Law and Humanities Quarterly Reviews

Silva, J. T. S. (2023). A Comparative View and Brief Analysis at the New Right to be Forgotten: The European And American Privacy Law. *Law and Humanities Quarterly Reviews*, 2(2), 25-41.

ISSN 2827-9735

DOI: 10.31014/aior.1996.02.02.57

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research Law and Humanities Quarterly Reviews is a peer-reviewed International Journal of the Asian Institute of Research. The journal covers scholarly articles in the interdisciplinary fields of law and humanities, including constitutional and administrative law, criminal law, civil law, international law, linguistics, history, literature, performing art, philosophy, religion, visual arts, anthropology, culture, and ethics studies. The Law and Humanities Quarterly Reviews is an Open Access Journal that can be accessed and downloaded online for free. Thus, ensuring high visibility and increase of citations for all research articles published. The journal aims to facilitate scholarly work on recent theoretical and practical aspects of law.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Law and Humanities Quarterly Reviews
Vol.2, No.2, 2023: 25-41
ISSN 2827-9735

DOI: 10.31014/aior.1996.02.02.57

A Comparative View and Brief Analysis at the New Right to be Forgotten: The European And American Privacy Law

Julieth Tatiana Salgado Silva[1]

[1] School of Law, The University of Melbourne, Melbourne, Australia

Correspondence: Julieth Tatiana Salgado Silva, E-mail: tatianasalgadosilva@gmail.com

Abstract
The purpose of this research is to make an analysis of the moment when the privacy of an individual became a sensitive element which could be internationally protected and limited to public accessing. The research tends to start by showing the current perspective of the privacy understandings, based on sounded cases of celebrities which allowed Courts to make and establish positions to direct the treatment of the privacy right; after, it seeks to make an overview of the scenario when privacy is highly controversial: internet and social networks. Then, the study of the European and United States legislations in the subject will open the door to bring the analysis of the new right to be forgotten and how this new concept is being treated and has developed in the last years.

Keywords: Privacy, Privacy Law, Privacy Right, Social Media

1. Introduction

A photo of Clarence W. Arrington appears on the front page of the New York Times magazine in an article entitled "*The Black Middle Class: Making It*." (Arrington v. New York Times Co., 1982). Across the Atlantic, in the UK, the famous model Naomi Campbell was photographed leaving a rehabilitation clinic for drugs consumers (Campbell v. MGN Ltd., 2004). Those two pictures published without the permission of the photographed: Arrington, a stranger; Campbell, a lavish and famous model. To the demands of both against newspapers and photographers privacy breaches, the US Court (New York) in Arrington rejected the existence of any rights against the New York Times, while the European Court in Campbell ordered the defendants to pay compensatory remuneration for the violation of the privacy of the model.

The list could go on and on to be endless: Princess Caroline of Monaco is photographed with their children without their consent (Von Hannover v. Germany, 2004); president of the International Automobile Federation is slandered by a British newspaper which provided a hidden camera to a prostitute to take pictures during sadomasochistic sex acts with supposed Nazis issues or Lorena McKennitt, a famous Canadian singer, is threatened by the publication of a book about his private affairs written by an old friend and employee, as stated in court case McKennitt v. Ash (2007).

Cases like this happen all over the world and because of them, the courts have reacted in dissimilar ways. Such reactions are often the product of the notions of privacy that the legal system has accepted.

Conversely, and not far away from an imminent proposal, people tagged want to recover their lives after harmful publications regarding their past acts; this arguing their rights to continue in a normal way of living and, in concrete, their *right to be forgotten*, as extracted and mentioned for the first time in the *Google Case* (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos. 2014).

2. The Problem: privacy, internet and social networks

Arrington and Campbell cases, expressed the adoption of two cornerstone models and systems of protection of the right to privacy.

Arrington

In what apparently could be understood as an association praising the published history and Arrington figure, it proved to be an insult to the statements in the article and baseless implicit connections between the visions of the young man and those expressed in the text. Mr. Arrington did not consent to publish that photo (1982), much less in a national magazine. The photo was taken by a photographer linked to the newspaper and presented Arrington as an example of the expansion of professional black middle class in American society. The author of the article concluded that "this group has been growing much more uprooted from their less fortunate compatriots" (1982).

By contrast, Arrington, a young financial analyst who began his career at General Motors at first and then at the Ford Foundation, understood the text not only as controversial, but as expressing ideas that he did not share. He and the readers who read the article found "insulting, degrading, distorting and reprehensible" (1982). The facts indicated that this article meant to Arrington that society associate him with ideas that were not his and insinuated that he had changed his way of thinking, thus betraying his "social class" (1982). Some theories that Arrington brandished in his claiming were: i) Arguments based on violations of New York state statutes for the protection of civil rights; ii) Arguments based on violations of the common right to privacy, and iii) Violations of the constitutional right to privacy.
The three were rejected. In interpreting the Statute the Court decided that "a photograph published in a newspaper and associated to a public interest article is not considered a" commercial use "or for purposes of marketing and / or advertising, as if the statute forbids" as stated by The Court (Murray v. New York Magazine Co., 1971).

The Court mentioned that the claim pursued by Arrington will not succeed (1982), being the only exceptions that this photograph had no actual connection with what has been published, or that the article and the photograph were a commercial disguised promotion. These exceptions were not present in the case, as the relationship between the published text, the photo and Arrington undoubtedly existed.

The Court also decided that there was no support in the judicial precedent for finding a violation of the common right to privacy and, finally, that there was no state action or a violation by the State or any of the organizations, institutions or state entities, as the New York Times is a private newspaper.

Campbell

In Europe, the well-known Naomi Campbell rejected more than once the overture of been dealing with addiction to drugs. Campbell was photographed coming out of rehab and pictures were published in a newspaper run by MGN Limited. In this case the model demanded monetary compensation to the English courts, receiving a favourable decision. Under the doctrine of breaking confidences and Article 8 of the European Convention on Human Rights, which protects the right to privacy and family life, Campbell argued that disclosure of the location of the meetings of drug addicts was a violation of privacy and that the published photographs exposing this private information (Campbell v. MGN Ltd., 2004).

In these two cases there can be interpreted two points on which rotate the notions of privacy. The first is the notion of control and the second the notion of privacy as the right to the private life or the dignity, according to Levin Avner & Sanchez Abril Patricia. (2009).

