Privacy as an Asset

Position Paper

Jarek Gryz
Department of Electrical Engineering
and Computer Science
York University
Canada
jarek@cs.yorku.ca

ABSTRACT

Many attempts to define privacy have been made over the last century. Early definitions and theories of privacy had little to do with the concept of information and, when they did, only in an informal sense. With the advent of information technology, the question of a precise and universally acceptable definition of privacy in this new domain became an urgent issue as legal and business problems regarding privacy started to accrue. In this paper, I propose a definition of informational privacy that is simple, yet strongly tied with the concepts of information and property. Privacy thus defined is similar to intellectual property and should receive commensurate legal protection.

KEYWORDS

Privacy, intellectual property

1 INTRODUCTION

Many attempts to define privacy have been made since the publication of the seminal paper by Warren and Brandeis [26]. With the advent of information technology, the question of precise and universally acceptable definition of privacy became an urgent issue as legal and business problems regarding privacy started accruing. The problem is compounded by the fact that the traditional concept of privacy which covered only intimate and sensitive information left out many other aspects of our life represented today in digital form. This tension has led some researchers to coin a new phrase, *informational privacy* [4], [16], [3], [18], distinct from, and to be treated differently than, the traditional object (or objects) of privacy. However, no agreement has been reached yet as to what this "new" concept of privacy is supposed to cover and what right it represents. In fact, extending privacy beyond its traditional domain muddled even further philosophical and legal discussion on the subject; as Judith Thomson observed [21, p. 286] "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is". The goal of this paper is thus modest: I will not attempt to provide yet another definition of privacy that covers *all* its aspects; I will concentrate here on informational privacy only.

The informational privacy regulation in the US has its origin in the set of recommendations, called Fair Information Practices (FIP), proposed by the US government advisory committee in 1973. There are five main principles of fair information [6]:

- There shall be no personal records systems whose existence is secret;
- Individuals have rights of access, inspection, review, and amendment to systems containing information about them;
- There must be a way for individuals to prevent the use of information about themselves gathered for one purpose for another purpose without their consent;
- Organizations and managers of systems are responsible for the damage done by the systems and for their reliability and security;
- Governments have the right to intervene in the information relationships among private parties.

The FIP doctrine is clearly outdated. As observed in [6, p. 97], its "most significant weakness (…) is its failure to specify a stronger form of the interest individuals have in their personal information. Under FIPs, individuals have only limited rights to control their personal information-rights usually limited to inspection, challenge, and review. A much stronger form of interest would be a property right rather than a mere judicial or administrative interest." The idea of treating personal information[1] as property seems very intuitive, yet it has not been widely explored. In this paper I develop this very idea: I propose a definition of privacy that is simple, yet strongly tied to the concepts of information and

[1] Roughly speaking, *personal information* is any information about me; its precise meaning will be explained in Section 3.

property. In particular, I will argue that personal information can be understood as *intellectual property* and should receive similar legal protection. This is not to say that personal information *is* intellectual property; rather it shares with it – rather unique for property – ontological status as *information.* One of the most persuasive arguments against treating personal information as property has been the imprecise use of the concept of "information ownership" in the context of privacy protection. However, the very concept of intellectual property ownership which is nothing else than "information ownership" is well understood. Moreover, the legal framework for intellectual property protection has been in place for some time now and I believe it can be used - with some necessary modifications - for privacy protection as well.

2 OWNERSHIP OF PERSONAL INFORMATION

The fact that privacy has value is indisputable. In most of the literature on privacy, however, that value is placed in the realm of ethics. It has been argued that privacy is an indispensable part of human integrity, dignity, and liberty or a necessary element of intimate social relationships. Notwithstanding ethical aspects of privacy, one cannot miss, however, an economic element of it: personal information can be traded, sold, and stolen. Privacy has an economic, often pecuniary, value [13]. Indeed, it is the economic value of privacy – although not referred to as such - that is dominant in recent discussions of privacy. We worry that by giving away too much information – or by having it stolen – we are deprived of some good that has more than just moral value. However, for any good to be sold or stolen, it must be owned by someone in the first place. This is the main thesis of the paper: personal information is best understood and should be treated as property that we *own* (the precise meaning of what I mean by ownership will be spelled out below).

