Profiling Online Social Networks Users as an Omniopticon Tool

Miltiadis Kandias, Lilian Mitrou, Vasilis Stavrou, Dimitris Gritzalis

INFOSEC Laboratory, Dept. of Informatics
Athens University of Economics and Business
76 Patission Ave., GR-10434, Athens, Greece

kandiasm@aueb.gr, l.mitrou@aegean.gr, stavrouv@aueb.gr, dgrit@aueb.gr

Abstract: Online Social Networks and Media indicate and incorporate the shift to interpersonal, horizontal and mutual communication and, thus information aggregation. Online content of interest (namely, YouTube videos and comments or Tweets), along with online relations (friendships, followings, mentions, comments, etc.), may be collected and utilized for a variety of purposes. In our previous research we have demonstrated that it is possible and potentially trivial (by utilizing a simple personal computer and a broadband internet connection) to extract personal sensitive information such as political beliefs and psychosocial characteristics (such as narcissism and predisposition towards law enforcement) about Online Social Networks (OSN) users in an automated manner. Web 2.0 technological features combined with voluntary exposure to an indefinite audience in OSNs give rise to traditional surveillance as Government is enabled to connect the dots, combine information about political beliefs and every-day activities and generate mass user profiles on the base of identifying patterns. Despite the lack of centralized control over the Internet, its platforms and applications allow multilevel and latent surveillance, thus posing new risks for individuals by forming new power relations and asymmetries. Our research highlights how Web 2.0 and OSNs (YouTube and Twitter) may become a topos of participatory panopticism, an omniopticon in which the many watch the many and can reconstruct sensitive information out of seemingly anonymous data/content. Individuals may be confronted with social exclusion, prejudice and discrimination risks both in their workplace and in their social environment. In our paper, we focus on the results of this type of surveillance that facilitates the exculpation of such penetrating and privacy-violating technologies and amplifies the threshold of societal tolerance towards a panopticon-like state of surveillance. Furthermore, we analyse and discuss implications of data mining as data processing with focus on the new European law and the legal framework in the US.

Keywords: Social Media, Profiling, YouTube, Twitter, Panopticon, Omniopticon, Ethics, Surveillance.

Biographical notes: Miltiadis Kandias is a Researcher with the Information Security and Critical Infrastructure Protection Laboratory (Infosec Lab) of Athens University of Economics and Business (AUEB), Greece. He holds a BSc in Informatics and Telecommunications from the University of Athens and an MSc in Information Systems from AUEB. Currently, he is a PhD candidate at AUEB in the field of Security Data Science. His research focuses on the extraction of psychosocial characteristics on an individual basis exploiting Open Source Intelligence techniques.

Lilian Mitrou is an Associate Professor at the Dept. of Information and Communication Systems Engineering of the University of the Aegean, Greece, and a Visiting Professor at Athens University of Economics and Business. From 1998-2004 she was the national representative in the EC-Committee on the protection of individuals with regard to the processing of personal data. Her professional experience includes senior consulting and researcher positions in private and public institutions. Her research interests focus on privacy and data protection, e-Democracy and e-Government services, and Internet Law. She has published extensively in journals, books and conference proceedings.

Vasilis Stavrou is a Researcher with the Information Security and Critical Infrastructure Protection Laboratory (Infosec Lab) of Athens University of Economics and Business (AUEB), Greece. He holds a Diploma in Computer Engineering from the University of Patras, Greece, and an MSc in Information Systems from AUEB.

Dimitris Gritzalis is Associate Rector and a Professor of IT Security at the Dept. of Informatics of Athens University of Economics and Business, Greece. He is, also, the Director of the Information Security and Critical Infrastructure Protection (Infosec) Laboratory, and the Director of the MSc Programme in Information Systems. He holds a BSc degree (Mathematics, Univ. of Patras), an MSc (Computer Science, City University of New York) and a PhD (Critical Information Systems Security, Univ. of the Aegean). His current research interests focus on Information Security, Critical Infrastructure Protection and Social Media Intelligence. He has served as Associate Commissioner of the Greek Data Protection Commission and as the President of the Greek Computer Society.

1 Introduction

Web 2.0 technologies have facilitated the interaction among communicating individuals, the ability to create, redistribute or exchange information and opinions online and also the participation in virtual communities. Moreover, the "average communicating individual" has become a content contributor/generator who interacts with other users along with the exchange of information. The term "user" reflects an approach in which the subject is acting on the basis of content generation or application usage. On the other hand, "communicating individuals" do generate content and use applications but they are characterized by certain intentions, emotions and motives. The environment of OSN (Kaplan, Andreas, Haenlein, 2010) is dominated by the "user-generated content", namely by information produced, received and disseminated by "non-professionals", in particular, but non only, through Online Social Networks (OSN). The paradigm of Internet has changed, i.e., from static and isolated repositories of information the Internet shifted to dynamic, user-driven and participatory sites.

Web 2.0 interactivity and applications allow or enable users to create online profiles as well as to share personal details and preferences (Boyd, 2007). OSNs define access to user-created content via social relationships, thus becoming also informal but all-embracing identity management tools (Piskopani and Mitrou, 2009). Communicating individuals reveal aspects of their personality and behavior in OSNs. By revealing aspects of their personality, communicating individuals engage in the self-construction of their identity (Albrechtslund, 2008); they form their personal identity in and through OSNs. "Users" are encouraged by the nature and the structure of OSNs to reveal and disseminate information, to produce, share or "comment" content, resulting to a "participatory culture" (Van Dijck, 2009).