2.1 Notions of privacy on the internet

There is not a unique definition of privacy. Certainly, the concept reflects the relationships among members of society and between governments and individuals. Different companies adopt a notion of another, and that notion informs the public about policies, legislation, and even academic discourse.

The two prevalent notions, as evidenced by modern Western laws and legal discourse, are those mentioned above: Privacy understood as control and privacy and dignity. American jurisprudence grants a position to the notion of privacy as control over personal information and therefore the autonomy to decide with whom to share it. By contrast, European courts take the notion of privacy as dignity, that is, as a human right to privacy, a right and substantive value of first order.

2.1.1 Privacy as control of the personal information and freedom

This notion represents individual freedom to control personal information. In other words, it is the freedom to choose who has access to such information. Two of the manifestations of this notion are the Fair Information Practices (FIPs) and the tort of liability of American common law for public disclosure of private facts. The first practice provides the individual control over information that is disclosed. In turn, the individual has the necessary information about data collection mechanisms that are implemented, which means that this individual takes many more responsible and informed decisions about whether or not disclose such information.

The aim is for the individual to make an informed and knowledgeable decision when it comes to disclose your information. Also, fair information practices provide the subject of control over their data: from the supply thereof, the monitoring on the use, disclosure and retention of such personal information. Protection systems based on the FIPs distinguish between information collected by an organization because the same individual provided it, and the information collected or provided by third parties. The control of information, not surprisingly, is evident in its fullness when the information is provided by the individual directly.

- As freedom

In "The Two Western Cultures of Privacy: Dignity Versus Liberty," James Q. Whitman (2004) has curious questions: Why do French people evade talking about their salaries, however, they do take off their bikini’s top? Why Americans undergo extensive credit reports without rebelling themselves? The author agrees with the two notions outlined above and argues that privacy is understood by Americans, essentially, as the freedom to decline government interference in their private sphere. He continues mentioning that this freedom is expressed with high intensity, for example, in protecting the sanctity of the home against governmental actors 18 and attenuated in the field of media invasions.

2.1.2 Privacy as dignity

This is the prevailing notion in Europe. Notable academics, lawyers and American philosophers have addressed this notion of privacy and dignity, although the country's laws do not reflect it. This is the aspect of privacy defending by Samuel Warren and Louis Brandeis in their article on the Harvard Law Review (1890). Threatened by "the intensity and complexity of life" and "the recent discoveries and methods of conducting business”, these authors noted that “seclusion and privacy have become indispensable for the individual”. Also, they said that it was imperative for the law to protect privacy under the principle of "inviolability of personality". All private

interests share a value: respect for individual dignity, integrity and independence. The moral personality of someone defines the essence as a human being. A violation of privacy leaves the person at the mercy of the complaint and the public scrutiny. This nudity to the outside world, gives people and their sense of self vulnerability in an offensive way to their human dignity.

A look to the privacy focusing on the aspect of human dignity inevitably involves the reflection of personality development *per se* and the "inner me". From this point of view, privacy involves the right to keep certain aspects of private life away from others and, therefore, the right to build different "situational personalities." In doing so, the individual discloses aspects of their privacy in different environments and in different contexts. The biggest risk is the lack of ability to freely manage which private information was disclosed and in what context, which leads to catastrophic social consequences.

Originally developed this notion in France and Germany, the right to protection of privacy proposes the creation and maintenance of a personal identity, intimacy, and a community. Thus, European countries follow one way or another this notion focused on the protection of human dignity and, consequently, see it as an inherent right of personality.

The supreme legislative consecration of that notion appears collected in the European Convention on Human Rights, Article 8.1. This article presents under the protection of the right to respect for private and family life that: *"Everyone has the right to respect for his private and family life, his home and his correspondence"* (1950).

2.1.3 Privacy in the internet and social networks

How these ideas are manifested in the internet networks? The article *"Two Notions of Privacy Online*" (2009), Professor Sánchez Abril from the Miami University, USA, and Professor Levin from Ryerson University, Canada, conducted studies on the protection of personal information and expectations of Privacy on Social Networks (OSN-Online Social Networks). The study aimed to investigate how to explain that users of social networks tended to disclose such personal information and still retain somehow any expectation of privacy. How do users of these websites define their expectations of privacy? Is this always an unreasonable expectation? These were the two key areas of a socio-legal research.

The researchers of this global project interviewed approximately 2,500 young people who use the Internet. Ages ranged between 18 and 24 years old. The theoretical assumption of this research effort were the two dominant and competing notions of privacy on the Internet: the idea of privacy as a control and the idea of privacy as dignity.

Until the date of publication of the article, the idea of privacy as a control was predominant. The article focused on an analysis of two leading social networks in the internet market (Facebook and MySpace), and concluded that these networks propel a notion of privacy and user control over it.

However, social networks present a unique challenge in modern times: extreme control on privacy does not prevent Internet users, in an effort to socialize, disseminating personal information to third parties users or no-users that can be catalogued as unwanted, defamatory and many times available to any undetermined number of participants. Many of those participants disclose information without caring, apparently, of losing control over it. Nevertheless, there are well known reactions of indignation when personal information is disclosed, used, or accessed by unauthorized users belonging to another network or simply individuals outside this.

The article, therefore, presented an idea of privacy in social cyberspace that states the following: participants in social networking sites have a legitimate expectation of privacy online, the privacy that network provides itself and the one that is expected from the network. This notion projects the two symbolic aspects that have been discussed academically and practically understood to privacy: the sphere of control and of dignity. According to this notion raised by Abril and Levin, the information is considered by the participants in social networks as "private" as it will not be disclosed outside the network in which it was initially released, if it was originated from

or within they; or if the information does not affect the character of the Internet user, if the same one was originated by others.

2.2 The new manifestation of privacy rights in the digital environment: the right to be forgotten in Europe

In this sense and with the statements just made, it will be a step opening-not a new notion of privacy-but rather a retrospective right to select and organize those personal data likely to undermine the pure personal rights: honour, privacy and image. But, how and why to establish that right? Troncoso admits society does not understand what happens when everything is available, ready to be known and stored indefinitely. (Troncoso Reigada, Antonio, 2012).

