Internet privacy in higher education in a non-democratic context

1. Introduction:

We live in a world where we rely more and more on the internet for most of our communication activities. In our email communications, social networking, banking activities, internet searches, and our news consumption, we share, receive and exchange a large amount of data. The data consists of a wide variety of personal information that is stored, thanks to cloud computing, in servers that belong to companies that provide us with email service, social networking platforms, online games, and other internet services. While privacy has always been an important human right issue, it is now even more important with the internet. Research shows that advances in digital technologies combined with the collection and storage of an unprecedented amount of personal information represent major challenges to internet users' information privacy (Angst and Agarwal, 2009; Malhotra et al. 2004; Ward et al. 2005). Culnin and Bies (2003) argue that privacy is one of the most significant political, legal, ethical and social issues of today's information age.

This paper will describe and analyze the ways in which we as internet users are becoming more and more vulnerable in our work places. The paper will not focus on the broader issues of internet privacy related to people's use of the internet such as anonymity, data security, http cookies, or device fingerprinting. The paper will focus on internet privacy within an institutional context, more particularly in the context of higher education. As students, faculty, and staff, we use internet services provided by the university. The university gives us email addresses, access to computers and internet connectivity, manages our academic and financial records, and keeps records of our library activities, among many other things. The institution stores all this data on each user in its servers and hand over the management of this data and services to an information technology department. As users, we cannot opt out of these services. For instance, university administrations use information systems which allow the administration to communicate and manage its various transactions with its personnel who have no choice but opt in to such systems. The inability to opt out of these university services adds to the vulnerability of internet users.

The paper focuses on personal data, not secret data, of employees (in our case students, staff and faculty) that employers (university) have access to. There are at least four sets of problems the paper tries to address. First, the issues for privacy in the employer-employee relationship in today's world give rise to many problems related to the presence of security camera, email communication, browsing history, and communication systems increasingly reliant on cloud computing. Personal data of employees is now digitized and encompasses other aspects of employees' information, such as information collected through video cameras, and this digitized information can travel fast and wide. Second, in employer-employee relations, employers are in a powerful position as they can anticipate privacy violation claims simply by informing employees that monitoring, surveillance and search may occur. Employees may be informed during the hiring process, in the employees' handbook, or through posted policy statements. The third set of problems relates to the overall willingness among internet and modern technologies users to give up their privacy for the convenience these technologies offer (Schneier, 2013). The internet allows greater and easier access to information, security cameras arguably enhance security, and using the same devices to solve professional and personal issues is quite convenient. The fourth set of problems relate to human rights in non-democratic countries. In Morocco, the existing laws do not necessarily protect citizens since the courts and the overall political system do not abide by the principles of rights of citizens. The political culture, and by implication the culture within all institutions as well, allows for the exercise of political power to occur without respect of the law. In such systems, possibilities of abuse of power coupled with impunity are current (Madani, et. al., 2012).

This study provides an examination of internet privacy at a Moroccan higher education institution, Al Akhawayn University in Ifrane (AUI), from the perspective of the users as well as the administration. The choice of AUI is based on the fact that the university is a pioneer institution in internet connectivity in Morocco. The first Internet protocol suite (TCP/IP) connectivity was established at AUI in 1995 which marked the official birth of the Internet in Morocco. We believe that AUI must therefore continue its pioneering role in internet related policies in the same manner it does in terms of infrastructure. The questions and issues related to internet privacy at AUI are for the most part the same in other workplaces. Institutions and organizations, whether educational, business or not-for-profit, offer internet services to their employees (or students) who shares large amounts of private data. Internet users within these institutions lose control over their private data while these institutions become empowered by the amount of private data they control.

