CENTRUM Católica's Working Paper Series

No. 2014-02-0006 / February 2014

The Right To Be Forgotten – Is Privacy Sold Out in the Big Data Age?

Vincent Charles, Madjid Tavana and Tatiana Gherman

CENTRUM Católica Graduate Business School
Pontificia Universidad Católica del Perú

The Right To Be Forgotten – Is Privacy Sold Out in the Big Data Age?

Vincent Charles[a]*
[a]CENTRUM Católica Graduate Business School
Pontificia Universidad Católica del Perú, Lima, Peru
E-mail: vcharles@pucp.pe

Madjid Tavana[b,c]
[b]Business Systems and Analytics Department
Lindback Distinguished Chair of Information Systems and Decision Sciences
La Salle University, Philadelphia, PA 19141, USA
[c]Business Information Systems Department
Faculty of Business Administration and Economics
University of Paderborn, D-33098 Paderborn, Germany

Tatiana Gherman[d]
[d]School of Business and Economics
Loughborough University, Leicestershire, United Kingdom

*Corresponding author at: CENTRUM Católica Graduate Business School, Calle Daniel Alomia Robles 125-129, Los Alamos de Monterrico, Santiago de Surco, Lima, Peru. Tel.: +511 626 7100.

CENTRUM Católica's Working Paper No. 2014-02-0006

The Right To Be Forgotten – Is Privacy Sold Out in the Big Data Age?

Abstract

The potential of big data has exceeded the expectations of most organizations. However, despite its vast importance and application, some important aspects of big data remain the subject of debate. One of the most sensitive and worrisome issues for big data is the *privacy of personal information*. The purpose of this paper is to explore how the major theories of philosophical ethics may be used as a referential framework for conceptualizing the evolution of the concept of privacy of personal information in the big data era. We identify a gap in big data research and suggest that while privacy has been extensively explored in different settings, it has not been sufficiently studied relative to the social and technological changes in the big data era. We attempt to fill this gap by proposing that the study of privacy be closely tied to the evolution of the social structure.

Keywords: Big data; Data analytics; Information privacy; Ethics; Human rights.

1. INTRODUCTION

Over the past years, there has been a growing and widespread interest in exploring the potential of using big data, mainly by forward-thinking organizations. Organizations have finally realized that data has become the lifeline of any modern business, as raw data can be transformed into meaningful information useful at all levels of the organization. Big data expands the opportunities of making better decisions at the strategic, tactical and operational level.

Even though the concept of big data is not new, the term is still somewhat vague as there is no unique and rigorous definition, approach, or perspective (for more details regarding the concept of big data, kindly see Beyer and Laney, 2012; Charles and Gherman, 2013; Hammond, 2013; Laney, 2001; Ohlhorst, 2013; and The Rise of Industrial Big Data, 2012). The present paper recognizes the exponential growth of both human and machine generated datasets that has occurred in the last few years, accompanied with greater coverage and scope. According to IBM (2012), 2.5 quintillion (2.5×10^{18}) bytes of data are created every day at a global scale, and 90% of the overall data available has been created in the last two years alone, most of which is unstructured. We consider the information not only generated by companies and other types of organizations but also by social media and the Internet, in general (i.e., digital transactions, sensor information, among many others).

Although initially a challenge, the collection, storage and processing of such a large amount of data has been managed fairly well using existing and developing technologies. The real challenge facing companies is how to interpret the data and how it can be used to obtain the most economic and social value so that it can be turned into a competitive advantage for the company. Or in other words, big data´s potential comes from the "identification of novel patterns in behavior or activity, and the development of predictive models, that would have been hard or impossible with smaller samples, fewer variables, or more aggregation" (Einav and Levin, 2013, p. 2).

It is becoming increasingly clear that big data is creating the potential for significant innovation in many sectors of the economy, such as health care, retailing and manufacturing, government services, just to mention a few. According to McKinsey (2013), big data analytics could generate up to $190 billion annually in health-care cost savings alone by 2020. Nevertheless, at the present time, most companies lack the knowledge of designing such predictive models, which basically means that most companies collect massive amounts of data

with a "just in case we need it" approach. Thus people have become more critical than ever before in gaining the greatest potential from big data. Without human interpretation, judgment, involvement, commitment, common sense, and ethical values, big data is both meaningless and worthless.

One thing is certain: the future of big data is yet to be written. Jahanian (2013), for example, addressed the importance of big data through the following words:

"First, insights and more accurate predictions from large and complex collections of data have important implications for the economy. Access to information is transforming traditional businesses and is creating opportunities in new markets. Further, Big Data is driving the creation of new IT products and services based on business intelligence and data analytics, and is boosting the productivity of firms that use it to make better decisions and identify new business trends.

Second, advances in our ability to store, integrate, and extract meaning and information from data are critical to accelerate the pace of discovery in almost every science and engineering discipline. From new insights about protein structure, biomedical research and clinical decision-making, and climate modeling, to new ways to mitigate and respond to natural disasters, and develop new strategies for effective learning and education – there are enormous opportunities for data-driven discovery.

Third, Big Data will be a key component to solving the Nation's most pressing challenges – in education, healthcare, medicine, energy, transportation, commerce, disaster prevention and mitigation, and cyber and national security – yielding enormous societal benefit and laying the foundations for U.S. competitiveness."

