



The 9th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, November 14th 2014



**MANAGING INFORMATION RECOURCES IN AN
ORGANIZATION. A PERSPECTIVE UPON ITS MASS
MEDIA EXPOSURE**

Totladze Giorgi

Ministry of Defence of Georgia / Department of Information Technology / Tbilisi /
Georgia

Abstract:

The purpose of this work is to find out what is information resources in the 21st century, how we can manage it, how it can be transformed into strategic resource rather than overload to give competitive advantage over others and achieve the goals of organization.

The work also tries to define and show us what challenges we will face to due to the increasing role of information resources. And this challenge is represented by mass media, and to be more precise, by online social networks.

Online social networks are discussed from the perspective of the employer and employee in terms of security and privacy invasion, employability and finally some recommendations are suggested.

1. Introduction

Information Resource Management - (IRM) A philosophical and practical approach to managing government information. Information is regarded as a valuable resource which should be managed like other resources, and should contribute directly to accomplishing organizational goals and objectives. IRM includes (1) identification of information sources, (2) type and value of information they provide, and (3) ways of classification, valuation, processing, and storage of that information.

Information resource management (IRM) has been with us for almost three decades. Numerous articles and monographs have been written about this interesting unconventional field of management. This paperwork serves to defining information resources, managing it and some issues that organizations should be concerned about in terms of security issues against its mass media exposures. Information explosion, reducing papers and extensive use of information handling technologies are examined as causes for the inception of IRM. As any other concept IRM had to be put to the test through its use in government and military sectors, as well as in private business.

Coin has two sides, so has the IRM. From one side it has a large economy of scale, it can be effective and efficient, can provide one with competitive advantage upon others and etc... but on the other side, it must be managed, protected and controlled.

Problems, challenges and some moot points connected with mass media exposure will be discussed below in terms of "second side of the coin", some experiments and vision will be shown to provide us with a motive for critical thinking towards privacy and security issues which seems quite harmless at a glance.

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

2. Information recourses

One of the dilemmas facing 21st century's manager is that on the one hand they seem to be suffering from information overload, but on other hand, there are lack of proper information and they often complain about shortage of information needed to make vital decisions.

Symptoms of overload are a growth of incoming information, including electronic mail, an explosion in the volume of information sources (there are over 10,000 business newsletter titles and a similar number of CD-ROM titles). Symptoms of scarcity are the lack of vital information for decision making, unexpected competitor moves and the inability to find the relevant 'needle in the haystack'.

2.1 Information as a strategic asset

There is also the crucial problem of exploiting an organization's proprietary information as a strategic asset.

Underlying these problems is that of having "the right information, in the right place, in the right format, at the right time".

If we have the information in the above mentioned manner, we can freely call these information as a strategic resource.

3. Security policy/issues

Consider that everything is ok with the above mentioned issues, what another problem can be found?

"Over the last 16 months," - says Glenn Greenwald – "as I've debated this issue around the world, every single time somebody has said to me, "I don't really worry about invasions of privacy because I don't have anything to hide." I always say the same thing to them. I get out a pen, I write down my email address. I say, "Here's my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting. After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." [1]

As Glenn Greenwald tells us not a single person has taken him up on that offer. He was checking that email account religiously all the time. He had no e-mail received to that regard. And of course there's a reason for that, which is that we as human beings, even those of us who in words disclaim the importance of our own privacy, instinctively understand the real importance of it. It is true that as human beings, we are social animals, which means we have a need to share the information about what we know what we are doing and saying and thinking to other people, which is why we voluntarily publish information about ourselves online. But there is another point equally essential to what it means to be a free and fulfilled human being is to have a place that we can go and be free of the judgmental eyes of other people. There's a reason why we seek that out, and our reason is that all of us — not just terrorists and criminals, all of us — have things to hide. There are all sorts of things that we do and think that we are willing to tell our physician or our lawyer or our psychologist or our spouse or our best friend that we would be mortified for the rest of the world to learn. We make judgments every single day about the kinds of things that we say and think and do that we're willing to have other people know, and the kinds of things that we say and think and do that we don't want anyone else

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

to know about. People can very easily in words claim that they don't value their privacy, but their actions negate the authenticity of that belief.