To address the four sets of problems, the paper adopts a human rights-based approach. Article 24 of the Moroccan Constitution stipulates that private communication in all its forms must be protected. Law 09-08[i] related to the protection of individuals with regards to processing of personal data was promulgated in 2009. It sets the legal requirements about individuals' privacy rights, and it delineates the different rights such as the right to be informed of any operation that involves access to individuals' personal information, and the right to give or not give permission for such access. It also gives the right to individuals to access their data, and make the needed corrections and modifications. The Law also describes the roles and responsibilities of the person(s) or entity holding and processing these data, and the sanctions regarding the non-compliance with this law. A human rights-based approach emphasizes that human rights must be achieved in ways that impact society as a whole with an eye on the long term. This paper argues that laws and policies are very important but they do guarantee privacy protections. In non-democratic countries, and in the absence of an independent judiciary, laws do not always protect the rights they are supposed to protect. The paper argues that all the stakeholders, administration, students, faculty, staff, and technology services must be involved in creating a safe environment. The institutional culture of the university must nurture the values of privacy as a human right, and this culture is the making of the whole community. Internet users must take an active role in this process of protecting their data and must be educated about what they disclose when they interact online or use the services provided by the university.

This paper aims to answer the question of how to provide a safe environment to protect the privacy rights of the internet users within higher education institutions in a non-democratic country. The paper will first summarize some of the major arguments in the literature related to issues of privacy, internet regulation, and the nature of technology. After a short description of the methodology, the paper will outline the results from both the survey and the interviews. The survey investigates primarily the extent to which the university community is concerned about privacy and the level of their awareness of the amount of data the university controls. The paper will conclude with a list of recommendations on the course of action to take to provide a safe environment for internet users in higher education.

2. Morocco as a non-democratic country

Morocco's political regime is a *competitive authoritarian* regime rather than a transitional democracy. Competitive authoritarian regimes utilize elements of democracy to ensure continuing domination over opposition forces. Levitsky & Way (2002) authored the concept. They conceive competitive authoritarianism as civilian regimes in which "formal democratic institutions are widely viewed as the primary means of gaining power, but in which fraud, civil liberties violations, and abuse of state and media resources so skew the playing field that the regime cannot be labeled democratic" (p. 4). Such regimes are competitive because democratic institutions are real and "opposition forces can use legal channels to seriously contest (and occasionally win) power; but they are authoritarian in that opposition forces are handicapped by a highly uneven—and even dangerous—playing field. Competition is thus real but unfair" (ibid).

Thus, competitive authoritarian regimes are hybrids characterized by the presence of some democratic institutions and some democratic practices (such as elections, multi-party system and a constitution) within the authoritarian state. Levitsky and Way introduced the framework to challenge the "democracy bias" of most literature about post-cold war regimes. Hybrid regimes are typically categorized as flawed and incomplete and described as transitional, e.g. as "evolving democracy," "nascent democracy," "ongoing democracy," or "would be democracies." For countries where the "transition" isn't moving forward, terms such as "stalled," "protracted" or "flawed" democracies are typical. Levitsky and Way argue that such characterizations are misleading because they assume that hybrid regimes are—or should be—moving toward democratic forms of government, when in reality many regimes remain stable or actually increase authoritarianism. Guillermo O'Donnell (1996) and Thomas Carothers (2002) suggested we should stop treating such cases as transitional and conceptualize them as distinctive forms of non-democratic regimes.

The Moroccan state creates democratic institutions and promulgates law and policies to use as a site of struggle with opposition forces while steadfastly maintaining control by establishing an uneven playing field. The uneven playing field is primarily manifested in maintaining a non-independent judiciary system that allows it to bypass the same laws and policies it establishes. Although the constitution designates the judiciary as a separate branch of government, the judiciary system in Morocco is far from independent. The king chairs the High Council of Judiciary Power and appoints its members. As such, the courts often fail to produce fair and balanced rulings, frequently basing their decisions on recommendations from security forces (Madani, et. al., 2012).