The potential of big data is, truly, unimaginable, and as previously mentioned, it has already started proving its importance and application in several areas of research. But despite the many benefits one can obtain through big data analytics, there remain some important concerns. These concerns include analytical knowledge, understanding how the data can explain behavioral factors, and, not the least, philosophical and ethical challenges. In the present paper, we will focus on the *privacy* concerns raised in the age of data revolution. Though the challenges that big data poses to privacy may be familiar, they may be more critical those most can see (Ramirez, 2013), which calls for a revision of the meaning of privacy of *personal information*.

The remainder of the paper is structured as follows. In Section 2, we briefly concentrate on defining the concept of privacy of personal information as it relates to its invasion, while also presenting some current international perspectives and challenges which can be raised in the age of big data. In Section 3, we discuss the concept of the human factor, the position of the individuals in today's market economy and the controversial topic of the individuals' rights, which we view within the framework of various theories of philosophical ethics which are outlined in Section 4. In Section 5, we discuss the transformation of the concept of privacy in terms of the evolution of the social structure, followed by the conclusion which consists of final insights and reflections.

2. PRIVACY OF PERSONAL INFORMATION AND BIG DATA

Although privacy seems to be a commonsense concept understood, to some extent, within every human society, it is rather puzzling and rather hard to define (Kemp and Moore, 2007). To quote Post (2001) "privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all" (p. 2087). In the words of Beaney (1966), "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right" (p. 255).

Whenever scholars talk about privacy they tend to introduce the concept by citing the difficulty in defining it. The present paper makes no attempt, whatsoever, to fill this gap which would be a monumental task that could be the focus of future research. However, for the purpose of the present study, which is to outline the evolution of the concept of *privacy* in the context of big data, it is worth highlighting a few perspectives on its meaning in order to be able to capture its essence and value.

Privacy was first invoked in cases dealing with the protection of the physical body, and its scope has been expanded over the last couple of decades to apply to more abstracts aspects of the person, such as the protection of personal information, reputation, and civil liberties (Kasper, 2005). Table 1 provides this information. Hence, it is important to observe that for many decades, academics have defined privacy as a right to personhood, intimacy, secrecy, limited access to the self, and control over information.

Insert Table 1 Here

The literature regarding the nature of privacy is abundant; and for more information, the reader is referred to Altman (1975), Burgoon et al. (1989), DeCew (1997), and Westin (2003). Also, previous research shows mounting levels of concern about privacy of all types (Electronic Privacy Information Center, 2008; McRobb and Rogerson, 2004; Walczuch and Steeghs, 2001; and Zakaria et al., 2003).

It is important to note that Simms (1994) distinguished between four types of privacy that the individual may want to protect from any indiscretion which are depicted in Figure 1. This perspective seems to be consistent with 30 years of previous research:

1. *Physical inviolability*: it basically refers to the individual´s right to have a "personal space" and to the intangibility of the person by others. This state can be identified with Westin´s (1967) first state of privacy called *solitude*, a state in which the individual is separated from the rest of the people and also freed from the observation of other people. This space is, ultimately, the most complete state of privacy that an individual can attain.
2. *Social inviolability*: it refers to the freedom of the individual to decide how, when, and in what way to interact with anyone in his/her private life. Westin (1967) previously referred to this state of privacy as *intimacy*, a state in which the individual is acting as a part of a small unit.
3. *Information inviolability*: it refers to the individual's right to decide how, when and to what extent his/her personal data may be made available to third parties. This state is more or less similar to the third state of privacy defined by Westin (1967) called *anonymity*, "which occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance".
4. *Psychological inviolability*: it refers to the individual's right not to be compelled to disclose his/her private thoughts and feelings to third parties, while having complete control over his/her emotional state. Ultimately, this last state can be identified with the fourth state of privacy defined by Westin (1967) called *reserve*, "which is the most subtle state of privacy, is the creation of a psychological barrier against unwanted intrusion".

Insert Figure 1 Here

Returning to the paper's main idea, the right to privacy can, therefore, be stated as the fundamental right of the individuals to control information about themselves and control the situations in which such information may be disclosed.

Regarding the term *personal data*, this is defined as "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information or a computer's IP address" (Naughton, 2013).

In this context, Ohlhorst (2013) brought to the attention that "…there is a great public fear about the inappropriate use of personal data, particularly through the linking of data from multiple sources. Managing privacy is effectively both a technical and a sociological problem, and it must be addressed jointly from both perspectives to realize the promise of Big Data" (p. 122).

As The Economist (New Rules for Big Data, 2010) pointed out very well, in the new era of Big Data, there is a necessity to create new principles to cover the area of privacy of information. "Much of this concern is focused on the privacy of personal information, and is fuelled by both the widespread use of information systems by organizations to capture, store and process information, and the ease of transmission of information between organizations" (Zureik et al., 2010, as cited by Ball, Daniel, and Stride, 2012, p. 1). But, of course, as to who should create these new principles and regulations is a political question, which would be worth exploring in more detail.