It is highly possible that has already passed the time when we all had absolute power of control over our intimacy; it is probably that one of the side effects of the trivialization of the information published on the Web is one unpardonable loss of privacy that has not ceased to belong to us only in part, but when we want to recover -that probably, be already recorded in indelible ink on any computer over the world: with these parameters, can we expect a right to forget or to be forgotten (right to oblivion, as well) by making a selective deletion of some of the online information that has been submitted and is detrimental for us?

On the 28th of February, 2012, it was opened by the Vatican, Roman Capitoline Museum, an exhibition that, under the interesting name of Lux in Arcana, - Light on the Mystery-, sought to leave at the general view declassified documents from the Vatican Secret Archives which had been and remained hidden or secret for centuries, so far away from information, curiosity and, what is worse, to popular culture; In summary, hidden from the freedom of opinion and information, as Weber comments (Weber, Rolf H., 2011, pp 120-130). It is clear what are the dangers that lurk under the decision, usually arbitrary, to determine what information is accessible and what information has to evade to the healthy or unhealthy interests from other people. It is therefore not easy, from a dogmatic point of view, and not easy from a legislative point of view, to shape a so sensitive profiles right and limits.

Special mention needs to be done regarding the processing of personal data which are of historical interest. In this case, similar to what happens when there are other legitimate reasons such as information finalities or the cited public access sources, the right to be forgotten in the internet media can easily decay, because the data of historical and cultural character must be preserved in the way as the objective to be achieved with its conservation and management does not expire or lose intensity by the simple passing of time.

The study in comparative perspective can be of special interest on this last point. In Italy, the *Garante per la protezioni dei dati personali* approved a code of conduct that sets rules and limits on the use of personal data collected in independent historical research and the right to education and information. Therefore, it is warranted that access to documents and files is respected in light of people's dignity and specially the right to personal identity. And, also, it states that the collection of data archives for historical research should be encouraged and treated as a valid form of data retention given the operating profit of them. In a specific legislative context, the Spanish one for instance, such provision provides legal security and, given that the legal system lacks a code of conduct similar, is not insignificant to note here the benefits of it and the more desirable future action of the Spanish authorities to protect data in a similar way, comments Simón Castellano (Simón Castellano, Pere, 2011).

What is undeniable is that this right has entered into force, at least in Europe. It suffices to go to a very recent article made by Jef Ausloos (2012) to draw conclusions in this regard. Meanwhile, its definition in the European legal texts themselves: "The right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes". This is undoubtedly a broad and vague concept, but a good start (at least to define it). The limitations or, in the words of the article, the disadvantages arising from own eventual regulation of the right to be forgotten, can be condensed into the following sections:

a. *Limited Scope*. In the sense that it gives the feeling that the limited scope of the right to be forgotten has to be disturbed by a previous "contractual" relationship, that is, in which the affected has previously consented (this is

not always the case and, as an example, there are cases where the interest of the affected- as happened in Spain- to delete the information displayed online is derived from information appearing in the search tools that had been pardoned by the government after it had served part of the penalty imposed). As Ausloos says, the concept is not adequate to address privacy issues in which the data is obtained legally without the consent of the person. It is also important to remember that the law only provides a solution subsequent to privacy issues.

b. *Anonymized Data*. That is, the individual cannot claim the data separation or selection in regards anonymous information. It does not exist or is not known who could be asserted against this law. The reason for this argument is subtle: the counterweight of anonymity of information posted on the Internet is the lack of credibility.

c. *Subtle Censorship*. It is also one of the most sounded arguments against the establishment of the right to be forgotten: to enable people to eliminate the data that affect them, relevant information can be incomplete, inaccessible or wrongly representative of reality. That is, as we shall see in detail, the establishment of this right could pose an insurmountable friction with the freedoms of expression and information. In short, it could open a door to other forms of censorship.

d. *Practical Difficulties*. It can be analysed and possible explained just with a question: how do we proceed to eliminate harmful data (and only these) for people who are in ubiquitous and opaque multi-platform?

e. *The Illusion of Choice*. It is, perhaps, a "fantasy" or an illusion. The "right to be forgotten" is certainly insufficient to address privacy issues in the internet network. The introduction of a "right to be forgotten" only postpones the illusion of choice. Additionally, it may aggravate the situation of the individual and offers a wildcard for more privacy intrusive applications. They might be created a certain degrees of frustration at not seen made a right that has been granted.

3. The legal nature of the right to privacy in the United States

The term "privacy" in the United States attracts a wide range of legal doctrines, philosophical and political debates. Thus, the American right to privacy has found its manifestation in dissimilar legal institutions, including constitutional rights, laws or special statutes, and own actions of common law.

The United States Constitution enumerates through a system of *numerus clausus* rights and powers of the federal government. Many of the civil rights guaranteed to Americans are established in the first 10 amendments to the Constitution, which is known as the Bill of Rights. Interestingly, the word "privacy" does not appear in the Constitution or in the Bill of Rights. It was the Supreme Court which found that both the Charter of Rights and the Fourteenth Amendment of it, protect the right to privacy related to freedom of association, physical integrity, and individual decisions about education, life family and sexuality.

In this line of thinking, the development of American constitutional right to privacy has focused on understanding it as a right to physical, information, decide freely, to property and freedom of association. As it is right and at the same time constitutional warranty, privacy can also be described as the right of individuals against government interference in their private lives.

The legal framework in which the right to privacy was generated started from the interpretation of freedom as a fundamental value in American society. That is why privacy and freedom are intertwined terms yet come alive. Some examples of the various types of legal and social problems described under the umbrella of privacy in the United States are: laws governing the right to refuse care, or the unlawful registration of a personal residence (right to physical privacy -spatial), the right to monitor computers in the workplace (data privacy), the right of same-sex couples to choose marriage (privacy option-selection), and the right to include or exclude third parties (privacy of association). Despite the literal absence of the term "privacy" in the Constitution, certain rights to privacy are doctrine established through judicial precedent.

The privatizing dimension of the right to privacy is reflected in the reaction of the American civil system to attack this right from an individual's hands. This reaction involves the granting of compensatory actions with non-contract binding, for instance, common law private actions aimed at protecting the privacy of the individual concerned. As stated in Court, perhaps for the constitutional silence and the many aspects that are generated, the US rightfully been difficult to define the right to privacy. (Griswold v. Connecticut,1965, pp 479- 509).

While some legal theorists as Allen (Allen, Anita, 1988) define privacy as a function of accessibility to the person others like Fried (Fried, Charles, 1968, pp. 475-482) have defined it in terms of control over information or in the case of Solove (Solove, Daniel J., 2002, pp.1087-1094 as the person and its privacy.