Web 2.0 communication is undoubtedly a mass communication but not necessarily "a mass-self communication" as characterized by Castells (Castells, 2013), as the identification of potential receivers is not always "self-directed". Due to the nature of online social networking, individuals are exposed to a mass audience, even when they obviously communicate online with a specific audience in mind. When used to convey personal information or preferences, OSNs augment their users' visibility, not only to their chosen "friends" but also to other persons (as "friends" of "friends"), agencies and institutions. OSNs enable and facilitate information exchange between an indefinite number of "friends"/"users" (Marwick, 2012). By generating content in OSNs, individuals are generating information flows. Social networks and media indicate and incorporate the shift to interpersonal, horizontal and mutual communication and offer the ability to increase information aggregation. Through their participation, "users" produce persistent, replicable and searchable information (Boyd, 2007). Being "subjects in communication" users make their data available to others, thus becoming "objects of information" and, therefore, "objects of surveillance" (Fuchs, 2011).

Several inherent features of Internet (especially Web 2.0) supported technologies and platforms (e.g., digitization, availability, recordability and persistency of information, public or semi-public nature of profiles and messages) encourage not only new forms of interaction, but also novel surveillance tendencies via behavior and sentiments' detection and prediction. Any content uploaded online can be accessed, recorded, stored and retrieved "without respect for social norms of distribution and appropriateness" (Farinosi, 2011; Lange, 2007). Such sites and interaction platforms are, by design, destined for users to continually follow digital traces left by their "friends", "followers" or persons they interact with often by simply consuming or commenting user-generated content. As noted by Lampe et al., OSNs are founded on the premise of surveillance, where individuals are not only allowed but expected to "track other members of their community" (Lampe, Ellison and Steinfield, 2006).

While users' content visibility increases, the architecture of the majority of Web 2.0 applications allows exposing content to unwanted and/or invisible audiences. Moreover, if "Panopticon" creates a "consciousness of permanent visibility", Internet technology hides both, the possibility of surveillance, and the signs of what/who is monitored. This is true, although persons living in ubiquitous computing environments and acting in OSN contexts could assume (or accept, if not wish) that they will/could be monitored by everyone. If the metaphor of "Panopticon" offers the ultimate example of unilateral and vertical surveillance, Internet platforms and applications allow multilevel and latent surveillance, thus posing new risks for the rights of the individuals by forming new or reinforcing old power relations and asymmetries. Such information (a) symmetries co-define the playground/playfield between government/political actors and citizens or between employers and employees, thus affecting individual autonomy and participation to public sphere. The conscious or unconscious voluntary exposure of personal information to an indefinite audience gives rise both to the "traditional" and social panopticism (Nervla, 2010; Jurgenson, 2011), the Web 2.0 becoming slightly but definitely an ideal "topos" for "social surveillance" (Tokunaga, 2011; Marwick, 2012) and "participatory panopticism" (Whitaker, 1999), an Omniopticon, in which "the many watch the many" (Jurgenson, 2011).

The rest of the paper is organized as follows: in section 2 we quote the results of our research on profiling within Twitter (detection of narcissism) and YouTube (predisposition towards law enforcement and political affiliation detection). In section 3 we discuss the capabilities of OSN user/usage profiling. In section 4 we comment on the potential discrimination risks that arise from OSN profiling. In section 5 we discuss state surveillance parameters, while in the final section we develop our commentary over the capabilities offered by OSN for the so-called participatory panopticism.

2 OSN Profiling: Personality and Behavior Analysis

In our previous research we have demonstrated (Kandias et al., 2013, Gritzalis et al., 2014) how multifaceted information revealed and shared in OSNs can be utilized so as to predict the behavior of the employees via examining traits of predisposition of delinquent behavior and thus augment existing surveillance methods (Kandias et al., 2013). We have extracted conclusions over the users regarding the personality traits of narcissism (via Twitter) and predisposing towards law enforcement (via YouTube). It is also possible to extract those conclusions, along with group dynamics analysis and introversion.

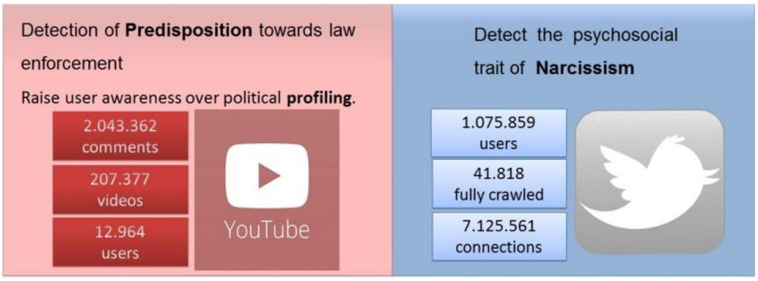
In order to show that this does not require considerable computational resources but, instead, it can be performed with limited resources thus trivializing surveillance potential/ arsenal, we performed our experiments on a Core2Duo processor (3GHz) and 4GB of RAM. That means that an individual willing to develop profiling algorithms is able to achieve it by solely using her personal computer revealing that it may generate a kind of ubiquitous social surveillance. In Table 1 we quote the time demanded so as to collect and process OSN generated personal data for a single, average user. The demanded time depicts the capabilities of mass surveillance since utilization of processing and bandwidth intensive technologies (namely cloud computing and distributed systems) would unlock the ability to monitor and classify large amounts of communicating individuals in a few seconds.