To sum up, privacy is a very sensitive topic and one of the biggest worries when talking about Big Data. By just glimpsing at the social networks, it is more than evident how much personal information people disclose to the rest of the world. It has become increasingly fashionable to think that companies should not only invest in the technology to collect and process the data, but that they should also invest in providing the public information regarding how their data is used, with whom it is shared and with that purpose, which would, in return, provide for greater individual control.

It is believed that this tension between the individuals' interest to protect their own privacy and the companies' interest to exploit personal information could be resolved by means of empowerment, which is, giving people more control. This way, they could be given the right to see and correct their personal information that an organization holds, while also having some influence regarding how it is used and with whom it is shared (New Rules for Big Data, 2010). But is this truly the solution? Let us discuss a few more concepts.

3. THE POSITION OF THE INDIVIDUALS IN THE MARKET ECONOMY

There is no doubt that the issue of the individuals´ rights is one of the most critical topics in today's world. We live in a capitalist world, a world which proclaimed the right to the freedom of speech and the right to privacy, among other universal human rights. One can recall the situation of the ex-socialist countries, for example, in which communism had left the communities with deep scars; communities in which the word *right* itself was questionable, or even worse: it was dead. As such, for many countries, the transition from a centralized/ state-owned economy to a functioning market economy was synonymous with a better life, and has meant the return of the *rights* to life. Now conditions are changing slowly but surely towards a totally different social context.

But before we elaborate on this, we must first understand the position of the individual in this equation.

Treating people as intrinsic values of the society and not just as mere parts of an impersonal economic gear evokes the deontological moral philosophy of Kant ([1785] 1990). Kant's categorical imperative requires us to be able to agree to the universalization of our own principles of action without contradicting ourselves (unconditional obligation that proclaims its authority in all circumstances), from which we can reach the conclusion that we need to treat people with respect, and moreover, that we need to respect their rights and not harm their integrity. In fact, each of us wants and claims to be treated with respect, as an end in itself and not simply as a means of enrichment for others. The concept of the *individual* should never be understood merely from the human resources perspective which considers individual more as a means for an organization to obtain its goals. From an ethical standpoint, people cannot be treated just like means, and this distinction is essential in the business ethics perspective.

Whereas in socialism the human factor was the least valuable asset in the economic context, the modern economic system can now endorse the individual as the most valuable asset.

In addition to any purely moral considerations regarding the duty of companies to treat individuals (be they employees, customers, providers, community in general, etc.) as human beings with intrinsic value, there can be an economic return from treating people with respect in the modern and competitive market economy. The fact that still many of the companies have failed to understand this basic truth is symptomatic of the rudimentary state of parts of our current society.

4. PHILOSOPHICAL PERSPECTIVES ON THE ISSUE OF PRIVACY OF PERSONAL INFORMATION

The ethical issues with respect to the issue of privacy of personal information have been clouded by the rapid change in technological innovation and the accelerating increase in the use of social media. Therefore it has been problematic for corporate leaders, policy makers and consumers to develop strategies for dealing with big data that enhances its usefulness but does not compromise the rights of private citizens and consumers to their privacy of information. Attempts to regulate the actions of corporations with respect to privacy issues could be met by resistance under the pretext that either technological change or social behavior has changed the rules. For example there have been numerous privacy issues relating to social media sites such as when Facebook's Graph Search gave strangers greater access to "private" data and Google was arbitrarily "stealing" passwords and emails. At one point Facebook announced a privacy policy that would have allowed anyone with an Internet connection and a few dollars, armed with nothing more than a Facebook user's phone number and home address, to gain critical private information that would have allowed an identity thief the ability to apply for a loan or a credit card in the name of the unsuspecting person. There have been attempts to correct this unbridled invasion of privacy, but the issue of rights has been complicated by the rapid increase in new technologies and emerging social habits.

Ironically, we find that new ways to examine and discuss privacy of personal information issues consistent with today's environment of rapid change can result from studying well-known philosophical ideas that may be hundreds of years old. In this search we can consider several philosophical systems that are the basis of ethical theory. The deontological system judges the morality of an action based upon its adherence to a rule or rules as well as upon duty or obligation. Consequentialism holds that the consequences of one's conduct are the ultimate basis for the rightness or wrongness of the conduct (i.e. "the ends justify the means"). Virtue ethics focuses on the character of the agent rather than on the nature or consequences of the act and pragmatic ethics treats morality like science, such that it can be subject to revision as it advances socially over many lifetimes.

Theories of rightness or wrongness based on deontology are independent of subjective opinions, social conditions, personal feelings, the character of the agent, or the consequences of the act; they are right or wrong based upon some higher order imperative or universal law.

Adopting an ethical strategy based on this approach could be very effective in today's rapidly changing environment because it would ensure a sense of stability to the judgmental system- i.e. it would not change with time and could be adhered to under even more rapidly changing circumstances. It would also not be subject to fickle and self-serving opinions or various stakeholders that do not look at the whole picture but only their own self-interest.

Thus the rapid pace of innovation and social change in our society may require us to consider such kind of ethical systems in order to achieve a sense of stability and objectiveness. Moreover the privacy issue is amenable to these types of arguments because human rights are generally considered to be a deontological concept.