Despite so many contradictory formulations, the most accepted interpretation in American law is privacy as "the right to be let alone," translated as the individual's right to be left in peace, tranquillity and solitude, the way how Cooley mentions (Cooley Thomas, McIntyre, 1888). Thus, privacy tends to be formed to protect the autonomy of individuals against interference above anything else.

American legal philosophers, since ancient times, have conceived autonomy as the central value of privacy. In the words of Stanley Benn (1971), philosopher and theorist of law, the individual is both a product and a promoter to choose his being. Their decision to keep certain things private and do other public is fundamental for the development of their identity as an autonomous person who freely elects their own projects in life. Professor Richard Parker (1974, p 281) described privacy as the control over when and by whom the various facets of our lives can be perceived by others. The legal philosopher Alan Westin (1968, pp 166-170) described it as all these actions of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Some philosophers have confronted this approach of autonomy with central values in other jurisdictions. For example, the continental European model of privacy protection values individual dignity above all and this value, in practice, means that individual dignity is equally balanced against freedom of expression. By contrast, in the United States, freedom of expression, also based on the autonomy, overrides individual privacy needs, resulting some power from freedom of expression versus privacy.

3.1 Approach and history

Since the late nineteenth century, the concept of privacy is progressively took over the American consciousness. Historians have attributed that awakening to the increase in the density of population in cities, the number of literate population and dissemination of information. All these factors contributed to a social approach to privacy and the inevitable question of how the law might respond to it.

Privacy as a civil action was introduced for the first time in American jurisprudence in 1890 with the academic article "The Right to Privacy" by Samuel Warren and Louis Brandeis (1980), published in the Harvard Law Review. Warren, from a prominent family in the society of Boston, and Brandeis (1980), who would become a renowned judge of the Supreme Court of the United States, were at that time partners in the practice of law. According to the legal legend, Warren proposed Brandeis write the first article on privacy in the United States after the Boston Press published intrusive facts about the wedding of his daughter.

This highly persuasive essay, promoted the creation of a new civil law to protect the personal space of the individual against unauthorized disclosure to the public. The article began with a detailed statement of the contemporary state of privacy law in the late nineteenth century. In those years, the American press embraced what later became known as "yellow press", these marked by sensationalism and gossiping. This press, according to the authors, was "surpassing in every direction the obvious bounds of propriety and decency".

Warren and Brandeis also blamed the technology for providing such intrusions into private life. For the authors, the new mechanical instruments like the camera "threatened to bless the prediction that what is whispered in the

privacy is trumpeted from the rooftops". The authors concluded with a novel suggestion: the creation of a new action liability to protect the "sacred confines of private and domestic life".

Seventy years after Warren and Brandeis established the conceptual framework of this action arising from liability, William Prosser (1960, pp 383-389) cemented his place in American jurisprudence. Prosser wrote another very influential article where he categorized and coined the right to privacy in four different aspects of liability. Two of these actions are related to the dignity, invasion of privacy by intrusion and public disclosure of private facts. The other two actions are closely related to the publication and property rights: "false light privacy" and invasion of privacy by appropriation. These four classifications of Prosser are presently incorporated in the *Restatement (Second) of Torts*, published in 1977, an official compilation that brings together the state of the US liability laws and forms the legal foundation on privacy in many American states, as Keeton informs (Keeton, W. Page, 1984).

The jurisprudence in this area has not been homogeneous. Several states have rejected the implementation of the four actions and the relative paucity of legal precedent in this area suggests that demands for violation of privacy rarely go to trial. This, because a claim for public disclosure usually requires the introduction of embarrassments facts in the public media and the admission of the truth of these facts, it is likely that the increased risk of exposing to light the same facts has deferred to potential applicants.

A product liability case product of an action for violation of privacy, like any other civil case, requires enough substantial damage to warrant demand given the legal costs of the process. It also requires translating the damage to dignity in a quantifiable compensation, which is not impossible but, is an arduous exercise. MCClurg (MCClurg, Andrew J.,1995, pp 1000-1001) insists that it is for this reason that the actions for breaches of privacy are often rejected prematurely, resulting in perhaps the Courts often do not know these cases.

3.2 Four categories of invasion of privacy

The four civil actions for violation of privacy recognized in US law are, as mentioned before, intrusion upon seclusion (private sphere), the appropriation, the false light privacy and publicity given to private life. Each one of these actions covers the legal treatment to detriments related to privacy.

3.2.1 Intrusion upon seclusion

Civil liability for intrusion or invasion into seclusion bring together data collection practices. It requires the plaintiff to show that the defendant (a) intentionally interfered, physically or in different way, (b) in seclusion or solitude of another or in their private affairs or problems, (c) in a manner highly offensive to a reasonable person. This civil action applies to situations where information is discovered in a furtive manner in a private place. This action gives the injured party the right to recover monetary damages (compensation) for invasion into seclusion and solitude. The action clearly includes non-physical invasions like those that are "sensory unjustified intrusions such as telephone and electronic invasions and spying eye or photographically".

3.2.2 Appropriation of the name or likeness

The action by appropriation is widely understood only as a violation of the property. The action is not directed against intrusive means of collection of information or embarrassing publications. Rather, it focuses on the commercial use of unauthorized identity of a person and their consequent damage to the dignity. The claim in a civil suit covered in this action is based on the recognition that an individual has an interest or right of ownership of their name or figure. The action applies when the information of the defendant or his or her image are used without consent for commercial purposes of the defended.

3.2.3 Distortion of image

This action product of the violation of privacy is similar, *mutatis mutandis*, to the action for defamation. While defamation laws protect the reputation of the individual, the action for distortion of image focuses on repairing the harm caused to the individual's peace of mind. The action includes the situation in which false or misleading information is published on an individual. The information must have been disseminated with knowledge of their falsity and must be considered highly offensive.

As it is greatly summarized in Court case (Cefalu v. Globe Newspaper Co., 1979) as with other civil actions for violation of privacy, an action for image distortion must involve inherently private matters. As such, any matter that has been disclosed to others or is visible from a public place is not protectable no matter how offensive are its implications.