3. Privacy

Westin (1967) defines information privacy as the ability of the individual to control when, how, and to what extent his or her personal information is communicated to others (Westin, 1967). One of the main key words in this definition is “control”, and given the era of cloud computing, we can safely conclude that internet users have very limited control over the content of most of their internet activities. Another definition of privacy raises important questions on whether privacy is an objective matter that can be controlled at all. Harper (2004) defines privacy as “the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values” (p. 3). For Harper, privacy is a subjective matter because what may be private information for one person, such as his/her medical condition can be public information for another. The first person wants his/her medical information to remain private while the second wants to make it public, in cases for instance when such action helps him/her cope with the condition. Harper argues that while privacy laws can protect some aspects of users’ privacy, they are not enough unless the users are active participants in the protection of their own privacy. Both Westin and Harper focus on private information, and not necessarily on personal data, the kind of data employers have access to. These definitions are applicable to personal data because privacy laws account for both personal data held by employers and personal data that can be obtained by governments or other public or private agencies.

An important contribution to understanding the relationship between privacy and power is Michel Foucault’s theory of surveillance. This is particularly relevant in the context of non-democratic countries. The theory was inspired by Bentham’s Panopticon, which is Bentham's plan for a prison where the inmates behave in conformity not because they are under direct threat, but under the possibility of being watched and observed by the powers that be. What the current state of Internet privacy has created among its users is a panopticon-effect, an awareness of the possibility of being watched without necessarily being the case. When people are aware of being watched, they tend to act in a way that is not the byproduct of their own agency but the byproduct of society’s expectations. One argument people make to justify the presence of surveillance and to justify their consent to it, is that “as long as I am not doing anything wrong, then there is nothing I should worry about.” Greewald (2014) argues that this attitude lead to self-deprecation: "I have agreed to make myself such a harmless and unthreatening and uninteresting person that I actually don't fear having the government know what it is that I'm doing” (Greenwald, 2014). The university community, much like other work places, must take an active role in protecting its privacy to avoid turning a higher education institution into a place of docility and submissiveness.

4. Privacy and the internet legal framework

Apart from the fact that the technology backing and running the Internet is detrimental to users' privacy, the legal framework built around Internet usage is no more empowering. Privacy online is usually conceived of in either a right-based conception of privacy in which privacy is a right to every Internet user, or a utilitarian interest-based conception in which privacy can be given up partially for free online services. The state of the Internet today reveals that the interest-based conception is slightly preferred. The approach to privacy protection on a global level is “loosely defined self-regulatory approach” (Fernback & Papacharissi, 2007, p. 716). The Internet is deregulated, and Internet companies are at the forefront of the battle to defend the idea of deregulation to keep states and governments off of the Internet. This idea is “follows in the tradition of self-regulation prevalent in the USA”, headquartering most the Internet big companies, “which is founded on a lack of government involvement in regulating consumer privacy” (Fernback & Papacharissi, 2007, p. 719).

As noble as this mission may sound, and as much as it shows a dedication to a communication medium free of interference, “within a deregulated, unenforceable, and unmonitored model of industry self-regulation, trusting in an industry’s intentions is offered as the primary means of ensuring privacy protection” (Bodle, 2011, pp. 156). Indeed, the only form of protection a user is offered when using an Internet service is to accept or decline the Terms of Service Agreement which includes a privacy policy. Privacy policies explain in sophisticated legalese language how the user's data that is available to the company will be dealt with. The complexity of those documents doesn't encourage the users to read or try to understand them, and that it because they “contain 'catch- all stipulations' to protect companies against litigation, and provide protection through ambiguity” (Bodle, 2011, p. 161). Privacy policies are there to protect companies, they are generally written “with the threat of privacy litigations in mind rather than commitment to fair data handling practices” (Pollach, 2007, p. 107).

Both the Internet's technological and legal reality put the user in a weak position in front of corporate power. The implications here are mainly commercial use of data, but the recent NSA revelations have shown that the implications can also be political. In non-democratic environments such as Morocco, the stakes are higher. The state can in total impunity use private information accessed in an illegal manner to incriminate people who hold dissenting views or who threaten the status quo.