The most famous and central philosophical concept based on deontology is the categorical imperative of Immanuel Kant which may be defined as a way of evaluating motivations for actions. It has been developed in three formulations as presented in Figure 2. Having policy makers think in terms of deontological theories such as the categorical imperative would be useful to keep them thinking at a higher level and in an unbiased way as well as not resorting to excuses for unethical actions based upon their technological expertise or their knowledge of social media. For example, the CEOs of a group of social media companies could convince a group legislators to accept very lax standards on privacy of personal information by claiming that stricter standards would jeopardize the freedom of those who want to have their information more accessible to interested parties, such as for social purposes or to obtain discounts and deals from companies. A deontological based system would not justify actions based upon these kinds of arguments which would be seen as subjective, bound by the particular social habits and fashions of the time and ultimately seen as a means to an end. Hypothetical imperatives (as opposed to categorical imperatives) tell us which means best achieve our ends but they do not tell us what ends we should choose.

Insert Figure 2 Here

Consequentialism is a class of ethical theories holding that the consequences of one's conduct are the ultimate basis for any judgment about the rightness or wrongness of that conduct. Consequentialism is usually distinguished from deontological ethics, although some argue that they are not mutually exclusive. For example, human rights, which is commonly considered a deontological issue can be justified with reference to the consequences of having those rights. So too, the privacy of information issue can be considered both founded upon deontology as well as

consequentialism. Business policy makers who consider the consequences of their actions in our rapidly changing society should consider how protecting the privacy of personal information is good for business in the long run because it protects both their businesses and their customers from unforeseen consequences such a major hack attack carried out by an unknown assailant or potential lawsuits from customers whose have suffered large economic losses because of a breach of their privacy. The engagement in practices that take a more aggressive approach to protecting privacy of information can also have beneficial consequences that might be hard to measure in advance, such as fostering a sense of loyalty of the customers to the business which could result in long term economic benefits to the customers as well as the business.

The theory of virtue ethics was born with Plato and Aristotle and is a collection of ethical philosophies that place emphasis on being rather than doing. Virtue ethics relies less on an act in any particular instance and instead considers what the decision to carry out such an act says about one's character and moral behavior. The study of virtue ethics can provide a useful way to examine the privacy of information issue in today's business and social environment. The important strategic decisions that affect privacy rights of individuals are often made by a small group of decisions makers and in many cases may depend upon the opinion and choice of one or two people such as a CEO or CIO (chief information officer). The theory of virtue ethics would study the effect that the moral character of such individuals would have on making the right decisions from an ethical standpoint; their moral character could be determined by a variety of different virtues such as wisdom, prudence or justice. This approach illustrates the importance of having the people with the proper moral character or the right mix of moral virtues in positions of authority in high tech companies or any organizations that would have an impact on the right to privacy. This could have important policy considerations in the area of human resource management for these types of organizations.

The last theory of philosophical ethics we shall discuss is that of pragmatic ethics which is aimed at social innovation. It differs from the others theories in that it concentrates on society as a whole instead of individuals as the entity that achieves morality, it does not hold any moral criteria as beyond potential for revision and it allows that a moral judgment may be appropriate in one age of a given society, even though it will cease to be appropriate after that society progresses (for example, the writings of Thomas Jefferson framed slavery as ultimately immoral, yet temporarily moral until America was ready for abolition). This approach to

philosophical ethics, which was held by the American philosopher and psychologist John Dewey, may have a great deal of potential in helping to frame the issue of privacy of information within the context of a rapidly changing society. In particular it would allow for decision makers and policy planners to consider the right to privacy issues in a constant state of flux and provide them the flexibility to constantly update policies based upon moral considerations that may change with time. So for example the adoption of innovative technologies that can create more effective decision making strategies using big data may ultimately affect what is considered morally right for the society as a whole with respect to the privacy of information. Note that the pragmatic approach to ethics seems to be in stark contrast to the deontological approach which assumes that what is considered morally correct depends on some universal law and not tied to any particular conditions or circumstances, although the pragmatists would acknowledge that it would be appropriate to practice a variety of approaches.

Thus we see that the various theories of philosophical ethics provide us with a variety of ways to study the issue of privacy of information in our rapidly developing society. Each approach is based upon certain principles which may be in contrast to one another. But these theories show how these traditional philosophical viewpoints can shed a great deal of insight into the privacy of information issue.

5. THE EVOLUTION OF THE CONCEPT OF *PRIVACY*

Now let us turn our attention once again to the issue of privacy. The interest of the companies to gather as much information as possible about different types of individuals, generally called stakeholders, has increased significantly with the rise of big data. To better understand the concept of *privacy*, it is worth analyzing the transformation of the concept within the contradictory framework of socialism-capitalism (see Figure 3).

Insert Figure 3 Here

It is interesting to note that during the communist regime, each individual (whether aware or not of the situation) had one big personal *file*, filled-in with all kinds of personal information by a "concerned" authority (be it the company that employed the individual or a public administration office). The individuals did not have access to their files and had no idea what the file was about or the type of information available inside, in which were recorded all sorts of details, not only related to the professional trajectory of each individual, but also related to their

political and ideological beliefs. An individual´s file contained the same information about the spouse, children, and all the rest of the family members, dead or alive.