3.2.4 Publicity given to private life

The civil action by public disclosure of private facts applies when highly offensive and private facts are unjustifiably publicly disseminated. The action requires the plaintiff to show that the defendant (1) was publicized, (2) to a private matter, (3) which is not of legitimate public interest, where (4) such disclosure is highly offensive to a reasonable person. The action of public disclosure of private facts give rise to compensation for the wrongful publication of true facts but informative, private value, and offensive.

However, the law adopts a stricter position with the understanding that there can be no reasonable expectation of privacy once the information has been disseminated or exposed publicly. In this regard and in order to accommodate the concerns that can generate the constitutional guarantee of freedom of speech, public affairs with informative meaning or value are not covered by this action, even though they are private in nature. These requirements mean a significant barrier to the plaintiffs and the obtaining of damages in lawsuits arising from violation of privacy actions.

3.3 Limits

The law has placed barriers to compensation after damages for privacy intrusions in the area of torts or liability. The information released must be completely private and secret, without informational value, and offensive.

3.3.1 The reasonable expectation of privacy

Before moving on a trial on privacy, US courts must first determine whether the information to protect is private according to its original nature. This is determined by applying an objective standard. That is, if there was a reasonable expectation of privacy. Such expectation of privacy is reasonable if a person of ordinary sensibilities might have felt it or experienced it in the same context.

American jurisprudence, in many occasions, relates this criteria with the place (space) where the invasion of privacy occurred, inquiring if the applicant had a reasonable expectation of privacy there, in that place, regardless the own expectative context, the environment, or cultural sensitivities that might exist. Areas such as house, a hotel room, a tanning booth and a shopping bag have been recognized as private under certain circumstances arisen on each case. Information that is not entirely unique or secret is rarely protectable. For example, an individual cannot enjoy privacy in a public place.

In one case (Duran v. Detroit News, Inc., 1993), a Colombian judge sued a newspaper for invasion of privacy by releasing her identity. The judge, whose participation in the prosecution of drug lord Pablo Escobar put at risk in Colombia, sought safety by moving to Detroit, Michigan. The court denied compensation on the basis that her actions, while remaining in the United States, revealed its identity "openly to the public eye". As she ate in

restaurants and bought articles in shops and using her real name, the court affirmed that the information disclosed was not private and thus, denied the action of privacy reasoning that these daily actions were visible by human or mechanical means.

Other US courts (Arrington v. NY Times Co., 1982) have decided that activities occurring in front of a class full of students, in the doorway of a house and in a congested city are not protectable under the protection of privacy, even when the injured underwent damage in their dignity.

US courts usually deny concept of privacy protection if the object of the violation is not absolutely secret. The New York court in *Nader v. General Motors Corporation* concluded that the information disclosed must have been completely secret to maintain an action for privacy. In that case, a well-known activist for the protection of consumer rights sued General Motors claiming that the cars company violated his privacy. The plaintiff complained that representatives of GM interviewed their colleagues about racial and religious opinions, sexual orientation, personal habits, and political trends of the plaintiff. The court refused to grant the remedy sought by the activist because the information that Gm pursued was not secret. In the reasoning of that court, the fact that the applicant previously spread the information to their friends and colleagues destroyed the secret criteria and, therefore stripped from the protection of the law.

In another case (Wilson v. Harvey, 2005), a humiliated college student sued three fellow students because they distributed a pamphlet that included his photo, email address, telephone and falsely showed him as a gay looking for a couple. The Court concluded that the fact that his contact information and photo were accessible to all students and teachers through the website of the university and, therefore, no secret, was determined to not consider any privacy violation.

The requirements of detention and concealment limit privacy protection: this is that, once that information is visible or reported or disseminated, somewhere, it can legally be collected and disseminated to anyone and anywhere.

3.3.2 Absence of public or media interest

The First Amendment to the United States Constitution prohibits the government from silencing the expression of true information, either by direct regulation or through authorized private lawsuits. Scholars in the field have argued that legal action by public disclosure of private facts, given the direct threat to freedom of speech, is unconstitutional. Some states have refused to recognize the action by public dissemination for this reason as in Court case Hall v. Post. (1988). But legal analysts maintain that the action by public disclosure only protects information that does not have informative interest or that does not belong to the "legitimate public interest". The *Restatement* (Restatement (Second) of Torts 652, 1977) defines these flexible and docile concepts as follows:

> *"Included within the range of legitimate public interest issues are the type commonly understood as 'news'. To a considerable extent, according to the moral community, publishers and broadcasters have defined the term (...). Authorized advertising includes publications concerning homicide and other crimes, arrests, police records, suicides, marriages and divorces, accidents, fires, natural disasters, death by the use of narcotics, a rare disease, the birth of child from a 12 years old girl, the reappearance of someone who had been killed years ago, [and] police report concerning the escape of a wild animal and many other similar matters of genuine, whether more or less deplorable, popular interest"*

Contrasting this, "with no informative value" is defined as one who becomes a morbid and sensational prying into private lives, so that a reasonable member of the public, with decent standards, would say that does not concern him.

3.3.3 Requirement of "opprobrious information"

The US right to privacy, and its civil actions arising from tort liability for violation thereof, judge whether privacy is deserved based on the content of the disclosed and, therefore, do not focus on the context of social relations or cultural or interpersonal understandings. In addition to check the spread to see if it was hidden enough to justify protection, courts look to the content to determine whether a reasonable person has a right to be highly offended by diffusion or discovery. Although the law provides little indication of what information is inherently opprobrious, Courts and legal analysts have offered some guide to what is marked as such as the *Restatement* (Restatement (Second) of Torts 652, 1977) indicates:

> *"Sexual relations, for example, are normally and entirely private matters, such as family disagreements, many humiliating or embarrassing or unpleasant diseases, many of intimate personal letters, details of the life of a person at home, and details of their past history would rather forget".*

US courts tend to find difficulty in determining whether the information disseminated is sufficiently offensive to a reasonable person. Lacking a consistent and contextual analysis framework, judges are forced to make uncomfortable and incongruous leap over whether such things as a mastectomy as in Court case *Miller v. Motorola, Inc*. (1990), plastic surgery as in Court case *Vassiliades v. Garfinckel's*. (1985), the romantic life as in Court case *Ben z v. Wash. Newspaper Publ'g Co*. (2006). and sexual orientation as in Court case *Sipple v. Chronicle Publ'g Co*. (1984) are private and highly offensive if they are widespread. These questions are almost impossible to resolve in a definitive manner without taking into account the circumstances of each applicant, due to the fact that they are highly dependent on historical moment, class, culture, education, and other sociological variables.