4. Mass media

The mass media are diversified media technologies that are intended to reach a large audience by mass communication. The technologies through which this communication takes place varies. Broadcast media such as radio, recorded music, film and television transmit their information electronically. Print media use a physical object such as a newspaper, magazine, book, pamphlet, flyer or comics, to distribute their information. Outdoor media is a form of mass media that comprises billboards, signs or placards placed inside and outside of commercial buildings, sports stadiums, shops and buses. Other outdoor media include flying billboards, blimps, and skywriting. Public speaking and event organizing can also be considered as forms of mass media. The digital media includes both Internet and mobile mass communication. Internet media provides many mass media services, such as email, websites, blogs, and internet based radio and television. Many other mass media outlets have a presence on the web, by such things as having TV ads that link to a website, or distributing a QR Code in print or outdoor media to direct a mobile user to a website. In this way, they can utilize the easy accessibility that the Internet has, and the outreach that Internet affords, as information can easily be broadcast to many different regions of the world simultaneously and cost-efficiently.

4.1 Mass media differentiation

Mass media contains: Radio, Television, Newspaper, pamphlet, billboards, internet and etc.

4.2 Social networks

I would like to concentrate on the internet based mass media means, such as online social networks.

A social networking service is a tool to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services for example online games, surveys and etc. Social networks are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network.

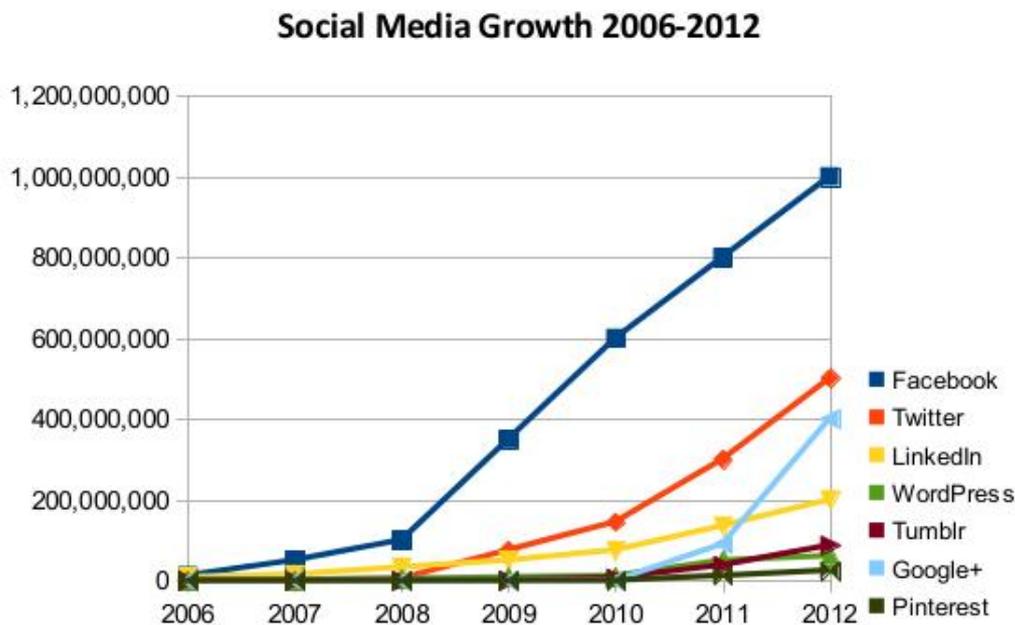
The main types of social networking services are those that contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages), and a recommendation system linked to trust. Popular methods

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

now combine many of these, with American-based services such as Facebook, Google+, YouTube, LinkedIn, Instagram, Pinterest, Vine, Tumblr, and Twitter.

There have been attempts to standardize these services to avoid the need to duplicate entries of friends and interests (see the FOAF standard and the Open Source Initiative. A study reveals that India has recorded world's largest growth in terms of Social Media users in 2013. A 2013 survey found that 73% of U.S adults use social networking sites.