Table 1. Indicative time complexity for the classification of an average user

Social Medium	Average user (dataset based statistics)	Indicative crawling and classification time
Twitter	~200 followers, ~400 tweets	1-3 minutes
YouTube	~150 comments, ~50 favorite videos	3-10 minutes

We have applied our methodologies to two popular OSNs, so as to highlight the applicability and the success rate of such techniques. We, also, exploited the available data in OSNs in order to examine the ethical and legal issues that arise from such profiling methods and the emerging surveillance potential. We have chosen YouTube and Twitter to apply our methodology, as OSNs are popular among users and have already been used in the context of cyber security (Kandias, Virvilis and Gritzalis, 2013).

Figure 1 Testing environments


Detection of Predisposition towards law enforcement
Raise user awareness over political profiling.
2.043.362 comments
207.377 videos
12.964 users
YouTube
Detect the psychosocial trait of Narcissism
1.075.859 users
41.818 fully crawled
7.125.561 connections

2.1 Twitter: User Personality Detection via Metadata Analysis

The methodology that was applied to the Twitter case study aimed at enhancing the prediction capabilities of the trait of narcissism, by applying surveillance techniques. To demonstrate such a potential, we focused on a Greek community of Twitter, consisting of 1.075.859 users of which 41.818 are fully crawled, and 7.125.561 connections among them. We also used these methods to highlight the social and legal impact of such an approach. To this end, we used data crawled by Twitter, so as to analyze the collected users in a graph theoretic manner. Additionally, we identified connections between usage patterns and defined which users' behavior could be considered as deviating from the average usage behavior in the social medium. Thus, surveillance can be performed, not only by content analysis, but also by performing analysis on the way that users connect to each other into the world of OSNs. In this case study the collected data was used for prediction and deterrence purposes. Each user's date was analyzed with graph theory under the prism of usage deviation. The basic results that refer to the Greek Twitter Community indicated that: (a) the majority of the Greek users make poor use of the medium, (b) there are a lot of normally active users, and (c) very few users are popular.

In order to classify the users to certain taxonomy we utilized three parameters, user's influence valuation, her klout score and her usage intensity. User's influence is defined as the set of users who are possible candidates to adopt her words by retweeting them. The influential set of each user consists of: (a) followers who directly learn her quotes, (b) her mentioners, (c) re-tweeters who mention her or repeat her word of mouth, even without following her, and (d) the followers of her last two categories, as there is a possibility to learn about her indirectly. The klout score is a metric that represents someone's influence within the OSN. Finally, usage intensity is the weighted aggregation of: (a) number of followers, (b) number of followings, (c) number of tweets, (d) number of retweets, (e) number of mentions, (f) number of favorites, and (g) number of lists.

Based on the available data, we spotted a threshold above which the users may become quite influential and perform intense medium usage. Therefore, we defined a specific point where a user turns from a normal one to a "media persona". Research has proved that individuals tend to transfer their offline behavior online. Thus, more extravert individuals tend to form large groups and communicate easier in the territory of OSNs, while introvert individuals tend to communicate less (Skues et al., 2012). Furthermore, researchers have connected excessive usage of OSNs to the personality trait of narcissism (Buffardi and Campbell, 2008; Mehdizadeh, 2010). Thus, we proposed a general taxonomy of the Twitter users, the data of whom were crawled and analyzed. According to our findings, the most influential users' influence valuation is between 942 and 3604 and usage valuation is between 21.004 and 569.000. Based on this, users whose sum of the previous values is higher of the threshold of 22.000 are classified in a different category of the taxonomy. Furthermore, the majority of the users with usage valuation above 21.000 are either real life celebrities or news media. This leads us to assume that the "normal" users with high scores should belong to a different category. The proposed categories appear on Table 2.

The above findings reveal the potential abilities that monitoring and surveillance mechanisms offer. Hence, monitoring the usage behavior of a participant in an OSN may lead to revealing personal traits that can be (mis)used for several purposes. Regarding the impact such mechanisms offer, one may notice that they affect both legal and social aspects. Both, user's privacy and dignity, two fundamental rights are at stake

Table 2. Proposed Twitter user taxonomy

Category	Influence valuation	Klout score	Usage valuation
Loners	0 - 90	3.55 - 11.07	0 - 500
Individuals	90 - 283	11.07 - 26.0	500 - 4500
Known users	283 - 1011	26.0 - 50.0	4500 - 21000
News Media & Personas	1011 - 3604	50.0 - 81.99	21000 - 569000

2.2 YouTube: Behavior Analysis and Political Beliefs

The experimentation with YouTube user-generated content highlights the twofold nature of online surveillance. On the one hand, surveillance may contribute towards mitigating some threats by predicting personal traits that malevolent users have been found to share. On the other hand, such profiling techniques may well expose sensitive personal data, involving political affiliation, which may lead to social and workspace discriminations. To deploy these aspects of surveillance applied on YouTube, we have experimented with an extensive Greek community of YouTube and we have gathered a dataset of 12.964 fully crawled users, 207.377 videos, and 2.043.362 comments.

To draw conclusions over the political affiliation of the users we utilized machine learning techniques to categorize user-generated content. Current approach is based on text classification which a valid methodology developed by computer and information science in order to categorize text content into predefined categories of interest. To do so, text classification facilitates machine learning and based on the procedure followed, the text content is assigned into the appropriate category it belongs to. Machine learning algorithms "learn" from the text examples they receive and construct underlying models that are able to determine the label of any text given as input. Label assignment requires the assistance of an expert, who can distinguish and justify the categories each text belongs to.