4. Discussion, privacy and the right to be forgotten: a brief conceptualization and panorama from Spanish and comparative law

No author has even tested a notion of the right to be forgotten; who have given any approach seem to be orientated towards the idea that we have a subjective right to delete from the online universe any trace that affects or may have affected some relevant aspect of privacy, honour or image of a subject. Looking deep inside, the problems caused by the abolition of that trace seems to be more of a technical nature rather than conceptual, but in no case it would be possible affirming the right to be forgotten if from the legislative bodies is not enabled a regulatory body that contains the legal consequence that the affected can do the removal of the reference to his personality in any field.

It does not seem easy to address a legal or legislative option such sensitive to ideological content and as difficult practical coverage as the right to be forgotten. It is worthy to mention that the Internet is first and foremost a huge network of insecurity. It is not just a matter of privacy of information, but rather the power to dispose of privacy. The right to be forgotten is an atypical figure in the sense that, to date, there is no legal formulation or dogmatic proposal, it is not indexed in any article at any stage, internal or international jurisdictions, the very only precise manifestation is included in a Spanish law disposition: Article 7 of the Organic Law of Protection of Personal Data, 15/1999, 13 December, hereafter, LOPD).

One of the first papers that from a scientific point of view but without any systematic effort and a more than tangentially way, referred to the right to be forgotten is owed to Xavier O'Callaghan (1991) who, in summary, and having an anticipation to the mentioned LOPD 1999, wrote:

> *"the assumptions may be substantially consistent with the definition of the right to honour. This happens in the dissemination of the contents of a judgment or process data, or data contained in public files. However, if these points were unknown in the circle in which the subject moves, because of the distance in time or place (for example, a conviction for many years is reported or disclosed in where the subject is, very far from that in which it occurred) may be interference in the right to privacy. It is what has been called (and been treated) as the 'right to be forgotten'. There is still an exception to the exception: if the*

> *subject has a public screening activity, the disclosure of such facts will not constitute interference with their privacy, precisely because of the nature of the subject."*

However, originally, the same author places the birth of this new and eventual subjective right in a case of American jurisprudence, which he realizes in a work of 1989 by Pablo Salvador Coderch, where it says:

> *"a young prostitute who came to be tried for murder, she left this life, he married and leads an exemplary life; years later, a film that recounts her life with her real name and saying that was a true case; the interested sues the producer of the film and wins the lawsuit; she had the right to be forgotten. Which is nothing but the right to privacy, which has been injured by that film, if not the right to honour, because of the certainty of the facts".*

4.1 Technical issues

As an introduction, referring to the privacy control technical options in the digital environment, most of these technologies pursue "invisible treatments", for example, data processing operations and especially personal, limiting or even cancelling at maximum, not only consent, but also the information concerned to the affected person, which either cannot know, or is ensured that in practice will be known as little as possible the processing of their personal data.

Invisible treatments, done by any mean, even though they can sometimes lead to a formal agreement, in any case they meet the requirement of free and informed consent to the processing of personal data, which requires EU legislation on protection of personal data.

In the Spanish case, Álvarez Marañón, researcher at the National Research Council (CSIC), has highlighted the full difference that exists between the relatively easy operation of deactivation of an account or profile from the removing or total deleting of that profile, which can be definitely impossible. This expert in cryptology and information security at the Institute of Applied Physics of the CSIC, has observed that disabling an account does not have "the slightest impact" and that usually becomes active again when a user re-enters their passwords; but in the case of the complete "elimination" of a profile, the complexity can become a handicap of such a nature that precludes such removal or deletion of information.

4.1.1 Technical issues in the case of search engines

Singular attention deserves the growing interest shown by citizens so that their personal data will not appear in the index or results offered by Internet search engines from the information identifying a person. In recent times the generalization of the benefits and use of these services is demonstrating important consequences when activating and allowing access to anyone into personal data which before were difficult to locate, because of being information stored on websites that allows its capture and access through indexing performed by search engines.

As already it was mentioned in relation to those who make information available on the network, although the treatment of user data may be legitimate in origin, for example the exercise of fundamental rights linked to freedom of speech, that does not mean to be guaranteed, at the request of the owner, the exercise of the rights conferred by the LOPD. Troncoso (Troncoso Reigada, Antonio, 2012) implies that technologies that do not prevent personal data indexing on search engines: we cannot forget that search engines only reflect partially what is published on websites and this to the extent that websites itself permit or deny totally or partially by scheduling of their websites so they cannot be crawled by search engines and, when appropriate, indexed for later appearing in searches of Internet users. Technology to websites do not appear on search engines has long existed, another thing is that websites do not implement it for whatever reason, but certainly the websites have the opportunity to appear or not appear in the search engines.

Therefore, when a person, having performed a search on a search engine, see your data appear on the Internet, should direct your request for deletion of data not to the search engine, but the responsible owner of the website,

who must attend such a request in accordance with data protection legislation which recognizes the right to cancel the data. After deletion of personal data in the relevant website, such data will no longer be accessible on the website, nor appear in search engines, who may no longer index deleted data when tracking the contents of the mentioned website. However, the exercise of this right in the Internet environment has a peculiarity in the case of search engines: to not appear in a search engine, first is to disappear from the website in which the data is showed, because search engines are limited to reproduce what is openly published on websites (social networks), as stated by Rallo Lombarte, Artemi (2010, pp 104-108).

4.1.2 Technical issues in the case of social networks

Briefly, it is important to mention that social networks currently provide users the ability to define their profiles. This capability allows users to graduate with some precision the visibility of their personal data in and out of the network. Indeed, the user can at any time and without the need for any request to change the visibility of your profile, such changes having an almost automatic reflex in search engines, is to appear or disappear. In this regard it should be noted that social networks already have a mechanism for social network users can exercise the right to be forgotten with effects in and out of the corresponding social network, thus also with effect on search engines.

Perhaps one of the most outstanding aspects of analysis is the one which refers to whether the user profile that social networks are configured by default must be publicly or may be closed or open, but in any case, the users would be able to configure to his or her liking at the time of registration.