The graph bellow (Fig.1) shows its importance and diffusion:



<http://www.dstevenwhite.com>

Fig.1 Importance and diffusion

5.Privacy

Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators. Users of these services also need to be aware of data theft or viruses. However, large services, such as MySpace and Netlog, often work with law enforcement to try to prevent such incidents.

In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, fatal to an individual, may be taken.

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

Furthermore, there are some problems over the control of data—information that was changed, deleted or removed by the user may in fact be retained and passed to third parties. This danger was highlighted when the controversial social networking site Quechup harvested e-mail addresses from users' e-mail accounts for use in a spamming operation.

In medical and scientific research, asking subjects for information about their behaviors is normally strictly scrutinized by institutional review boards, for example, to ensure that adolescents and their parents have informed consent. It is not clear whether the same rules apply to researchers who collect data from social networking sites. These sites often contain a great deal of data that is hard to obtain via traditional means. Even though the data are public, republishing it in a research paper might be considered invasion of privacy.

Privacy on social networking sites can be undermined by many factors. For example, users may disclose personal information, sites may not take adequate steps to protect user privacy, and third parties frequently use information posted on social networks for a variety of purposes. "For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information".

Following plans by the UK government to monitor traffic on social networks schemes similar to e-mail jamming have been proposed for networks such as Twitter and Facebook. These would involve "friending" and "following" large numbers of random people to thwart attempts at network analysis.

Privacy concerns have been found to differ between users according to gender and personality. Women are less likely to publish information that reveals methods of contacting them. Personality measures openness, extraversion, and conscientiousness were found to positively affect the willingness to disclose data, while neuroticism decreases the willingness to disclose personal information.

6. Impact on employability

Social networking sites have created issues among getting hired for jobs and losing jobs because of exposing inappropriate content. Social networking sites are places on the Internet where users can update their statuses and express their personal opinions about life issues to their friends. This is controversial because employers can access their employee's profiles, and judge them based on their social behavior. According to Silicon Republic's statistics, 17,000 young people in six countries were interviewed in a survey. 1 in 10 people aged 16 to 34 have been rejected for a job because of comments on an online profile. This shows the effects that social networks have had on people's lives.

There have been numerous cases where employees have lost jobs because their opinions represented their companies negatively. In September 2013, there was a case when a woman got fired over Facebook because she posted disruptive information about her company stating that military patrons should not receive special treatment or discounts. A manager of the company found her opinion online, disagreed with it, and fired her because it completely went against the companies' mission statement. In November 2012 there was a case in which a woman posted a racist remark about the President of the United States and mentioned content about a possible assassination. She lost her job, and was put under investigation by the secret service.

MANAGING INFORMATION REOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

Not only have employees lost their jobs in the United States, but it has happened with social network users internationally. In April 2011, a Lloyd's banking group employee in the United Kingdom was fired for making a sarcastic post about the higher salary of her boss in relation to hers. In February 2013 there was another case where a flight attendant working for a Russian airline lost her job because she posted a photo of herself giving the middle finger to a plane full of passengers. The photo went viral exposing it all over the Internet. In November 2009, a women working for IBM in Quebec, Canada, lost her company's health insurance benefits because she posted photos displaying her mental health problem. The company decided to cut her benefits because it was costing them additional funds.

Incidents like these have provoked that some privacy policy implications needed to be implemented to clear up whether companies have the right to see and inspect their employee's profiles. In March 2012, according to the announcement, Facebook decided they might take legal action against employers for getting access to employee's profiles through their passwords. According to Facebook's high officials, the company has elaborated some tools enabling Facebook users to control and check up who sees their profiles and information on it. According to Facebook Chief Privacy Officer for policy, Erin Egan, online social network's users shouldn't be obliged to share/provide with private information to the their potential employers' to get a job. According to the network's Statement of Rights and Responsibilities, sharing or soliciting or insisting to get a password is a violation to Facebook. Some people may still provide their potential employer's with their password information to get a job, but according to Erin Egan, Facebook will continue to do their best to protect the privacy and security of their users.