As a consequence, the file contained information such as whether a close relative was a political prisoner or a former legionnaire, an uncle belonged to a religious cult, a family member fled abroad, or a sister was dating a foreigner, among others. The file even included reports about one´s possible marital infidelities, sexual orientation, or other so-called questionable behaviors, such as drinking, smoking, currency trafficking and goods purchased from the local shop or brought from outside the country, along with reports regarding the individuals´ habits of attending religious services , reading foreign publications, visiting foreign embassies or repeatedly meetings foreigners.

The lack of privacy was pushed to the extent that the reports included whether the individuals exhibited any behavior hostile to the socialist political system, whether they said political jokes at any point of time or made fun of any political leader, whether they made critical remarks of the state of affairs in the country, and even whether they were listening to hostile radio stations.

For those who lived or heard about it, this was, in short, the dreadful reality in the socialist countries. For the people living under these conditions privacy was an ideal worth fighting for but completely out of reach. But nevertheless individuals tried to protect whatever information was possible, with the strong belief in their hearts that no one, absolutely no one, had any right to "enter" or "access" their privacy.

Today we sometimes think of the invasion of privacy as a thing of the past, yet many private companies are making huge profits by invading individuals' privacy by collecting their personal information in the era of big data expansion.

So what happened?

While in the past, one suffered political oppression as a result of disclosing personal information now it is very feasible for companies to gather even more information using technology without any intent of aggression towards the individual.

From the authors´ perspective, one possible explanation is the following, which may be subject to debate.

In the capitalist system, perception has changed substantially. Take for example, the social networks, such as Facebook or Twitter, whose rise to dominance has seen their user-base

grow to hundreds of millions. Nowadays, individuals are happily posting information (which once they would have tried to protect) on the social networks in a deliberate and consensual way. The social pressures arising from the expansion of social networks are enormous and have created the illusion that using them makes you cool. How many times do we hear the phrase: "If you are not on Facebook, you do not exist"?

In capitalism, we assume that the right to privacy is an automatic right of each citizen (as opposed to socialism) and the freedom of each individuals gives him or her the right to decide what personal information to reveal to others. But the rise of social networks has now made it "trendy" to share as much of your privacy with others as possible and if you choose not to do it, somehow you become "antiquated". Whereas in socialism you suffered oppression, nowadays you are cordially "invited" by social pressure to reveal as much private information as possible.

Having your habits, activities, and preferences retrieved and registered is now a routine practice. And it is to be noted that "personal information is increasingly used to enforce standards of behavior; information processing is developing, therefore, into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct..." (Simitis, 1987, p. 707).

All of this can facilitate an improved social adjustment for the individual but may compromise the individual's freedom and his or her capacity to make his or her own decisions.

From this perspective, we can say that big data is the new invention (highly profitable!) of capitalism. Thus the issue of privacy is more important than ever before and although capitalism respects the right of privacy, we have not yet determined a workable definition nor have learned how to use it. It is up to us to redefine the limits and meanings of our own rights in the era of big data.

Hence, the increased access to personal information in the age of big data has sharpened the need to revisit the meaning of the concept of privacy.

6. CONCLUSION

The primary purpose of the present paper is to examine and discuss some key aspects of the evolution of the concept of *privacy* of personal information in the new era of big data, as well as to acknowledge the need to create new principles related to the topic of privacy of information. The paper explores how the various theories of philosophical ethics may be used as a referential

framework for explaining the evolution of the concept of "privacy" and how this is linked to big data. We hope to have contributed to the advancement of the scholarly debate in this area.

Here are our final reflections with respect to the concept of *privacy* of personal information in relation to big data.

The social setting of our society has changed tremendously over the past few years and we are now witnessing the mutation of the very definitions and meanings of traditional concepts, such as *privacy*. We must admit that privacy is no longer what it used to mean. One of the effects of the big data age is a divorce of privacy from the person. Basically this means that with more and more of our personal information being routinely collected and stored by companies or willingly disclosed via a computer and an internet connection, our privacy is now being traded as if it were to be a commodity. "Add to that emerging technologies like Google Glass and facial recognition technology [already deployed by Facebook] and you've got a recipe for ubiquitous mass online surveillance not just by intelligence agencies, but by all. And it's unclear how all this will be used in the near or long-term future." (The Guardian, 2014).

The ethical issues with regard to respecting privacy in the big data age need to be established on the basis of general premises regarding the status of individuals in today's capitalist society.

Ohlhorst (2013) makes a very reasonable assertion: "Many online services today require us to share private information (think of Facebook applications), but beyond record-level access control we do not understand what it means to share data, how the shared data can be linked, and how to give users fine-grained control over this sharing" (p. 123).

It is our belief that in a democratic capitalist society it is right and also necessary that individuals fight by all means to have their right to privacy respected. Even the case of willing disclosure does not give a third party a moral right to own it and make use of it. Fundamental universal human rights can never be transferred.