In order to examine user content we decided to examine YouTube's basic module, i.e. its videos. As we cannot examine the video per se, we decided to draw conclusions over its content based on its comments. Thus we utilize text classification to perform comment classification. To categorize comments into categories of interest we used the following classification algorithms: (a) Naïve Bayes Multinomial (McCallum and Kamal, 1998) (NBM), (b) Support Vector Machines (Joachims, 1998) (SVM) and (c) Multinomial Logistic Regression (Anderson, 1982) (MLR). Furthermore, we compared the results and picked the most efficient classifier.

Classifier's efficiency comparison was based on the metrics of precision, recall, f-measure and accuracy (Manning et al., 2008). These metrics derive from the field of information retrieval and facilitate the choice of the most appropriate classifier. More specifically, accuracy measures the number of correct classifications performed by the classifier. Precision measures the classifier's exactness. Higher and lower precision means less and more false positive classifications (the comment is said to be related to the category incorrectly) respectively. Recall measures the classifier's completeness. Higher and lower recall means less and more false negative classifications (the comment is not assigned as related to a category, but it should be) respectively. Precision and recall are increased at the expense of each other. That is why they are combined to produce the f-score metric that is the weighted harmonic mean of both metrics. F-score may facilitate the classifier selection process, as picking a classifier solely based on precision or recall may lead to more or less false positive (and false negative) classifications regarding the scope of the study. Thus, a more weighted combination (i.e. the f-score) leads to a balanced rate of false positives and negatives.

Table 3. Classification algorithms metrics comparison 1 – Political profiling

Metrics									
Classifier	**NBM**			**SVM**			**MLR**		
Classes	**R**	**N**	**C**	**R**	**N**	**C**	**R**	**N**	**C**
Precision	65	93	55	75	91	74	83	91	77
Recall	83	56	85	80	89	73	77	93	78
F-Score	73	70	60	76	89	73	80	92	77
Accuracy	68			84			87		

By using comment classification we were able to categorize comments into one of the following (indicative) categories, i.e. radicals (R), conservatives (C) and non-political (N) content according to specific metrics (Table 3). Multinomial Logistic Regression achieves better precision value and SVM better recall value. Multinomial Logistic Regression achieves a slightly better f-score assessment. Support Vector Machines and Multinomial Logistic Regression achieve similar results regarding both recall and precision metrics. As a result, we chose Multinomial Logistic Regression because of the better f-score value achieved for each category.

The same methodologies were applied to the dataset, in order to extract conclusions and classify users into predefined categories with respect to another psychosocial trait (i.e., predisposition towards law enforcement). User generated content is analyzed by the same algorithms and users are classified into two categories, those negatively predisposed towards law enforcement (P) and those who are not (N) (Table 4).

Table 4. Classification algorithms metrics comparison 2 – Predisposition towards law enforcement

Metrics						
Classifier	**NBM**		**SVM**		**LR**	
Classes	**P**	**N**	**P**	**N**	**P**	**N**
Precision	71	70	83	77	86	76
Recall	72	68	75	82	74	88
F-Score	71	69	79	79.5	80	81
Accuracy	70		80		81	

The above results show that user profiling may lead to gaining probabilistic knowledge regarding user's OSN usage pattern. Such knowledge may be able to predict potential threats and protect critical infrastructures, such as hospitals, power plants, governmental organizations and military organizations from malicious employees. However, it could be used for the revealing of sensitive personal data and increase the surveillance arsenal/instrumentarium while exposing citizens and employees to discriminative practices. Otherwise, user privacy is exposed to be exploited for discriminative purposes.

3 OSN as Personal Information Source

The combination of Web 2.0 technologies, user-generated content and the growth of ICT (data warehousing, data mining, broadband internet access etc.) has enabled fast and efficient processing of vast amounts of information. Thus, novel and invasive Open Source Intelligence (OSINT) techniques have been developed by researchers and practitioners along with military organizations in order to extract user/usage patterns and correlations between seemingly unrelated data (namely psychosocial characteristics and OSN usage patterns). OSINT (Steele, 2007) refers to intelligence collected from publicly available sources, such as websites, web-based communities (i.e. social networks, forums, blogs) and publicly available data. Such techniques facilitate the extraction of knowledge when this is not easily accessible.

From the point of view of surveillance goals, OSINT processes rely on vast amounts of reliable information. The more reliable the data, the more accurate and intrusive the analysis of the subject (the monitored subject could be anything, such as an event, a single person, a group of people or a collective sentiment over another subject). However, collected data are not always as reliable as demanded, especially in the case of processing vast amounts of data. Therefore, the problem that emerges is associated to the fact that a user may be assessed on the basis of unreliable and inaccurate data which are utilized out of context. To this extend the following key points must be taken into consideration, since the quality of the results of the surveillance is directly connected to the quality of the gathered data:

- Uncovering data location: It is required to have knowledge of the locations from where the appropriate data can be gathered.
- Sources pre-processing: The pre-processing of the useful and the irrelevant sources of information is important, so as to avoid collecting outdated or useless data.
- Results refining: After having generated conclusions over the subject of interest, it could be useful to further process the results in order to focus on the required knowledge and provide us with further analysis of the subject’s parameters. A process of meta-training on the collected data could reveal secret connections or correlations between the parameters of the dataset.

Moreover, even if the above key points are met, the decision process is based on probabilistic methodologies that do not produce deterministically accurate results. So a person or her online usage patterns may be classified into certain categories (similar to those quoted in the following sections) based on accurate data but in a probabilistic manner that does not exclude false positives/negatives. This means that the person is incorrectly classified to a category (false positive), or it is not classified to a category but it should have been (false negative).