An additional problem arises when the supplier of the data or user of social networks has died and their relatives try to control their digital memory. Every day more often the web and social networks have to manage digital posterity of its users and many already have established protocols for that purpose, but in the network is still difficult to control certain contents. In these cases, explains Guillermo Vilarroig, "nothing can be done but take legal actions". The media, he adds, will not change the archives that are indexed by Google. Search engines will not stop indexing contents.

5. The tension between privacy and the right to freedom of speech

In the current scenario in which we find ourselves, and after taking the pulse of the rules and sensitivity legal, which puts us in the area of Common Law, we can reach a consideration that allows us to mention that the main sticking point, the axis of the conflict on the right to be forgotten, arises in the tension between privacy and freedom of speech.

It seems logical that the right to be forgotten has entered in fight. In the words of Franz Werro (2009, p 292), referring to American law: "As a result of it, the development of a right to be forgotten in the United States, does not come, as in Europe, resulting from a balance between two rights recognized in the Constitution, but rather a series of attempts by various states to create for their citizens a sphere of inviolable privacy with respect to the media (...) ". In complete harmony with what manifests Professor Werro, and *contrario sensu*, we must agree that the starting point in the new configuration of the right to be forgotten is, at least in the European legal context, the confrontation between freedom of speech and information and the right to privacy.

Reaching an approach to the very recent and second last sentence of the Spanish Supreme Court on the matter. It is primarily to mention that in the conceptualization, regulation and dogmatic argumentation of the privacy protection, has longer beat and beats finding a constitutional basis for the right of privacy. This has deep consequences in the way of understanding this right.

As the main idea an conclusion from the sentence, it was deducted "as it pertains to the problem of collision between the fundamental right to honour and personal privacy, on one side, and freedom of information and speech, on the other, it is to be assumed that it is not possible to exercise absolute and unconditional withdrawal of the latter, since the Constitution in Article 20.4 provides that freedom of speech and information are limited by

respect for the rights recognized in this Part, by the precepts of the laws that develop it and, especially the right to honour, privacy and reputation". That is, without resorting to more dogmatic support, because the clarity of the text and context is indisputable, constitutional freedom of speech is not an absolute right; it finds one of its limits on the protection of privacy.

6. Prospects for the implementation of the right to be forgotten

After what has been exposed so far, it feels that a right that aims to break through just in retrospective, is find itself with the paradox that perhaps will only be possible to adopt it "hereinafter" from the moment when it will be legislatively collected and go into force and towards the future.

6.1 Technical resources and possibilities

We have to go back to the alternatives offered in the well-studied article by Jef Ausloos (2012) which provides three mechanisms which he grouped under the name *codes*.

- *Expiry Date*: One possibility is that the data shared online are born with an expiration date, so that come the day when the information decay. However, as acknowledged by the author, the viability of this theoretical principle is far from obvious. Alternatively, a deeper technical protection could be inserted in the data, similar to the DRM protection (referred to Digitals Rights Managements, access protection system for protected works) of intellectual property. Although the interesting research being carried out seems to throw encouraging results, however, the idea that a person will have to give an expiration date each time personal data is being collected seems unrealistic. In addition, you run the risk of becoming merely a pro- forma requirement that no one really pays attention to. And what is worse, nothing would prevent someone copied or decipher the data for as long as they are accessible.

- *Reputation Managers*: This possibility, described as interesting trend is characterized by the appearance of the managers of reputation in the Internet, websites that offer themselves to control all information circulating about a person, the defence of its technical reputation and legally, for example, through the removal of harmful information or making it inaccessible; and even define their image. This clearly illustrates the potential threats of censorship and embezzlement and distortion of information on the Internet.

- Alternatives: Refers to search for alternatives that arise with privacy protection as a standard of normal operation of the online communications. These projects are usually open source, allowing entry worldwide. One of the most notable and recent examples in this regard is "Diaspora". It is a social networking platform built from scratch with the protection of privacy in mind and is fully developed by a global community of volunteers. It will be interesting the success of a service with that difficult market penetration. The large amount of privacy and security of the files that are developed (mostly by volunteer) for web browsers also offer individuals the opportunity to have greater control over their personal data.

7. Conclusions

It is impossible to clarify whether we are far from establishing an effective system of privacy protection through the so-called right to be forgotten, although it appears that it is. We have seen that the only two legislative realities at European level indisputably in a shy way, enable the right to be forgotten are Directive 95/46 / CE of the European Parliament and the Council of October 24, 1995, on the Protection of Individuals with regard to the processing of Personal Data and the free movement of such data and Directive on the protection of privacy in the digital environment 2002/58 / CE of the European Parliament and of the Council of 12 July 2002.

We turn again to the aforementioned article by Professor Ausloos, for whom there is still a blind spot in the current context of the right to be forgotten; the scope of the right of application should be limited to cases where the owner of the data provided his or her unequivocal consent, that demonstrates a sense of privacy as a control, not dignity.

All other situations that legitimize data processing involve "need" and are out of the free wish of the interested person.

And, as a security measure against censorship and deleting of unwanted data, the "right to be forgotten" must be limited by a "public interest". This exemption would cover, but will not be limited to the issues of freedom of speech. This author, whom we are following, introduces two interesting correcting concepts, making known that to decide in their application, it could have a standard of "substantial importance" (with respect to personal data) and a proportionality test (with respect to the application for removal). But ultimately, will be the judges and national authorities of data protection who decide on the exact scope of the exception. The providing of the evidence has to be done by the data controller.

So to conclude, it can be brought up again a quote from Professor Troncoso, for who deserves specific mention of respect for the principle of quality in the processing of personal data for journalistic purposes or literary or artistic expressions. In fact, the balance between freedom of speech and the right to data protection should be primarily done from the principle of quality, not from the principle of consent which implies an uncritical automation, nor from the information principle because it will carry the implementing bureaucratic solutions.

The principle of quality is the most important within the substance of the fundamental right to protection of personal data in the areas where there are exceptions to consent, keeps within itself: the principle of adequacy and prohibition of excess, which requires that released data is suitable and relevant for journalistic purposes and not excessive data is published, preventing freedom of speech will be exercised in an excessive and outrageous manner that does not serve for the political debate; the principle of legitimate aim, which demands that the processing of personal data are exclusively journalistic or artistic or literary expression purposes, having to keep the interference with data protection consistent with the purpose of formation of free public opinion, which is what justifying its preferential protection; the principle of accuracy of the information, which requires it to be true, and correct and to cancel erroneous or inaccurate data, which is particularly applicable to the publication of media on the Internet, given the permanence of information and easy location via search engines.