5. Online computing and privacy

Online computing has been transformed in the last decade, arguably since the democratization of Internet access and increasing popularity of Internet-enabled devices such as smartphones and tablets. One important aspect of these new developments is the phenomenon of cloud computing and they are detrimental to the user's privacy. Cloud Computing consists among other things of online collaboration, media center storage, streaming solutions, all of which encourage users to give up astronomical amounts of private data for the sake of convenience, that is, doing all their tasks at their one online stop shop. Cloud computing services provide more computing power and more storage space than the user's personal computer or device. This factor alone motivates users to be lazier about which data to keep on the company's servers, since thanks to Moore's Law, “it becomes easier to save everything than to figure out what to save” (Schneier, 2014). Consolidation in the cloud enables enormous amount of user data to be linked, cross-searched and thus made meaningful.

Instead of buying the licenses to operate software such as Photoshop and have them installed in computer labs, universities purchase the right to use the software and gets access to the

Photoshop cloud. All the activities at the university are stored in Adobe servers and it is through cloud computing that access to and use of this editing software is made possible.

These computing trends can be used to enhance the user's experience as many of those companies claim, but they also enable companies control over large amounts of private data.

6. Methodology

The study used surveys and interviews as the primary data collection tools. The quantitative 21-question paper survey was distributed on campus. It examined the opinions of respondents on the issues of access to private information. It examined their level of awareness with regards to AUI's access to their information and data, and their level of concern vis à vis their privacy. In other words, the main questions revolved around whether they know what type of data AUI administration has access to and whether they feel concerned about that. The last section of the survey asked questions about whether the respondents perceive internet services as a "right" to access a public utility or as a "service" offered by the university, and whether they want to have a policy on privacy at AUI.

The initial sample consisted of 300 convenient surveys. The study used stratified sampling with proportional allocation. The size of the sample in each stratum is taken in proportion to the size of the stratum. We used gender, school (the School of Science and Engineering, the School of Business Administration and the School of Humanities and Social Sciences), university level (freshman, sophomore, junior, and senior), and Moroccan versus international students. The final sample consists of 100 surveys, which constitutes roughly 5% of the overall population of AUI students (1974 students). The statistical software program SPSS was used to analyze the responses.

For the interviews, we used in-depth semi-structured interviews whereby we used a list of questions that covered some specific topics but had some leeway to change the order of the questions and to adjust the level and type of language (Berg, 2005). The interviews were conducted in English. The sample criterion was purposive (Patton, 2002). The interviewees were selected on the basis first of their administrative position and their level of expertise in the field. The interviews lasted from one hour to one hour and fifteen minutes. All interviews took place between March and April 2014. We interviewed five faculty members, three with expertise in international law and civil rights law, and two with expertise in internet security. The director and three staff members of the ITS were also interviewed. Senior administrators such as the vice president for Academic Affairs and the vice president for Student Affairs did not respond to our requests for interviews. Each interview was recorded and transcribed verbatim. The texts were thematically analyzed using Flick's (1998) method of thematic coding in order to identify the most relevant categories that depicted the interviewees' perspectives on the issues of privacy at AUI. This approach allows for the examination of the phenomenon directly from the perspective of the interviewees (Vettehen et al, 1996). While conducting semi-structured interviews as a methodology does not lead to generalizable results, it offers the opportunity to distill the interviewees' experiences and insights (Berger, 2007).

7. Findings:

7.1. Survey

The survey first gauged the level of awareness among AUI students of the extent of the university access to their private data. An initial search was carried out at the level of ITS to see what data ITS has access to and the result was the following. ITS had access to students email, N-Drive[ii], Jenzabar[iii], public printers, library, security cameras, passwords, cash wallet purchases, and financial information. More than half of the respondents were aware of the access to all these items. While access to Jenzabar data was obvious with 79.38%, awareness of access to passwords was relatively low with 52.04%. For email, 59.18% were aware that AUI had access to their email.

The survey findings show that AUI students are very concerned about their internet privacy. Only 2.04 percent said they were not concerned, the rest were alarmed 31.63%, very concerned 35.71, and concerned 28.57%. When asked about the reasons why they are alarmed or concerned, 70.10% of the respondents said invasion of privacy, 22.68% expressed worries that their data might be shared by a third party, and 17.53% said mistrust of ITS.