We would like to finish the present paper with a quote by Simitis (1987, p. 708) which we believe it is more valid today than ever:

"The processing of personal data is not unique to a particular society. On the contrary, the attractiveness of information technology transcends political boundaries, particularly because of the opportunity to guide the individual´s behavior. For a democratic society, however, the risks are high: labeling of individuals, manipulative tendencies, magnification of errors, and

strengthening of social control threaten the very fabric of democracy. Yet, despite the incontestable importance of its technical aspects, informatization, like industrialization, is primarily a political and social challenge. When the relationship between information processing and democracy is understood, it becomes clear that the protection of privacy is the price necessary to secure the individual´s ability to communicate and participate. Regulations that create precisely specified conditions for personal data processing are the decisive test for discerning whether society is aware of this price and willing to pay it. If the signs of experience are correct, this payment can be delayed no further. There is, in fact, no alternative to the advice of Horace: Seize the day, put no trust in the morrow…"

ACKNOWLEDGEMENT

The first author would like to thank Prof. Erik Brynjolfsson and Prof. Alex 'Sandy' Pentland from the MIT for their valuable insights.

REFERENCES

Altman, I. (1975). The Environment and Social Behaviour. Belmont, CA: Wadsworth.

Ball, K., Daniel, E. M., and Stride, C. (2012). Dimensions of employee privacy: an empirical study. Information Technology & People, 25(4), pp. 376-394.

Beaney, W. M. (1966). The Right to Privacy and American Law, Law and Contemporary Problems, 31, pp. 253-271. Retrieved January 4, 2014, from http://scholarship.law.duke.edu/lcp/vol31/iss2/2

Beyer, M. A. and Laney, D. (2012). The Importance of 'Big Data': A Definition. META Group (now Gartner). Retrieved August 1, 2013, from http://www.gartner.com/DisplayDocument?id=2057415&ref=clientFriendlyUrl

Burgoon, J. K., Parrott, R., LePoire, B. A., Kelley, D. L., Walther, J. B., and Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationship. Journal of Social and Personal Relationships, 6(2), pp. 131-58.

Charles, V. and Gherman, T. (2013). Achieving Competitive Advantage Through Big Data. Strategic Implications. Middle-East Journal of Scientific Research, 16(8), pp. 1069-1074.

DeCew, J. (1997). In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, NY: Cornell University Press.

Einav, L. and Levin, J. (April, 2013). The Data Revolution and Economic Analysis. Prepared for the NBER Innovation policy and the Economy Conference. Retrieved February 1, 2014 from http://www.stanford.edu/~leinav/pubs/NBER2014.pdf

Electronic Privacy Information Center. (2008). Public opinion on privacy. Retrieved September 10, 2013 from http://epic.org/privacy/survey/

Fried, C. (1984). Privacy. In F. D. Schoeman (Ed.), Philosophical dimensions of privacy (pp. 203-222). New York: Cambridge University Press.

Gavison, R. (1980). Privacy and the Limits of Law. Yale Law Journal, 89(3), pp. 421-471.

Hammond, K. J. (May, 2013). The Value of Big Data Isn´t the Data. Harvard Business Review. Retrieved July 13, 2013 from http://blogs.hbr.org/cs/2013/05/the_value_of_big_data_isnt_the.html

IBM. (2012). Simply Good Design. 2012 IBM SOA Architect Summit. Retrieved July 20, 2013, from https://www-950.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/SOA%20Design%20Principles%20

and%20Development%20Q4%202012_Final/$file/SOA%20Design%20Principles%20and%20Development%20Q4%202012_Final.pdf

Inness, J. C. (1992). Privacy, Intimacy, and Isolation. New York, NY: Oxford University Press.

Jahanian, F. (April, 2013). Next Generation Computing and Big Data Analytics. Testimony before the Committee on Science, Space, and Technology Subcommittee on Technology and the Subcommittee on Research. U.S. House of Representatives, USA. Retrieved December 1, 2013 from http://docs.house.gov/meetings/SY/SY19/20130424/100764/HHRG-113-SY19-Wstate-JahanianF-20130424.pdf

Kant, I. ([1785] 1990). Foundations of a Metaphysics of Morals. New York, NY: McMillan.

Kasper, D. V. S. (2005). The Evolution (Or Devolution) of Privacy, Sociological Forum, 20(1), pp. 69-92.

Kemp, R. and Moore, A. D. (2007). Privacy. Library Hi Tech, 25(1), pp. 58-78.

Laney, D. (2001). 3D Data Management: Controlling Data Volume, Velocity and Variety. Applications Delivery Strategies. META Group (now Gartner). Retrieved August 1, 2013, from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

McKinsey Global Institute. (2013). Game Changers: Five Opportunities for US Growth and Renewal, July [online] http://www.mckinsey.com/insights/americas/us_game_changers (accessed 13 December 2013).

McRobb, S. and Rogerson, S. (2004). Are they really listening? An investigation into published online privacy policies at the beginning of the third millennium. Information Technology & People, 17(4), pp. 442-61.

Naughton, J. (October, 2013). Why big data has made your privacy a thing of the past. Retrieved November 13, 2013, from http://www.theguardian.com/technology/2013/oct/06/big-data-predictive-analytics-privacy

New Rules for Big Data. (February, 2010). The Economist. Retrieved July 14, 2013 from http://www.economist.com/node/15557487

Ohlhorst, F. (2013). Big Data Analytics: Turning Big Data into Big Money. Hoboken, NJ: John Wiley & Sons, Inc.