The quality principle best explains the constitutional jurisprudence ponders freedom of information and privacy and is clearly applicable in this area. Thus, most of the criteria for the weighting of rights, the public interest, the truth or accuracy of the information, the essence of the information, data sensitivity, etc., have no place within the principle of quality. There are issues that, because of being of public interest, may be disseminated and may justify the collection and processing of personal data, even affecting the privacy of individuals or even involve a limit on their right to control their personal information.

The individual cannot object the publication of that information or the processing of personal data by the media, but affect the private sector. There is no chance to protect the intimate details of a person of public relevance when there is public interest, especially when their private behaviour contrasts with their public speech, for example, Berlusconi’s photos in private parties, and this can be measured by public opinion be criticized and encourage political change, something essential in the procedural value of freedom of speech.

If we conclude by protecting the right to privacy based solely on the principle of consent, we have adopted the philosophy of American privacy and we have abandoned the idea that privacy is based on human dignity, binomial, on the contrary, in which it has traditionally been based the privacy protection in Europe. The quality principle can however, correct the system leaks.

References

Allen, Anita. (1988). Uneasy Access: Privacy for Women in a Free Society. Parliament of the United States. Arrington v. New York Times Co. (1982) N.Y. Court of Appeals. 55N. Y. 2d 433; 434 N.E. 2d 1319; 449 N.Y.S. 2d 941; 1982 N.Y. LEXIS 3203; 8MediaL. Rep. 1351.

Ausloos, Jef.(2012).The right to be forgotten- Worth Remembering (Computer Law & Security Review, Vol. 28, No. 2, (pp.143-152).

Benz v. Wash. Newspaper Publ'g Co. (2006). No. 05-1760, 2006 U.S. Dist. LEXIS 71827 (pp.25).

Benn Stanley Isaac. (1971). Privacy, Freedom, and Respect for Persons. (Robert Pennock & John W. Chapman Eds., Nomos XII: Privacy 1,10, Atherton Press. (pp.1-26).

Campbell v. MGN Ltd (2004) UKHL22.

Cefalu v. Globe Newspaper Co., (1979). 391N.E.2d935.Mass.App.Ct.

Coderch, PabloSalvador. (1988) El Derecho de la Libertad. (The Right of Freedom). Colección Estudios Constitucionales. (pp.97-99).

Cooley Thomas, McIntyre. (1888). A treatise on the law of torts or the wrongs which arise independent of contract. 2nd ed., Callaghan and Company.

Dietemann v. Time, Inc. (1968). 284F. Supp. 925 C.D.

Duran v. Detroit News, Inc.,(1993). 504N. W. 2d 715, 718.Mich Ct. App.

European Commission. (2010). "A Comprehensive Approach On Personal Data Protection In The European Union" 609 final: http://bit.ly/bXUXvi.

European Convention on Human Rights, (1950).

Fried, Charles. (1968) Privacy. 77 Yale Law Journal. (pp.475-482).

Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González. C-131/12.ECLI:EU:C:2014:317.

Griswold v. Connecticut, (1965). 381U.S. (pp.479-509).

Hall v. Post. (1988). 372S.E.2d711.N.C.

Keeton, W. Page. (1984). Prosser & Keeton on the Law of Torts. 5th ed., Lawyer's ed.

Levin Avner & Sanchez Abril Patricia. (2009). Two Notions of Privacy Online. Vanderbilt Journal of Entertainment & Technology Law, Social Science Research Network, Vol. 11 (pp.1001-1051).

MC Clurg, Andrew J. (1995). Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places. 73N. C. L. Rev. 989 (pp.1000-1001).

Mc Kennitt v. Ash (CA), (2007) 3WLR194.

Mc Namara v. Freedom Newspapers, Inc., (1991). 802S. W. 2d901, 905Tex App.

Miller v. Motorola, Inc., (1990). 560N.E .2d 900.I11.App.Ct.

Newcomb Hotel Co. v. Corbett, 27G. (1921). App. 365.

O'Callagan, Xavier. (1991). Libertad de expresión y sus límites: honor, intimidad de imagen. (Freedom of Speech and its Limits: Honour, Privacy and Image) (Editorial Revista de Derecho Privado – Editorial de Derechos Reunidas, Edersa, Barcelona.

Parker, Richard B. (1974). A Definition of Privacy. Rutgers Law Review 27. (pp.281).

Prosser, William L. (1960). Privacy. 48 California Law Review (pp.383-389).

Rallo Lombarte, Artemi. El Derecho al Olvido y su Protección (The Right to be Forgotten and its Protection). Revista Telos, núm. 85 (pp.104-108).

Reeves v. Fox Television, (1997). 983F. Supp. 703, 709. N. D. Ohio.

Requa v.Kent School District. (2007). U.S. Dist. Lexxis 40920. D. Wash.

Restatement (Second) of Torts. 652.

Sabrina W. v. Willman, (1995). 540 N. W. 2d 364. Nec. Ct. App.

Sipple v. Chronicle Publ'g Co., (1984) .201 Cal Rptr. 665.

Solove, Daniel J. (2002). Conceptualizing Privacy. California Law Review. (pp.1087-1094).

Sutherland v. Kroger Co. (1959). 110 S.E. 2d7 16.

Vassiliades v.Garfinckel's. (1985). 492A. 2d 580, 590. D.C.

Von Hannover v. Germany, (2004) III Eur. Ct. H. R. 294.

Warren, Samuel & Brandeis, Louis. (1980). The Right to Privacy. (Harvard Law Review, Vol. IV, No.15. (pp.205-207).

Weber, Rolf H. (2011). The right to be forgotten: more than a Pandora's box? (Journal of intellectual property, information technology and e-commerce law, Vol.2, (pp.120–130).

Werro, Franz. (2009). The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash. Aurelia Colombi Ciacchi, Christine G (pp.292).

Westin, Alan F. (1968). Privacy and Freedom. (Washington and Lee Law Review, Vol. 25, No. 1. (pp.166-170).

Whitman, James Q. The Two Western Cultures of Privacy: Dignity Versus Liberty. (Yale Law School Faculty Scholarship, 2004) 1161-1162.

Wilson v. Harvey. (2005). 84 2N. E. 2d 83. Ohio Ct. App.