6.1 Top 10 Reasons Employees Get Fired

Because of some problems of privacy invasions, checking and inspecting employees' profiles and private information, some reasons of firing employees' have been revealed and highlighted. The list below shows some common reasons of terminating an employee from a job:

1. Damaging the property of the organization
2. Drug or alcohol possession at work
3. Falsifying organization records
4. Insubordination
5. Misconduct
6. Poor performance
7. Stealing
8. Using company property for personal business
9. Taking too much time off
10. Violating company policy

6.2 More Reasons for Termination of Employment

There are many reasons that companies fire employees. If you take a look at the stories about getting fired shared by About.com readers you'll find a variety of reasons people were fired from their job, including for posting on Facebook and some other activities related to the online social networks.

To take a better look in terms of online social network activities as a reason for termination of employment, the figures bellow will give us better opportunity for that.

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

Surveys report on the following reasons employers have terminated an employee from a job:

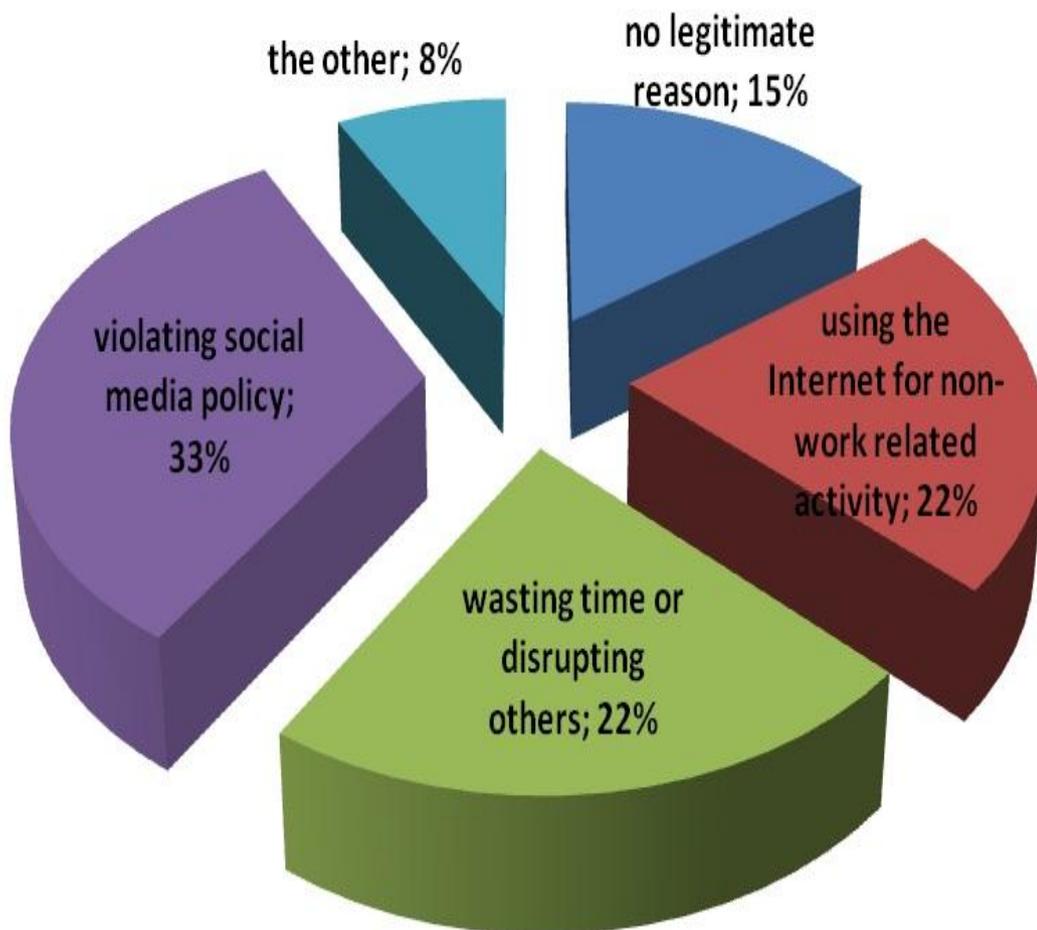
15% of employers have fired a worker for calling in without a legitimate reason (CareerBuilder);

22% of employers have fired someone for using the Internet for non-work related activity (CareerBuilder);

22% of employees know someone who has been fired for wasting time at the office or disrupting other employees (SHRM);

33% of employers have disciplined an employee for violating social media policy (SHRM).

