court docs, ZD Net, http://zdnet.com.com/2100-11-527611.html?legacy=zdnn).
Stern, Edward, 2001. Tarasoff cases weight patients' confidentiality rights with society's protection needs, MassPsy.comm (July). http://www.masspsy.com/columnists/stern_0107.html
Swire, Peter P., 2003. Efficient Confidentiality for Privacy, Security, and Confidential Business Information. Brookings-Wharton Papers on Financial Services, (Brookings, 2003). http://www.peterswire.net/
Wacks R., 1989. Personal information: Privacy and Law, Oxford University Press, Oxford.