The idea of using property rights in the context of privacy protection (although not as *information* ownership) has been entertained before. But all such ownership-based interpretations of privacy have been criticized for an unclear or metaphorical use of the concept of "ownership". The standard understanding of property is that it is excludable: if I own a car, you don't; if I sell it to you, you own it and I do not. With this understanding of "ownership", it is quite easy to mount convincing arguments against the ownership-based interpretations of privacy. Clearly, personal information is not lost when acquired by someone else (contrary to the standard interpretation of "ownership"). If it were, every release of personal information – to anyone and in any context – would diminish the level of our privacy. We do not perceive it that way. We do care, however, what happens with this information afterwards. If I share my marital problems with a friend, I do not expect this piece of information to go any further. Similarly, if a CCTV camera takes a picture of me walking into a bar at lunchtime I do not expect this information to reach my employer (even though the event took place in public space). In other words, if I provide someone with personal information that person or organization does not automatically acquire ownership of this information. This is different than selling or giving away any type of physical property: by selling you a car, I give up any claims to that car. Not so with personal information. Providing someone with personal information is similar (but not identical) to selling a license to intellectual property (such as software or industrial know-how). You may use this information, but you cannot – without my explicit permission – distribute this information any further.

What sort of object or commodity are we then protecting as private information? How can we provide a necessary legal protection for objects as intangible as information? I claim that personal information possesses similar properties as intellectual property and should be protected in a similar way. Intellectual property applies to noncorporeal, intellectual objects such as writings, inventions, and secret business information. Intellectual property rights usually include patents, trade secrets, copyright, trademark, industrial design rights, trade dress, etc. For our purposes, only the first three are of interest (the definitions provided below are taken almost word for word from [7]).

A *patent* is an exclusive right to use, sell, and authorize others to sell any expression or implementation of the protected work. A patent is granted for a fixed length of time but its object is publically disclosed. The subject matter of a patent - in contrast to a copyright - must be useful, novel, and nonobvious. For our purposes, the important feature of a patent is its public disclosure and ensuing dissemination of information. In return, the patent holder is granted the right to use, sell, and authorize others to sell the patented item.

A *trade secret* is any information that can be used in the operation of a business or other enterprise and that is hidden and sufficiently valuable to afford an actual or potential advantage over the competitors. An owner of a trade secret has exclusive rights to use it as long as the secret is maintained. If the secret is made public by the owner (rather than obtained via improper acquisition, e.g. a security breach) then the secret protection lapses and anyone can make use of it. From our perspective, an important aspect of a trade secret is its protection from misappropriation.

Copyright protects original works of authorship such as works of art or architecture and computer software. The domain of what can be copyrighted must be original and "non-utilitarian" otherwise it falls within the domain of patents. The principal rights that copyright protects are the rights to reproduce, distribute, and display the work publically. These rights are exclusive to the owner but can be sold or given up.

Where does private information fit within this framework? Clearly, it is a different *type* of information as it does not refer to any kind of invention, creation, or discovery. But the protection it requires appears to be quite similar to the protection we afford to intellectual property. Private information, that is, information we hide from the rest of the world seems to be closest to trade secrets. A privacy breach in this sense is as illegal as a security breach in business. On the other hand, when released to the world a trade secret loses its legal protection whereas private information does not. Once private information is sold or given away by us, it becomes public, but we should still retain control over it. Thus, it should receive protection given to patents or copyrighted work. We essentially sell a "license" to use our personal (albeit public) information but retain

exclusive property rights to it forever (this is different from patents which are granted for a fixed amount of time). In particular, a recipient of this information does not acquire by default the right to sell or distribute it any further.

3 PERSONAL INFORMATION: PRIVATE VERSUS PUBLIC

Let us be more specific about the type of protection different aspects of our personality require. Every person can be described via (possibly infinite) conjunction of attributes. The fact represented by this conjunction is not necessarily (indeed, quite unlikely) to be known by anyone. What other people know is always a subset of these attributes. People acquire this knowledge from many diverse sources but the most vivid one is their encounters with us. Such encounters can be direct - when we meet physically face to face - but they can also be via phone conversations, written correspondence, or social networks. When such encounters take place we are able – to some degree, at least - *control* the information other people receive about us. We present ourselves to them in a specific way; we show them a particular *persona*, that is, a person we want to be known as. This is not to say that other people know about us only as much as we let them know. There is much information about us that is publicly available and as long as we choose to live among other people there is nothing we can do about it (only hermits enjoy almost complete informational isolation). But we still can and do influence how we are perceived by others. Consider the following two contexts when we clearly try to influence how we present ourselves to another person: a first date and a military job interview. In the first encounter, we will try to emphasize our physical attractiveness, sensitivity, sense of humor, etc. In the second encounter, we present ourselves as disciplined, reliable, fearless, etc. Of course, these two *personas* will share a lot in common but they are sufficiently different that we would not want to swap one with another in these two situations.