The chart bellow (Fig.2) shows these figures:



<http://jobsearch.about.com/od/firedtermination/a/reasons-for-getting-fired.htm>

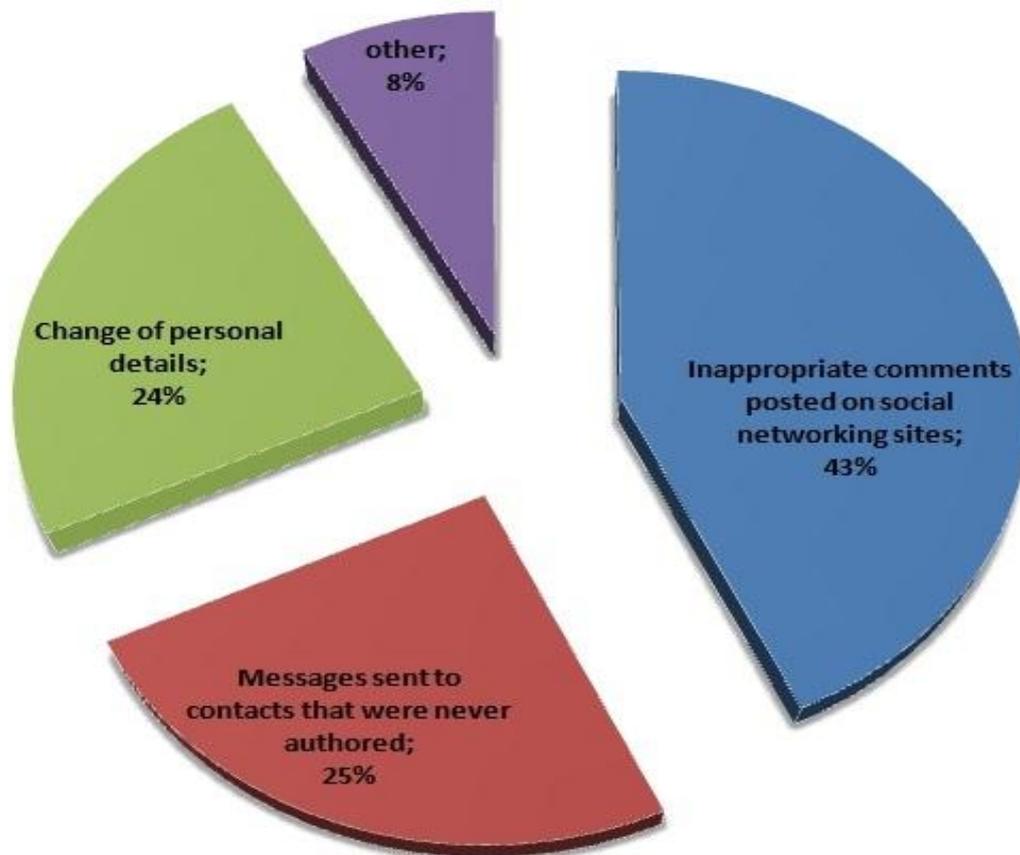
Fig.2 Reasons employers have terminated an employee from a job

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

7.Unauthorized access

There are different forms where user data in social networks are accessed and updated without a user's permission. One study highlighted that the most common incidents included:

1. Inappropriate comments posted on social networking sites (43%),
2. Messages sent to contacts that were never authored (25%)
3. Change of personal details (24%).



<http://www.wikipedia.org/>

Fig.3 Forms where user data in social networks are accessed and updated without a user's permission

The most incidents are carried out by:

1. The victim's friends (36%)
2. Partners (21%)

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

One in ten victims say their ex-partner has logged into their account without prior consent. The survey found that online social network accounts had been subject to unauthorized access in 60 million cases in 2011.