The participatory nature of Web 2.0 and OSNs offers a source of personal data (suitable for OSINT techniques), which are available for collection and processing, even, without the user’s consent (or knowledge). Users’ data/user generated content in OSNs is publicly available, since most of the communicating individuals neglect to use any privacy mechanisms, even if offered, or they are not even aware of or wiling for. Even when users do not fail to utilize the offered privacy mechanisms, it is possible to obtain their data indirectly through “crawling”, namely the process of collecting web based data by utilizing automated techniques and specialized software. Therefore, one could gather personal information even without having legitimate direct access to the target’s online profile by crawling either the medium per se, or other users that communicate with the target user. Thus, the surveillance capabilities over the communicating individuals expand along with the posed threat to their privacy and the demand for broader user privacy awareness. So anyone interested in collecting such data could crawl OSNs in order to gather personal(ly) identifiable information and analyse it.

Although the processing of such data may be used for fair purposes, so as to provide the user with a more personalized user experience, user's privacy may be easily infringed. The knowledge extracted using OSINT may be utilized for purposes ranging from profiling for targeted advertising (on the basis of analysing online features and behaviour of the users) to personality profiling and behaviour prediction for purposes such as employee screening, counter intelligence, threat prediction or forensics analysis (Kandias et al., 2010; Mylonas, Kastania and Gritzalis, 2013; Mylonas et al., 2013; Shaw, Ruby and Post, 1998).

4 User Profiling and Discrimination Risk

People participate in OSNs for various reasons, such as amusement, communication and professional networking. As the number of communicating individuals participating in OSNs started to increase, research has focused on examining the way they behave in the digital world. One of the most important findings is that individuals tend to transfer their offline behavior online (Amichai and Vinitzki, 2010). This is supported by a series of evaluated hypotheses, which revealed correlations between specific psychological characteristics (namely, extroversion, neuroticism, agreeableness, openness) and OSN usage. The behaviour and personality profiling may uncover and analyse psychosocial traits such as introversion, social and personal frustrations, divided loyalty, entitlement/narcissism, and predisposition towards law enforcement, political beliefs and group dynamics. Such traits can be processed in an automated and flexible manner, making it possible to perform psychometric evaluations by utilizing the content a user has made publicly available.

The case studies have been performed in order to achieve a twofold purpose: (a) From the privacy enhancing perspective: For raising user awareness over privacy issues and exploitation of user online data, and (b) from the information systems security perspective: for revealing new methods for human factors threat prediction. Human factor on security forms a major issue in cyber-security, as former and current employees or business associates may use their insider information advantage to harm an organization. Tackling down such threats, especially as far as it concerns critical infrastructures, it is considered as a political and social priority. Human factor threat prediction can be further enhanced by examining personal traits that indicate predisposition of delinquent behavior through OSN (Shaw, Ruby and Post, 1998). Thus, such a surveillance may help identify usage behavior correlated to narcissism or to negative predisposition towards the law.

Examination of the datasets collected from YouTube and Twitter may result to risks inherent in every kind of profiling. With "profiling" we understand methods involving mining of data and automated classification that is likely to assign individuals to particular categories mostly in order to take decisions concerning or affecting them. The definition of profiling of the Council of Europe Recommendation (Council of Europe Recommendation, 2010) focuses on the creation or use of profiles to evaluate, analyze or predict personal aspects such as performance at work, economic situation, health, personal preferences, or interests, reliability or behavior, location or movements.

The ability to predict individual attributes and behavior raises major issues. Profiling ends up at treating a person as belonging to a specific category, which in turn indicates what "sort of person" someone is, the category becoming more important than the individual herself. Predictive data mining and profiling (e.g., flagging someone as potential threat, offender or inaccurate employee) results to classifications that may have considerable implications for an individual's well-being, freedom and rights (Kosinski, Stillwell and

Graepel, 2013). In a micro-social level, data mining of OSN content may lead to extended discriminations and prejudice against persons with far reaching consequences for their life (social exclusion, unemployment, etc.).

A visible risk to consider is the possibility for discrimination in the workplace: OSN profiles, blogs, tweets, and online fora are increasingly monitored by employers searching for information that may provide insight on employees and prospective hires. Taking into consideration the exponentially growing participation in OSN, it is not surprising that employers are searching for unique information about applicants and employees not found with other selection methods.

A broader and potentially less censored or more honest array of information is easily accessible on the Internet (Kandias et al., 2013). It appears that some employers prefer the presentation of the private "digital alter ego" of the candidate than the profile which has been elaborated for professional reasons (Keber, 2014). Such findings indicate that the once clear lines between the private and the public, as well as the employee's personal and professional life, are gradually blurring. This is a result of: (a) the "boundary-crossing technologies" (Sánchez Abril, Levin and Del Riego, 2012), (b) the transformation of workplace structure and ethos through ICT, and (c) the radical changes in communication. The openness and sharing culture that dominates the OSN reflects a population that does not construct communication on the traditional division between private and public contexts. In other words, the more private information has become easily accessible and infinitely shareable and transferable, the more monitoring may extent to private spaces, activities and time (Fazekas, 2004; Mitrou and Karyda, 2006). Methods may allow employers to collect and aggregate information that reflects behavior of the user and her interaction with other users in contexts totally different from this of the workplace, in order to produce relevant patterns/ profiles and anticipate future behavior and threats.

Employers argue that the security enhancement perspective against the malevolent insider or other threats includes the prediction of malevolent behavior that may cause catastrophic results, in particular when the security of critical infrastructures is jeopardized. Furthermore, exploitation of user generated content in OSNs may provide the employer with useful information about the psychological state of the users and traits of their personality, so as to improve the organization's productivity and the group's efficiency.