On whether the university should store data in their servers of all internet and email traffic, 64.95% said no, 23.71 said yes, 11.34 said they did not care. When asked about how long the university should keep the data, 87.18% said they want their data stored for less than 3 months, 5.13 for more than 3 months, and 7.69% forever.

ITS has access to users' passwords, and in case a user forgets their password, ITS sends the original password to the user and advise his/her to change it. When asked about whether ITS should have access to the password or only be able to reset it, 79.17% said they did not want ITS to have access to the password, 12.50% said ITS should have access, and 8.33% did not care. As a technical solution to this problem, many information technology departments set up their systems to allow their staff the right to reset the password and not the right to access and know what it is. When asked if such option would be desirable at AUI, 64.21% agreed, 32.63% disagreed, and 3.16% did not care.

The survey asked whether respondents would agree that AUI administration shares users' private information with a third party without users' consent. The majority of the respondents 87.50% said no, 9.38% said yes, and 3.13% said they did not care. When asked if the personal information is provided to the police, 57.73% were alarmed, 18.56% were very concerned, 19.59% concerned, 3.09% were not concerned, and 1.03% did not care.

On the question of whether the administration should have access to internet browsing history, 86.60% said the university should not have access, and 7.22% said it should, 6.19 said they did not care. On the question of whether ITS can use students' data without their consent and without any legal obstacle…

The percentage of respondents who agreed or strongly agreed to have a privacy policy on campus was respectively 50% and 39.58%. There were 10.42% of respondents who strongly

disagreed. In response to the question about whether AUI students would feel empowered if a privacy policy is in place, 90.72 % agree with 44 % said they agree and 46.72% said they strongly agree. Those who disagreed were 4.12% and strongly disagreed were 5.15%.
On the question of whether the internet is a right of access to a public facility or a service offered by the university, 74.23% believe the internet to be a right and 25.77% believe the internet to be a service.

Of the percentage of students who believe the internet is a service, 24% strongly agree and 12% strongly disagree with the fact of having a policy. Of the percentage of students who believe the internet to be a right, 44% strongly agree and 10% strongly disagree with the fact of having a policy. What this implies is that those who believe access to the internet to be a right to a public facility expressed more concern for their right to privacy, as opposed to those who believe the internet to be a service offered by the university.

7.2. Interviews:[iv]

The interviewees all agree that privacy is very important and that a privacy policy is needed as a control mechanism to foster more accountability. They also agreed that all actions and policy decisions must involve all stakeholders. The findings can be divided into four broad categories: privacy and security in higher education, data security at AUI, the pragmatics of data privacy management, and privacy as a constitutional right in a non-democratic political environment.

Category 1: Privacy and security in higher education
The interviews raised broader privacy issues related to computer security within higher education institutions. Universities are centers of knowledge, research, discovery and intellectual exploration. Professors and students share their knowledge with each other and with other colleagues in universities all around the world. Information is a valuable asset in universities where intellectual property is developed. Intellectual property can be transformed into valuable products like computer programs or medical treatments and are therefore valuable and highly sensitive. Institutional cultures of universities promote open access to information which is necessary for creating opportunities of learning and research collaboration, and allows students and faculty to log in to the university system with their computers. This openness makes university systems harder to secure from outside threats. Faculty expressed serious concerns about what ITS is doing to provide such security for documents such as pre-publication research results, patented information, classified research, and research data.

Faculty also raised concerns about other less sensitive and yet very valuable information such as exams and grades. For instance, intercepting an exam while it is sent to a public printer may result in serious breaches in the whole integrity of the evaluation process. Some faculty members also keep records of their families and their children, such health and financial information. While the university may protect such information from outside intrusions, they have expressed concerns about access to such information from within the university.