When we create a *persona*, we not only decide what to include in it, but also what to exclude from it. Thus, it may not be a good strategy at the first date to release the information that our favorite hobby is hunting or – just the opposite - that we would never hurt a living creature at the military job interview. We hide this information because it may hurt the prospects for a new relationship or a job and we try to sell ourselves the best we can. The act of information concealment may have a very different moral status depending on the type of information and the context in which it happens. Consider again the first date. It is morally deplorable to hide the fact that I am already married, but it is morally neutral to avoid the subject of my snoring. On the other hand, when asked directly about either of these two facts I have the obligation to answer both questions truthfully. This distinguishes these two aspects of my *persona* from yet another one where not only I can hide the information but also have the right to refuse to reveal it. This is the category where *private* information falls into. Without trying to provide a complete definition of private information we can then say that the necessary condition for the information to be private is the social license to hide it.[2] The persona we create is a partial representation of the complete description of a person. Some of the properties are missing because they are not relevant in a particular context and some others are consciously hidden. Within the latter category, private information represents the properties that we are allowed to hide.

On the other end of the spectrum there is another (public) subset of attributes within our persona that other people may find particularly interesting or valuable. A person may sell the information represented by these attributes thus executing his right of publicity. Our legal system has recognized for at least a hundred years that "individuals have legitimate proprietary claims to their publicity interests" [17, p. 673]. In many cases, the elements of a person's public personality become valuable only after the investment of considerable time, effort, skill, and perhaps money [10, pp. 215-216]. If a person has worked to develop sufficient value in her name, then that person deserves property rights to control their resulting profitability [22]. Since the 19th century, various courts have indicated that publicity interests constitute a distinct kind of property. In 1891, the Supreme Court observed that "a man's name is his own property, and has the same right to its use and enjoyment as he has to that of any other species of property" [17, p. 677]. Since then courts have extended the scope of publicity protection beyond an individual's name to also include his nickname, likeness, a character that he created, his performance, his distinctive style, and materials closely associated with his personality.

The rationale for protecting publicity interests is similar to policy considerations that underlie copyright laws and is based on the argument that "encouragement of individual effort by personal gain is the best way to advance public welfare". Indeed, the right of publicity is in many respects similar or even equivalent in many respects to copyright. Copyright protects valuable achievements of authors, composers, and artists; similarly, the right of publicity protects a person's right in the value of his skills, craft, or talents. The main difference between the two doctrines is that for copyright protection the expression of a certain idea must be fixed in a tangible form; the interest protected in right of publicity is the person's intangible style, his persona. In fact, the boundary between copyright and right of publicity is not clearly defined which often leads to a conflict between federal policy concerning copyright (intellectual property) and state law doctrine of the right of publicity (privacy) [17].

The right of publicity is "broadly defined (…) as the right to own, protect, and profit from the commercial value of an individual's name, likeness, activities, and identity" [17, p. 677]. Normally, it is assumed that a person deserves this right because of the work and effort she put into developing her persona to be commercially valuable. But there are cases where no effort is necessary to reap rewards from one's personality: a naturally beautiful body can lead to modelling career without any time or labor expenditure. Indeed,

[2] A fixed definition of privacy is impossible as what is considered private varies widely between different cultural and social contexts.