Post, R. C. (2001). Three Concepts of Privacy, Faculty Scholarship Series. Paper 185, pp. 2087-2089. Retrieved December 13, 2013, from http://digitalcommons.law.yale.edu/fss_papers/185

Ramirez, E. (August, 2013). The Privacy Challenges of Big Data: A View from the Lifeguard´s Chair. Speech at Technology Policy Institute´s Aspen Forum. Retrieved January 5, 2014, from http://www.ftc.gov/about-ftc/biographies/edith-ramirez

Reiman, J. H. (1984). Privacy, Intimacy, and Personhood. In F. D. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology (pp. 300-316). Cambridge, MA: Cambridge University press.

Simitis. S. (1987). Reviewing Privacy in an Information Society. University of Pennsylvania Law Review, 135, pp. 707-737.

Simms, M. (1994). Defining privacy in employee health screening cases: Ethical ramifications concerning the employee/employer relationship. Journal of Business Ethics, 13(5), pp. 315-325.

The Guardian. (2014). Little Privacy in the Age of Big Data [online] http://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-data (accessed 11 July 2014).

The Rise of Industrial Big Data. (2012). Leveraging large time-series data sets to drive innovation, competitiveness and growth—capitalizing on the big data opportunity. GE Intelligent Platforms White Paper. Retrieved August 3, 2013, from http://www.ge-ip.com/download/the-rise-of-industrial-big-data/13476//

Walczuch, R. and Steeghs, L. (2001). Implications of the new EU directive on data protection for multinational corporations. Information Technology & People, 14(2), pp. 142-62.

Westin, A.F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), pp. 431-53.

Westin A. F. (1967). Privacy and Freedom. New York, NY: Atheneum.

Zakaria, N., Stanton, J. M., and Sarkar-Barney, S. T. M. (2003). Designing and implementing culturally-sensitive IT applications: the interaction of culture values and privacy issues in the Middle East. Information Technology & People, 16(1), pp. 49-75.

Zureik, E., Stalker, L. L. H., Smith, E., Lyon, D., and Chan, Y. E. (2010). Privacy, Surveillance and the Globalization of Personal Information: International Comparisons. Montreal, Canada: McGill University Press.