Category 2: Data security at AUI

One main concern discussed with the interviewees is data storage, retention, and retrieval. ITS keeps users' data stored in their servers after students' graduation or after termination of employment of faculty or staff. Data on the N-drive and users' emails are kept for an undetermined period of time as no formal policy has been adopted with this regard. According to Mr. Ktif and Mr. Cherif, two ITS staff members, keeping the data has proven to be useful. Students, faculty, and staff who left the university have in the past requested access to some of their documents on the N-drive or to some of their emails, and ITS was able to provide them with this information. The request for data retrieval has to be made by the person him/herself and must show proper identification; otherwise the data is not retrieved. Mr. Ktif and Cherif also added that even the university administration does not have the right to access students' emails or N-drive data unless the student concerned agrees to it. "This has so far been the practice," Mr. Cherif adds, "there is no policy to support the practice."

However, according to Mr. Iraqi, a current faculty and former ITS manager, there is no policy on data storage, retention, and retrieval. ITS has designed a procedure for retrieving private data but does not have a policy on what type of data to store, for how long, and who is authorized to access it. For example, the fact that ITS does not hand over information to administration without the user's permission is not based on a written policy. If the administration choses to challenge this decision for whatever reason, ITS will find it very difficult to respond to the challenge.

Category 3: the pragmatics of data privacy management

Three interviews were conducted with two former and one current ITS directors. These interviews provided valuable insights from the perspective of information and data managers into all the privacy concerns raised in the students' survey and the faculty interviews. The main argument is that while they recognize the need for a policy and the need for more awareness and training in matters of privacy, there are pragmatic reasons for why someone has to manage data to ensure proper operations of the University information systems. Somebody has to be able to backup data, generate consistency reports, manage the email system, and other tasks. The nature of the technology makes it impossible to do these operations without having access to the data themselves, including root/administrator privileges to access passwords. Unfortunately, the systems cannot be managed without these privileges.

The interviewees also argued that the notion of privacy should not be limited to digital data. Private data dealing with enrollment, academic, financial information are also handled by the Admissions and Enrollment Services and the Business Office. They admit that the scope is different since digital data is easy to access and to move. For them, policies are important as control mechanism and to maintain a degree of accountability in the eyes of all the stakeholders. Policies help make good decisions that optimize the wellbeing of everyone. The privacy policy must be enforced through some kind of auditing mechanism; otherwise the policy will not fulfill the mission it was meant to fulfill.

The current ITS director said that the university is relatively young and has been working on many fronts to establish the needed structures. He added that the university administration has just approved a document that proves AUI's compliance with "the legal, regulatory and contractual requirements that are related to the design, operation, use and management of the University Information Systems" in Morocco. He said that it is time for a privacy policy for internal control to minimize risk.

Category 4: Privacy as a constitutional right in a non-democratic context
Some interviewees raised important issues related to the question of policies in general and privacy policies in particular in the framework of the overall political environment. When asked about Article 24 of the Constitution which provides guarantees for the protection of citizens' privacy, Mr. Gunn, a law professor, said that this article is not different from other articles that guarantee freedom of expression or the independence of the judiciary. In non-democratic countries, such constitutional guarantees do not translate into citizens' rights being protected. For example the media laws are very restrictive even if the constitution guarantees media freedom. Mr. Kabel, an education and linguistics faculty agrees that policies are important because institutions can be held accountable when they are found to have violated them. He adds, however, that the fact that "policies are systematically violated undermines their whole purpose."

8. Analysis
From a human rights based approach, internet users must be empowered to know and claim their rights as well as participate in shaping decisions that impact their lives. This approach also holds institutions and individuals responsible for protecting people rights to privacy and holds them accountable by setting up mechanisms of oversight and transparency.

The first important finding was the high level of concern the respondents expressed *vis a vis* their privacy. This is primarily due to the nature of convenient sampling method used, as the people who agreed to fill out the survey are mostly people who were primarily concerned about their privacy. However, the level of awareness about the extent of the university's access to their data was quite low. More than 40% of the respondents said they did not know that the university administration had access to their emails and to their passwords.

The study did not find significant correlations to draw between the gender, university level, students' majors and the responses to questions about awareness and concern over privacy. The most significant correlation we found is related to the perceptions of the internet as a service versus as a right, with the expressed need to an internet policy. The students who believe the internet to be a service also believe that there is no need for a privacy policy. And the students who believe the internet to be a right also believe that a policy on privacy must exist. In other words, when the internet is perceived as a service, internet use is perceived as any other service so the users cannot claim any rights other than those granted by the service providers. When the internet is perceived as a right, then users think of themselves as entitled to other services such as protection of their data and privacy.