many attributes of perfectly ordinary people are valuable enough that businesses are willing to pay for them. Our shopping habits are worth the discounts we get from supermarkets, our opinions expressed in online surveys (read: information about ourselves) are rewarded with a raffle entry. Interestingly, not long ago we would say that the information we provide to a supermarket is public; now we want it to be protected as private. (A rather cynical observation might be that people want protection for this information *because* someone finds it valuable.) The reasons for this change have been intensely discussed for a while now [11] and I am not going to engage in this discussion. The point is that the distinction between the right of publicity (derived from unique personality or style) and the standard right of privacy that protects the mundane shopping habits is disappearing. In both cases, we are protecting publically available information from being *used for profit*. We are not protecting the information from becoming public because it has always been public, but from its use that has not been authorized by us. We want *control* over this information. Now, how much of the information about ourselves do we want to protect? Clearly, any information can be misused so it is impossible to specify a priori what type of information deserves protection. But whatever this information is, the protection it should receive is similar to what a patent or copyright provide, that is, the control of its use. We show in the next section how such protection can work in practice.

4 PROTECTING PERSONAL INFORMATION

One of the most comprehensive frameworks for understanding privacy has been proposed recently by Daniel Solove in [19]. Solove shifts away from the conceptual work on the term "privacy" itself and focuses instead on different kinds of activities that impinge on privacy. The goal of the taxonomy he develops is to identify and understand various types of privacy violations that have achieved a significant degree of social recognition. Although the primary purpose of the taxonomy is to aid in the development of privacy law, it also provides an excellent testing ground for the conceptual work on privacy issues. Any viable definition of privacy should be able to account for all the cases considered in the taxonomy. This is exactly how we will test the concept of informational privacy introduced in this paper. We shall proceed by reviewing privacy violations discussed by Solove and show that whenever these cases refer to informational privacy they can be conceptualized as property right violations with respect to personal information. This information should receive protection similar to trade secrets (if I never authorized its release) or patents (otherwise).

Solove identifies four groups of potentially harmful activities (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Various entities (people, businesses, and the government) collect information about an individual. This information is then processed (stored, combined, manipulated, etc.) and possibly disseminated (released to the public or transferred to others). Invasions involve impingements directly on the individual and do not necessarily involve information.

Information collection includes *surveillance* and *interrogation*. Surveillance by means of visual or audio eavesdropping is likely the oldest type of privacy violation and has been widely recognized and criminalized as such. According to our concept of privacy surveillance is simply theft of private information similar to theft of trade secrets. When someone wiretaps my phone and listens to my calls he acquires information that I consider private and since does it without my consent he steals it. Our theory explains in a straightforward way two borderline or disputable cases of surveillance: surveillance in public and covert surveillance (this is the case when I never find out that I have been observed and the information thus acquired is never used in any way). The first case – when surveillance is done in public places – has usually been dismissed by courts as privacy violation [2], [24]. Indeed, since the information gathered in public surveillance is openly displayed, no privacy violation takes place according to our theory either. On the other hand, covert surveillance with no damage to the observed subject (for example, when all surveillance tapes are destroyed) still represents - according to most scholars - a privacy violation. When reinterpreted in our theory, this is the case of misappropriation of trade secrets.

Interrogation "is the pressuring of individuals to divulge information" [19, p. 500]. The harm elicited through interrogation arises from the degree of coerciveness involved. If a neighbor asks me about my marital problems and I respond out of politeness, I would consider this an invasion of privacy but a minor one. If a potential employer asks me about my mental health problems and my future employment hinges on the answer (or the refusal to provide one), this is serious privacy offence. If one thinks of information as property, then an attempt at obtaining that property through coercion is a case of extortion. Again, our theory correctly identifies it as privacy violation.

Privacy violations that may happen during information processing, the second category in Solove's taxonomy, include *aggregation, identification, insecurity, secondary use, and exclusion*. In all these cases private information has been already provided by an individual, but his right to *exclusive ownership* of this information has been compromised. In aggregation, information from different sources is combined – without its owner's permission and often also without his knowledge – into a relatively complete profile of a person. Consider again an analogy with intellectual property. Apple holds a number of patents for iPhone and may sell licenses covered by these patents individually to different companies. However, Apple would never – presumably – agree to sell these licenses to a single company or allow them to be consolidated in a single product as it would grant a license to build a legal replica of an iPhone.