In this context, some argue that when one publishes something to all comers it is not reasonable to expect (current and future) employers respect her privacy and freedom of expression and refrain from judging her based on publicly available information (Sánchez Abril, Levin and Del Riego, 2012). In the US, surveys point out lifestyle concerns among the most common reasons for rejecting candidates (Broughton et al., 2009).

Employers are actually not prohibited to consider information about a person who is documented in publicly available OSN profiles, public posts or public Twitter accounts. Especially in U.S context, under the doctrine of "reasonable expectation of privacy" individuals have a quite limited expectation of privacy outside their home, where they have been traditionally allowed to conduct their life free from state surveillance. Quite recent jurisprudence of the U.S. Supreme Court (United States v. Jones, 2012) has extended this expectation also outside the "home-castle" or the "content of communications" ruling that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy". However, as far as it concerns the privacy on social media, information posted is potentially visible to all. Personal data revealed by an individual herself on OSN sites are regarded as accessible without being subject to specific procedural and substantial guarantees.

With regard to workplace privacy under the doctrine of reasonable expectation only a "minimal right to privacy", limited to those instances where the matter/area intruded upon is “intensely private”. Employees-privacy expectation and, thus, protection, are hardly-founded on constitutional and legal texts. On the other side in Europe respect for private life includes, to a certain degree, the right to establish and develop relationships with other individuals (Mitrou and Karyda, 2006). This approach puts limits to employer’s legitimate need for surveillance measures and use of personal data for other purposes than those originally collected or revealed for.

To highlight the difference between the choice for revealing voluntarily information in OSN profiles and the fact that some information may result as an outcome of crawling/-processing of user-generated content, one should note that the user cannot predict neither the exploitation of her personal data, nor the results of this process. As noted by Hull et al. (Hull, Lipford and Latulipe, 2011) information flows on social networking sites are mediated by the ways that those sites and their users interpret the meaning of online friendship and the social norms that go with it. Even in US, part of jurisprudence and legal doctrine accept a “limited privacy”, i.e., the idea that when an individual reveals private information about herself to one or more persons, she may retain a reasonable expectation that the recipients of the information will not disseminate it further (Strahilevitz, 2005). This approach is of importance in case that an individual disclose information related to herself in “non-public profiles”. Hence, both the wide availability of private information, as well as its use beyond the initial context that this information has been produced, may have far reaching effects for the employees’ rights and liberties.

As Nissenbaum (Nissenbaum, 2004) argues, the definitive value to be protected by the right to privacy is exactly the “contextual integrity” of a given contextual-self having different behavior and sharing different information depending on the context. Information gathered through OSN analysis is normally not only unintended as application information but often job-irrelevant or, moreover, related to sensitive activities and, therefore, information of the person concerned (religion, political beliefs, etc.) (Davison et al., 2012). A user data processing, without her consent, could lead to exposure of personal data of hers which could further lead to discriminations, conclusion extraction over sensitive personal characteristics and other inwardly characteristics of her behavior, sentiments and personality and affect her privacy, personality, and dignity.

5 OSN Data Mining and State Surveillance

OSNs and online services with user-generated content (such as Twitter or YouTube in our experiments) have made a staggering amount of information available to the government and public/ policy institutions. Online media and user generated content-mining provides support for decision makers to detect, track or even predict opinions and attitudes (Sobkowicz, Kaschesky and Bouchard, 2012). Political campaign information is supplemented by quite pervasive data gathering and mining in the context of social media too: inferences about political opinion and behaviour can be made by non-strictly political sources such as blogs, sites read or “likes”. In OSN environment the monitoring of citizens by political institutions, parties and candidates is reinforced both by the corporate policies and technical standards and defaults of the social media platforms they use and the sharing culture of users which is also encouraged by political institutions’ social media pages (Bennett, 2013). Social media and databases mining has played a very important role in the electoral campaigns in USA, one of the crucial parameters being the increasing capture of user-generated data from social media (Bennett, 2015). Despite privacy concerns “computational politics” in combination with “engineering of the public” (Tufekci, 2014) makes a critical part of designing and implementing a winning campaign. In Europe, collecting and processing data about political beliefs is regarded by law as a highly exceptional situation. Many international and national legal instruments prohibit explicitly the processing of personal data revealing political opinions (e.g. Art. 8 of the European Data Protection Directive and Art. 6 of the Convention 108 of the Council of Europe). Derogating from the prohibition on processing this “sensitive category” of data is allowed if done by a law that lays down the specific purposes and subject to suitable safeguards. Such derogations should rely on a manifest public interest or the explicit, informed and written consent of the person concerned.

Governments also seek to use the informational goldmine of online social media to extract implicit, previously unknown and potentially useful information and to discover or infer previously unknown facts, patterns and correlations (Rubinstein, 2012). Governments are interested in doing more than simply identifying individuals but furthermore in accumulating as much data about their citizens as they can. (Thorburn, 2012). Web 2.0 technological features combined with voluntary exposure to an indefinite audience in OSNs give rise to traditional surveillance as Government is enabled to “connect the dots”, combine information, find causal rules and statistical regularities and generate mass user profiles on the base of identifying patterns (Otterlo, 2014). The privacy/surveillance relevant application of user-generated content mining is the determination of correlation between characteristics and patterns and the respective classification of individuals.

The surveillance potential has to be considered also in view of Big Data technologies, which augment(s)/increase(s) knowledge discovery. What makes Big Data technologies and applications surveillance-relevant is not the size as such but the possibility to aggregate and correlate distinct and hidden (massive) data sets. OSN users may be soon overwhelmed by the increased level of sophistication and the pervasiveness of predictive and real-time large scale software (Buttarelli, 2014).