It is therefore crucial to change the perception of the students because understanding that internet is a right of access to a public facility will have a better impact that will help us to raise awareness regarding the importance of the development of a new internet privacy policy. There is a small percentage of respondents who do not seem to care about their privacy. They must be people who believe that as long as I am not doing anything wrong, then I should not worry about anything. More education on privacy rights is therefore needed.

Based on the interviews, there is a lack of policies on data storage, retention, and retrieval. Internet users are exposed and their data may end up in the wrong hands. Policies and procedures play a significant role in helping institutions develop safe environments that are engaging and supportive. Policies are important as control mechanism and to maintain a degree of accountability in the eyes of all the stakeholders. Policies help make good decisions that optimize the wellbeing of everyone. The results from the survey also strongly confirm this need for policy.

The absence of a policy creates an environment of confusion and uncertainty, and that was expressed clearly by faculty concerned about their pre-publication research results, patented information, classified research, and research data. Some faculty members also keep records of their families and their children, such health and financial information. While the university may protect such information from outside intrusions, they have expressed concerns about access to such information from within the university.

The ITS is engaged in good practices when it comes to protecting users' data such as granting access to data only when the person consents with a show of proper identification. However, in the absence of a policy, ITS is in a weak position to defend the good practice if the university administration or a third party, for whatever reason, decides to challenge the practice.

To sum up, while the policy allows users in theory to have the ability, to Westin's phrase, to control when, how, and to what extent their personal information is communicated to others, it does not guarantee that their privacy is protected. A more holistic human rights based approach needs to be in place to ensure that users are empowered with knowledge of their rights and responsibilities, and to ensure that institutions create a culture that nurtures the values of privacy as a human right. In non-democratic countries where laws do not necessarily protect the rights they are supposed to protect, people must be proactive in the protection of their own privacy.

9. Conclusions and recommendations:

In order to create a safe environment that protects the privacy rights of the internet users within higher education institutions, all the stakeholders must be involved. The institutional culture of the university must nurture the values of privacy as a human right. Internet users must also take an active role in this process of protecting their data and must be educated about what they disclose when they interact online.

The first step is to establish a policy, AUI Users' Privacy Policy. The policy needs to be in line with the existing laws in the nation (Article 24 of the Constitution and Law 09-08). The purpose of the AUI Users’ Privacy Policy is to protect users’ data and to necessitate transparency. AUI through its Information Technology Services (ITS) must uphold the highest standards of transparency by imparting greater disclosure, accuracy, and clarity into their communications with all stakeholders. This policy is developed with the recognition that Internet technologies continue to develop and to evolve, and that such changes may require alterations to the current policy. Any such alterations must not affect AUI’s general commitment to the protection of Users' privacy.

In order for the institutional culture of the university to nurture the values of privacy, a short, medium and long term communication campaign needs to be in place that includes a variety of communication tools such as workshops, public presentations, and promotional materials of various sorts. The campaign must take place over the years as technology evolves and so do privacy rights violations. The campaign aims to increase awareness among internet users and educate them about how to take an active role in the protection of their own private data.

The privacy issues addressed in this paper as well as its recommendations are applicable in other workplaces. Internet users in any institution lose control over their private data while these institutions become empowered by the amount of private data they control. If we are to avoid a situation where the internet become a potentially repressive tool controlled the already more powerful (whether employers, governments, or big internet companies), we must not only carry out similar studies in other institutions but also engage our academic communities in discussions about privacy rights in the age of the internet.

References:

Andrews, U. (2014). Privacy and cookies. [online] https://www.st-ndrews.ac.uk/terms/cookies/ (accessed 9 March 2015).

Angst, C. & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339-370.