Identification is a special case of aggregation when one piece of aggregated information contains the identity of a person. It represents privacy violation because personal information is revealed by its owner under the condition that it will remain anonymous, that is, more information is released than authorized by its owners. Insecurity covers the typical cases of ill-protection or mishandling of personal information through computer glitches, security lapses, abuses and illicit use. When we release personal information, we lease – under our theory - our property and expect

that it will be handled and protected properly. Secondary use is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent. Again, this type of privacy violation is an infringement of the exclusivity aspect of information ownership. Lastly, exclusion refers to failure to provide individuals with notice and input about their records. Federal privacy statuses guard against exclusion by mandating transparency and granting individuals the right to access their information. If we understand the right to privacy as the exclusive right to one's property then giving out the information to institutions or businesses (which is equivalent to leasing it) does not give them right to hide this information from us or restrict our access to it.

The third group of privacy violations includes *breach of confidentiality*, *disclosure*, *exposure*, *increased accessibility*, *blackmail*, *appropriation*, and *distortion*. Breach of confidentiality, disclosure, and exposure cover various aspects of disclosing personal information beyond the intentions of its subject and are similar to the case of *secondary use* discussed above. Blackmail may involve other threats than just releasing personal information so it is only marginally related to the issue of privacy protection. Indeed, many cases of blackmail involve the threat of revealing not private, but public information which just happens not to be widely known.

Increased accessibility does not involve direct disclosure. Rather, information that is already available to the public is made easier to access. The classical case is online publication of court records which are already publically available in paper form in court archives. Legal response to such cases is not uniform. Some courts find increased public disclosure harmless [25] whereas some others recognized the problem [23]. The likely source of this tension is the vagueness of the boundary between private and public domain. Indeed, the predicate "private" is a ternary relation with one of the arguments being the recipient of the information. The more people have access to information about me, the larger scope of this information I consider private and would like to hide from them. My car's registration number is public information for all my neighbors, but not for the users of Google Street View anywhere in the world.

One of the first cases categorized under the rubric of privacy violation involved a flour company using a picture of a minor without her consent [15]. This was the case of appropriation: the use of one's identity or personality for the purposes and goals of another. Appropriation involves the way an individual desires to present herself to society. Interestingly, courts have not been able to adequately explain the injury inflicted by appropriation and most contemporary cases tend to recognize that the tort of appropriation protects a "valuable right of property" [1, p. 375]. In fact, courts have transformed the targeted harm from one of appropriation to one of intellectual property which agrees quite well our view of privacy.

The last category of privacy violation in the third group involves distortion: the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public. Although distortion has been categorized by Prosser as one of the four major privacy torts [14], it often does not involve the use of personal information. False and defamatory statements can be made about *any* aspect of the person, including facts available to the public. When the distorted information is personal in nature our theory would classify it as misuse of private property. A publisher of an e-book would likely take legal action against anyone who modifies that e-book and claims that it is the original product of that publisher.

The last group in Solove's taxonomy, invasion, covers two cases: *intrusion* and *decisional interference*. Intrusion is defined here as invasion or incursion into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy. Although related to informational privacy, intrusions are clearly violations of physical or psychological privacy. Decisional interference – government's interference with people's decisions regarding certain matters of their lives – primarily concerns harms to autonomy and liberty, not to privacy [5]. Solove's decision to include decisional interference among privacy harms has to with a strong causal relation that it may have to actual privacy violations. Thus, neither intrusion nor decisional interference represents a direct violation of informational privacy.

5 CONCLUSIONS

Once we agree to treat private information as property, it can be sold, bought, and traded as any other property. Indeed, one can imagine creating an exchange market solely for the purpose of privacy trading. The idea of National Information Market (NIM), where information about individuals can be bought and sold at a market price has been proposed several years ago in [6]. Institutions gathering information about individuals would be allowed to sell baskets of information to other institutions willing to pay for it. Individuals would collect fees for the use of their private information similar to the system of copyright law established in the music industry whereby individual artists can collect fees based on use of their music.

Although Laudon's idea of NIM has been largely – and unfairly, I think – ignored, the idea of privacy as a commodity can be quite illuminating. If private information has monetary value, it can be quantified. We do not need to go as far as to attach a particular price to a piece of private information. But as long as we agree that one piece of private information is more valuable than another piece or that this piece is more valuable to one individual than to the other, we can then design different levels of protection of these pieces. One of the most spectacular failures of information technology in recent years was the assumption that anonymity guarantees privacy. The idea of anonymization, that is, removing personal identifiers from data, was intended to provide *complete* privacy protection for individuals. Numerous experiments and case studies showed convincingly that anonymized records can be very often re-identified with the use of publically available auxiliary information [20] [12] [8] [9]. Instead of complete privacy, we have no privacy at all. But we do not have to think of privacy in terms of these two extremes. Clearly, there is middle ground where *some* of the private

information can be released to *some* people. One may agree to release one's medical records only to research institutions, but even then without information about one's sexual orientation. Only when we treat privacy as a quantifiable object, can we assign different levels of protection to its different parts.