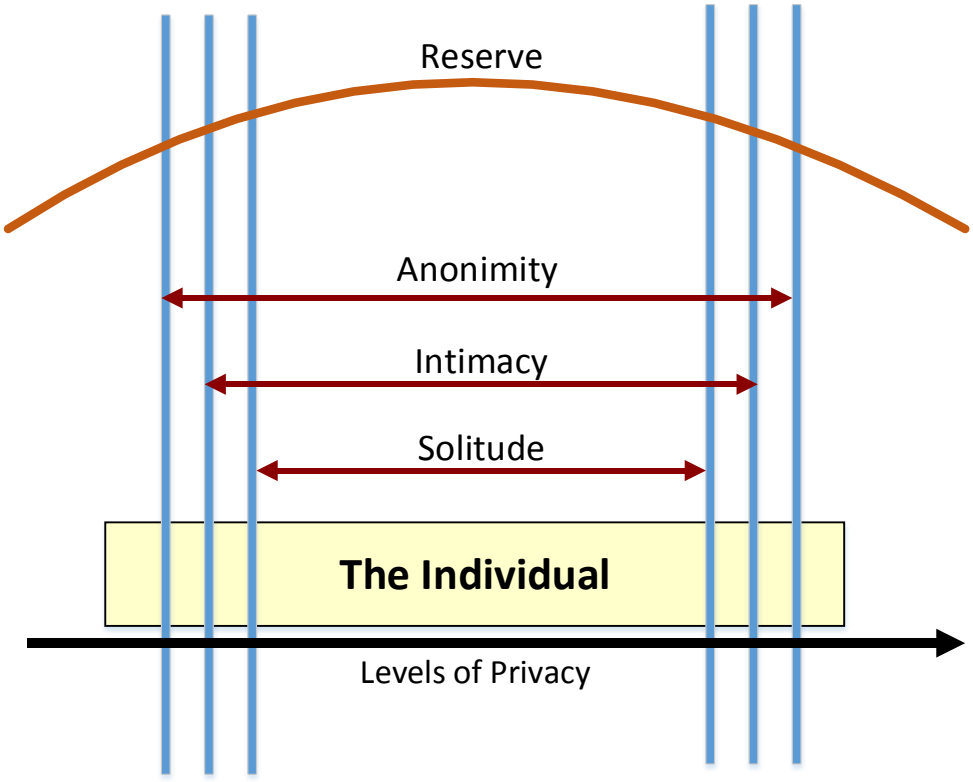

Figure 1. Levels of individual privacy

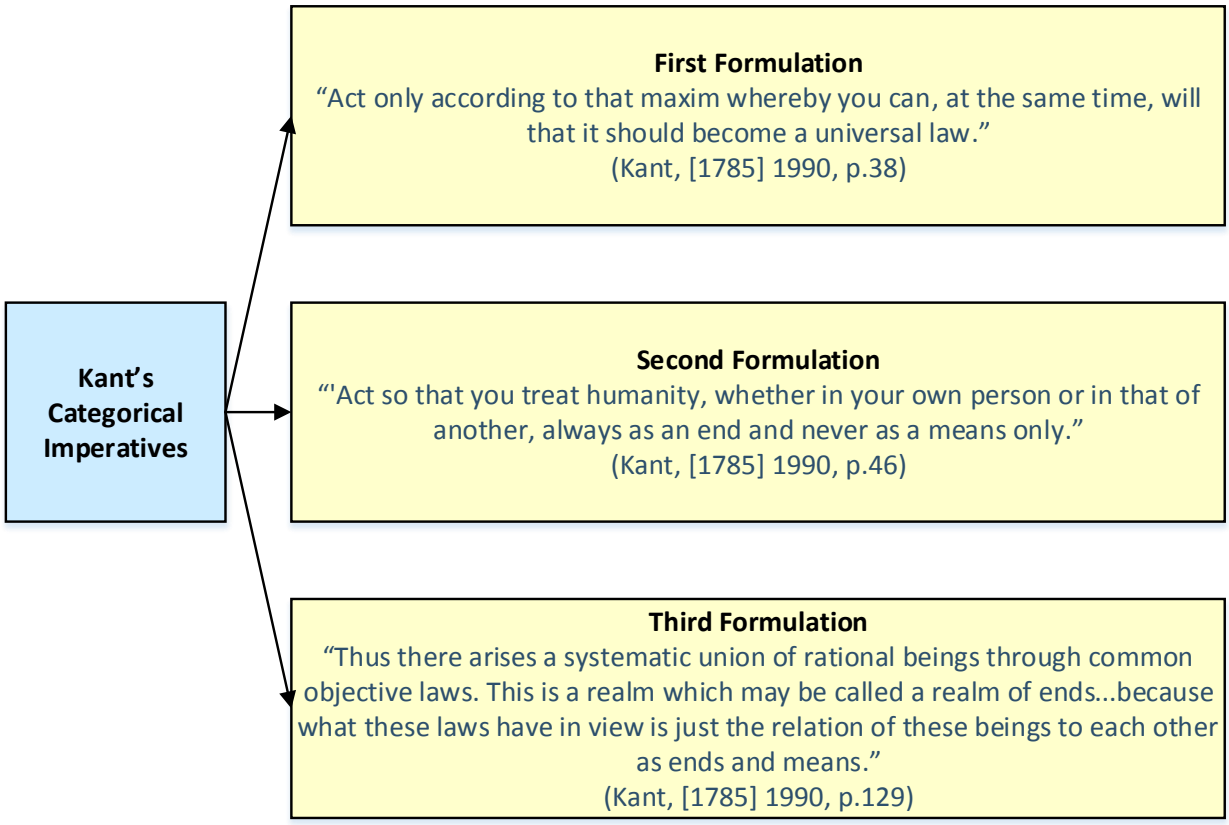

Figure 2. Kant´s three formulations of the categorical imperative

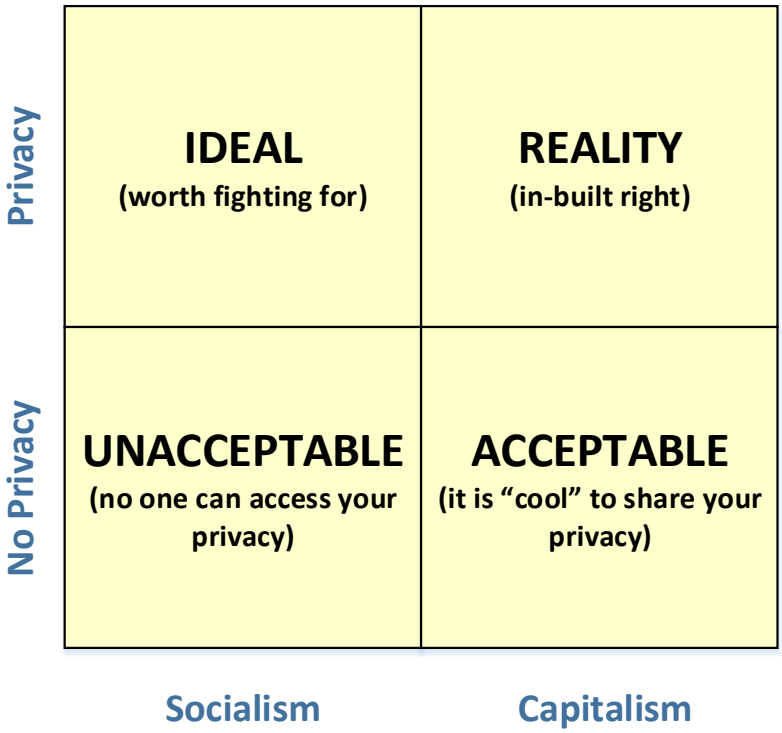

Figure 3. The mutation of the concept of *privacy*

Table 1. Different perspectives regarding the concept of *privacy*

Westin (1967)	"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."
Gavison (1980)	"The concept of privacy […] is a complex of […] three independent and irreducible elements: secrecy, anonymity, and solitude."
Fried (1984)	"Privacy is not simply an absence of information about what is in the minds of others; rather it is the control we have over information about ourselves."
Reiman (1984)	"Privacy protects the individual´s interest in becoming, being, and remaining a person."
Inness (1992)	"Privacy is the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent´s love, caring, or liking. These decisions cover choices on the agent´s part about access to herself, the dissemination of information about herself, and her actions."
Simms (1994)	"Privacy is fundamentally linked to the individual's sense of self, disclosure of self to others and his or her right to exert some level of control over that process".