8. Recommendations

Many companies have social networking policies that forbid the use of social networking sites at work, that prohibit posting proprietary company information online, and/or that limit what employees can say online.

8.1 What Not to Post On Social Networking Sites

Posting confidential company information, even if it's good or bad news, posting that you do not like your job or you have a job offer you're going to take even though it's not a great job, posting inappropriate information on Facebook, tweeting that you have a job offer while still employed, are just a few examples of what can get you in trouble, or cost you your job or a job offer.

Companies aren't just worried only about what you post, even though that's important. They are also concerned about the time you spend for posting. Employee productivity is a problem when employees are Facebooking, Tweeting, watching YouTube videos, and doing anything else other than working.

Simply using your work computer for any personal and private business can be a problem if your company has guidelines and internal regulations on computer use on the job.

Dan Prywes, an expert in labor and employment law and a partner in the Washington, D.C. office of Bryan Cave, explains that "Employers are within their rights to limit social networking site access and resume posting and you need to be prepared for the consequences when you post online."

Employers have the right to control your computer and check what's on it, because it's not really yours - it is the property of the company.

8.2 Violating Company Social Networking Policy

Facebook continues to be an issue and an employee time waste, despite all the warnings about carefully using the privacy settings. Even updating your status from work can violate company policy if you're not supposed to be using Facebook in the office.

Twitter is an issue too. Every tweet shows up in Google, so it's easy to see what you're posting. Blog posts show up on the search engines, too, so be cautious what you say when you blog.

LinkedIn can be problematic, as well, even though it's a professional networking site. There was one person who was fired ahead of schedule because he shared the news that he had received a warning with all his contacts on LinkedIn. That news got relayed to his boss and he was out of a job sooner rather than later.

Another person received a warning from his Human Resources Department because he gave a former colleague a reference on LinkedIn. Company policy prohibited references and Human Resources construed his referral to be a violation of that policy.

8.3 If You Are Fired

What can you do if a company withdraws a job offer or fires you because of what you posted? Not much. Most states are "employment at will" meaning that the company doesn't need a reason to terminate your employment.

MANAGING INFORMATION RECOURCES IN AN ORGANIZATION. A PERSPECTIVE UPON ITS MASS MEDIA EXPOSURE

Employers are not required to provide a reason or explanation when terminating an at-will employee.

Public posting of your resume or posting the "wrong" information online can cost you your job and getting fired can make it harder to get another position. Rather than setting yourself up for possibly losing your job, take care in what and how you post information online.

9. Conclusion

As discussed above, privacy matters as for the organizations (no matter public or private sector) as for the employees itself, so taking into consideration what side affects can have our "ordinary activities" on social networks, each person and organization should be very careful and protect itself not only with some technical means, but by realizing its pros and cons. Before making some international or national regulations and legislative frameworks or guidelines, which will regulate this "cyber world" of information technology and its mass media exposure, we should only rely on the common sense, best practices and taking risks of the uncertain future.

References:

- [1] Glenn Greenwald, Why privacy matters, TEDGlobal 2014 · 20:37 · Filmed Oct 2014
- [2] Ruth Stanat, The Intelligent Organization, "Drowning in data, yet starved of information"
- [3] <http://www.wikipedia.org/>
- [4] <http://dstevenwhite.com/2010/08/08/social-media-growth-from-2006-to-2010/>
- [5] <http://jobsearch.about.com/od/firedtermination/a/reasons-for-getting-fired.htm>
- [6] <http://jobsearch.about.com/od/onlinecareernetworking/a/violating-company-social-networking-policy.htm>
- [7] Gary D. Blass et al. "Finding Government Information: The Federal Information Locator System (FILS)", Government Information Quarterly, JAI Press, Inc., Greenwich, Connecticut. Vol. 8, No. 1, pp. 11-32. 1991
- [8] <http://www.businessdictionary.com/definition/information-resources-management-IRM.html>