The legal and philosophical aspects of privacy have been discussed for over a hundred years now. But the more recent technological challenges of protecting digital data seem unprecedented compared to threats to privacy of the past. The technical issues relating to privacy protection clearly affect the discussions about the definition of privacy at the conceptual level. What are the levels of data protection for personal information? What and from whom can we hide? How do we measure the cost of personal information that has been lost or stolen? What is the cost of data protection? These questions can be answered when – perhaps *only* when - we treat personal information as property and the right to privacy as a property right. This is not to say that this is the *only* way we should think of privacy, but I conjecture it may be useful in designing ways of protecting privacy in its other aspects as well.

References

[1] D. A. Elder, The Law of Privacy, 1991.

[2] *Florida v. Riley,* 1989.

[3] L. Floridi, "The Ontological Interpretation of Informational Privacy," *Ethics and Information Technology,* vol. 7, pp. 185-200, 2005.

[4] C. Gould, "Network Ethics: Access, Consent, and The Informed Community," in *The Information Web: Ethical and Social Implications of Computer Networking*, Boulder, Westview Press, 1989, pp. 1-35.

[5] L. Henkin, "Privacy and Autonomy," *Columbia Law Review,* vol. 74, p. 1410, 1974.

[6] K. C. Laudon, "Markets and Privacy," *Commun. ACM,* vol. 39, no. 9, pp. 92-104, 1996.

[7] A. Moore, Intellectual Property: Moral, Legal, and International Dilemmas, Rowman & Littlefield Publishers, Inc., 1997.

[8] A. Narayanan and V. Shmatikov, "Robust De-Anonymization of Large Sparse Datasets," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2008.

[9] A. Narayanan and V. Shmatikow, "De-anonymizing Social Networks," in *IEEE Symposium on Security and Privacy*, Oakland, CA, 2009.

[10] M. Nimmer, "The Right of Publicity," *Law and Contemporary Problems,* vol. 19, pp. 203-223, 1954.

[11] H. Nissenbaum, "Protecting Privacy in an Information Age: the Problem of Privacy in Public," *Law and Philosophy,* vol. 17, pp. 559-596, 1998.

[12] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review,* vol. 57, pp. 1701-1777, 2010.

[13] R. Posner, "An Economic Theory of Privacy," in *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press., 1984, pp. 333-345.

[14] W. L. Prosser, "Privacy," *Cal. L. Rev.,* vol. 48, 1960.

[15] *Roberson v. Rochester Folding Box Co.,* 1902.

[16] M. Scanlan, "Informational Privacy and Moral Values," *Ethics and Information Technology,* pp. 3-12, 2001.

[17] D. E. Shipley, "Publicity never dies; it just fades away: the right of publicity and federal preemption," *Cornell Law Review,* vol. 66, pp. 673-737, 1981.

[18] D. W. Shoemaker, "Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity," *Ethics and Information Technology,* pp. 3-15, 2010.

[19] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review,* vol. 154, no. 3, pp. 477-560, 2006.

[20] L. Sweeney, "Uniqueness of Simple Demographics in the US Population," Laboratory for International Data Privacy, Working Paper LIDAP-WP4, 2000.

[21] J. Thomson, "The Right to Privacy," *Philosophy and Public Affairs,* vol. 4, pp. 295-314, 1975.

[22] J. Treece, "Commercial Exploitation of Names, Likeness, and Personal Histories," *Texas Law Review,* vol. 51, no. 4, pp. 637-672, 1973.

[23] *United States Department of Justice v. Reporters Committee for Freedom of Press,* 1989.

[24] *United States v. Knotts,* 1983.

[25] *Walls v. City of Petersburg,* 1990.

[26] S. Warren and L. Brandeis, "The Right to Privacy," *Harvard Law Review,* vol. 4, pp. 193-220, 1890.