Bodle, R. (2011). Privacy and Participation in the Cloud: Ethical Implications of Google's Privacy Practices and Public Communications. In B. E. Drushel & K. M. German (Eds.), *The Ethics of Emerging Media* (pp. 155-174). New York, NY: The Continuum International Publishing Group.

Carothers, T. (2002). The End of the Transition Paradigm. *Journal of Democracy,* 13, No. 1: 5-21.

Culnan, M. & Bies, R. (2003). Consumer privacy: Balancing economic and justice considerations, *Journal of Social Issues* (59:2), pp. 323-342.

Fernback, J. & Papacharissi, Z. (2007). Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy polices. *New Media & Society, 9 (5),* 715–734.

Forcade, O. (2013). Une éthique commune va émerger en matière de renseignement. *Le Monde.* [online] http://www.lemonde.fr/societe/article/2013/10/31/olivier-forcade-une-ethique-commune-va-emerger-en-matiere-de-renseignement_3506527_3224.html (accessed 20 March 2015).

Greenwald, G. (2014). Why privacy matters [Online video file]. http://www.ted.com/talks/glenn_greenwald_why_privacy_matters (accessed 10 February 2015).

Greenwald, G., & MacAskill, E. (2013, June 6). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* [Online] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed 10 March 2015).

Harper, J. (2004). Understanding privacy—and the real threats to it. *Policy Analysis*, 520, pp. 2-17.

Levitsky, S. & Way, L. (2002) Elections without democracy: The rise of competitive authoritarianism, *Journal of Democracy*, 13(2), pp. 51–65.

Levitsky, S. & Way, L. (2010). *Competitive Authoritarianism*. *Hybrid Regimes after the Cold War*. Cambridge: Cambridge University Press.

Li, X., & Sarkar, S. (2006). Privacy Protection in Data Mining: A Perturbation Approach for Categorical Data, *Information Systems Research,* (17:3), pp. 254-270.

Madani, et. al. (2012). *The 2011 Moroccan Constitution: A Critical Analysis*. International Institute for Democracy and Electoral Assistance. Stockholm, Sweden.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research,* (15:4), pp. 336-355.

O'Donnell, G. & Schmitter, P. (1986) *Transition from Authoritarian Rule: Tentative Conclusions about Uncertain Democracies*. Baltimore: John Hopkins University Press.

O'Donnell, G. 1996. Illusions about consolidation. *Journal of Democracy,* 7, No. 2: 34-51.

Payton, T., & Claypoole T. (2014). *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Lanham, MD: Rowman & Littlefield.

Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM, 50 (9),* 103–108.

Rundhovde, H. (2013). I am not that interesting: Social media, privacy literacy, and the Interplay between knowledge and experience (Master's thesis). *University of Bergen, Norway*.

Schneier, B. (2013). Power in the Age of the Feudal Internet. *Multi-stakeholder Internet Dialog (MIND)*, *6*, 16-20.

Schneier, B. (2014). NSA Surveillance and What To Do About It. [Online video file]. Retrieved from https://www.youtube.com/watch?v=3v9t_IoOgyI (accessed 15 February 2015).

Solove, D. (2011*). Nothing to Hide: The False Tradeoff between Privacy and Security*. *New Haven, CT.: Yale University Press*.

Ward, S., Bridges, K., & Chitty, B. (2005). Do Incentives Matter? An Examination of On-Line Privacy Concerns and Willingness to Provide Personal and Financial Information, *Journal of Marketing Communications* (11:1), pp. 21-40.

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

[i] Loi 09-08 (Law 09-08), [online], http://www.cndp-maroc.org/images/lois/Loi-09-08-Fr.pdf (accessed 14 July 2015).

[ii] This is a data storage solution offered by ITS for AUI students, faculty and staff to keep their files.

[iii] Jenzabar is a student and faculty information management system.

[iv] Interviews conducted in April 2014 with faculty members: Jack Kalpakian, Ahmed Kabel. Jeremy Gunn; ITS staff: Hamid Harroud (director), Rachid Ktif, Ait Moulay Cherif; and two former ITS directors and current faculty: Tajeddine Rachidi Omar Iraqui.