Data mining of OSN crawled data may have far reaching implications when we refer to the surveillance context. Governments may make extensive use of Big Data for surveillance purposes, such as the case of US Government’s PRISM program that involves the US NSA collecting and analyzing foreign communications collected from a range of sources, including OSN companies (Cumbley and Church, 2013). When referring to Big Data possibilities, Podesta points out that the Dept. of Homeland Security will now be able to take on new kinds of predictive and anomaly analysis while complying with the law and subjecting its activities to robust oversight (Podesta, 2014). Thus, data management complexity for social networking sites and service providers has significantly escalated (Farrell and Newman, 2016).

The observation of the behaviour and characteristics of individuals through mining of large quantities of data may infringe fundamental rights, let alone the determination of correlation between every-day activities and political beliefs, between characteristics and patterns and the respective classification of individuals. The risk to stigmatize groups of persons or persons, as part of a group life, is high. As noted by the German Federal Constitutional Court (Rasterfahnung Urteil of the Bundesverfassungsgericht, 04.04.2006, 1 BvR 518/02, 23.05.2006), data profiling means a higher risk of becoming the target of further (official) criminal investigations and suffering stigmatization in public life (Čas, 2011). Studies conveyed how profiling and the widespread collection and aggregation of personal information increase social injustice and generate further discrimination against political or ethnical minorities or traditionally disadvantaged groups (Schermer, 2011).

On the other side online social media data mining seems to be the “future, if not the present of law enforcement and security “thus enabling governmental agencies to extract information from an individual's every day interests, affiliations and online activities. Largely and permanently available and accessible information allows diving detailed portraits and profiles. Online social media data mining is proved to be more efficient than "traditional" forms of surveillance as it allows identifying past or even future wrongdoers whom the government would otherwise never have been suspected (Harvard Law Review, 2014).

Despite the usefulness of such methods, concerns about privacy and personal data protection lead to significant public debate about the scope and barriers of surveillance. In particular after E. Snowden's disclosures public concerns and fears are steadily augmented and become more severe as data mining as analysed in this paper may not be based on any individualised suspicion resulting in invasive surveillance that can target everyone.

According to the mainstream/dominant theory and jurisprudence in the USA, there is no "reasonable expectation of privacy if data is voluntarily revealed to others" (Solove, 2006). The Supreme Court's jurisprudence ruling that one cannot have a reasonable expectation of privacy in information that is given to third parties (Smiths v. Maryland, 1979) or made accessible to the public (California v. Greenwood, 19988) is evoked to justify large-scale data mining even without ensuring compliance with substantial and procedural safeguards and requirements (concrete and serious suspicion, authorization, warrant, etc.), as such information falls outside the scope of the Fourth Amendment's protection . However it is worthy to mention that in the recent case United States v. Jones five Justices of the Supreme Court suggested that the collection of sufficiently large amounts of information might amount to a search (thus implicating the Fourth Amendment) regardless of physical trespass and it is obvious that at least the quantity of information collected about US (and non US) citizens is expanding at a prodigious rate (LaFave, 2012).

In Europe, agencies ground the legitimacy of collecting and analysing information gained through data mining methods by pointing to the fact that such data are manifestly made public by the person concerned (Art. 8 §2e of the European Data Protection Directive), which is the case if people generate content or comment on other users' content in social networks or media using their real identity and aiming at expressing their opinions publicly. In any case, however, data mining is a form of data processing that has to be fair and based on the grounds provided and required by European Law (mainly informed consent, legal obligation, overridden public interest such as prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the prevention of threats to public security) and subject to the respective procedural guarantees as laid down in national law (warrant, approval by a Data Protection Authority, consultation with the latter authority, etc.).

While reflecting on assessing the lawfulness of online social media data mining the new European data protection regulatory framework has to be taken into consideration: the General Data Protection Regulation (679/2016/EU) that is going to replace the 1995 Directive and the Police and Criminal Justice Data Protection Directive (680/2016/EU, that is going to replace the 2008 Data Protection Framework Decision. The new framework does not include specific rules on data mining but it regulates profiling (Articles 4 (4), 13 (2f), 21 and 22 of the Regulation and 3 (4), 11 and 24 (1e) of the Directive).

The European legislators dealt with profiling within the context of automated decision-making: decision-making based on profiling, should be allowed where expressly authorised by Union or Member State law including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision (Recital 71). In the Police and Criminal Justice Data Protection Directive it is explicitly provided that profiling which results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited.

The new instruments are therefore expected to affect the impact on data processing beyond the borders of European Union: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behavior of such data subjects in so far as their behavior takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviors and attitudes (Article 3 of the Regulation in combination with Recital 24).

6 OSNs a Topos of Participatory Panopticism

Despite the lack of centralized control over the Internet, its platforms and applications enable intrusive and thorough monitoring. As Fuchs argues, on Web 2.0 corporate and state power is exercised through the gathering, combination and assessment of personal data, thus power relations and relationships of communication becoming interlinked (Fuchs, 2011). Web 2.0 architecture is encouraging users' actual involvement in OSNs and empowering a mutual "sharing practice" (Albrechtslund, 2008). Both the Web 2.0 architecture and the users' attitude create a situation that may be characterized as panoptic in design. Social connections, comments, views and preferences (expressed through "likes" or "retweets") are turning into visible, measurable, searchable and correlatable content. This voluntary exposure and engagement with others is regarded as the tool to the practice of "participatory" or "interpersonal" surveillance.

Every OSN user can be equally observer and observed, controller and controlled. Moreover, in both cases we have examined (YouTube, Twitter), we have demonstrated that user profiling, along with detection of behavioral patterns, can be achieved using solely limited computer sources and publicly available user data that is easily accessible through the mechanisms provided by the OSN per se. OSN users' profiling may become an every-day routine, what Andrejevic has conceived as "peer-to-peer monitoring", understood as the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another (Andrejevic, 2005).

In fact, Web 2.0 and OSNs (YouTube and Twitter) are becoming the topos of "participatory panopticism", an Omniopticon in which not only the State and private entities but also "the many" watch "the many". Despite the widespread "exposure" tendencies (a kind of digital "exhibitionism"), which characterizes the OSNs it seems that users do not share the "total transparency" model (Brin, 1999). It appears more probable that they do have a false perception of remaining anonymous or being among "friends" and they lack a "perception of audience", i.e. they don't realize that they may be "watched" and analysed by so many. On the other hand, being aware of mass profiling capabilities of persons, on the base of their views expressed in OSNs, could have intimidation effects with further impacts on their behavior, the conception of their identity and the exercise of fundamental rights and freedoms such as the freedom of speech (Čas, 2011). Profiling may indeed entail the risk of formatting and customization of individual behavior that affects her personal autonomy (Dumortier, 2010).

Extending monitoring to social communication relationships of employees and candidates augments the chances of employers to influence behavior and promote the "well-adjusted employee" (Simitis, 1999). Individuals tailor their social identities and aim at controlling others' impressions and opinions of them through behavior and performances within particular audiences (Sánchez Abril, Levin and Del Riego, 2012). Information gathering about employee performances outside the traditionally conceived work sphere not only increases the dependence on (future) employers but has also a chilling effect on individuals' personality and freedom of expression. Being deprived from informational privacy, i.e. the capacity to control of the information concerning them, users and thus the capacity for autonomous decision - and choice-making and to maintain a variety of social identities and roles, OSN users may feel fear of discrimination and prejudice, which may result to self-censorship and self-oppression. They may sacrifice "Internet participation to segregate their multiple life performance" (Broughton, 2009).

In the context of the relation between government and citizens, the fear of widespread and strong data mining and profiling capabilities of the government may affect individual autonomy by reducing the citizen's willingness to engage in political activities and participate to public sphere and discourse. For this fear to materialize, surveillance and profiling do not even have to be effective (Schermer, 2011).

7 Conclusions and Further Research

In our paper, we focus on the results of OSN profiling methods that materialize privacy-violating technologies and amplify the threshold of societal tolerance towards a panopticon-like state of surveillance. We discuss the arising social threats that are based on user generated content exploitation and lead to political affiliation profiling or psychosocial characteristics extraction. Political beliefs and affiliation have been a cause for social marginalization, prejudice, and discrimination, especially in totalitarian and authoritarian regimes. A user might want to protect personal information other than political affiliation, namely information related to sexual orientation, racial discrimination or even the health condition of the user regardless of the national scope. Such an improper information disclosure could be easily conducted via expansion of the panopticon methodology on the condition that domain experts of each case are available to interpret the collected data and train an appropriate model.

To demonstrate the efficiency of such cases, we collected a vast amount of data from Online Social Networks. We focused on a fraction of Twitter and YouTube users, i.e., a community of 41.818 Greek users from Twitter and a community of 12.964 users, 207.377 videos and 2.043.362 comments from YouTube. Afterwards, we conducted content and graph theoretic analysis of the datasets in order to verify that it is possible to extract conclusions over users' psychosocial characteristic of narcissism and predisposition towards law enforcement and political affiliation, using the panopticon methodology. Our results confirmed the initial hypothesis that Twitter and YouTube are OSNs that can support the study of users' sensitive personal information.

Accordingly, privacy violations may occur, in case someone chooses to apply the proposed methods in an illegal or unethical manner. Users' privacy and dignity may be at stake if someone uses the method to promote employee/user discrimination and careless punishment. Therefore, such methods should be utilized in the course of a legitimate action. Thus, the dialectic over the issue should follow the road of selecting the appropriate field of application for these profiling techniques, similarly to other proactive detection techniques, even of differentiated scope. Furthermore, we highlight possible consequences of the described panopticon method in terms of state surveillance. Regardless of the scope of the implementation, the resulting threats include working place discriminations, social prejudice or even stigma and marginalization of the victims. These phenomena could be identified even in a democratic and stable society. Such panopticon-like technologies enable multilevel and latent surveillance, thus posing new risks for the rights of the individuals. As a result users voluntarily expose their personal information to an indefinite audience and actively engage in the surveillance of other users, a state which leads to social panopticism (Nervla, 2010; Jurgenson, 2011).

For future work we plan to further study such panopticon-like technologies such as big data classification, predictive analytics and behaviour detection and recognize more aspects of this social threat. We intend on spreading our research on other social media and study the phenomenon under the prism of different tools and methodologies along with privacy enhancing remedies.

Acknowledgements

This work has been partially funded by the European Commission (Framework Programme 7, project "Public Perception of Security and Privacy: Assessing knowledge, collecting evidence, translating research into action" (PACT)).

References

Kaplan, A., and Haenlein M., (2010) 'Users of the world, unite! The challenges and opportunities of Social Media.' *Business horizons*, Vol. 53, No. 1, pp. 59-68.

Boyd, D., (2007) 'Social network sites: Public, private, or what.' *Knowledge Tree,* Vol. 13, No. 1, pp. 1-7.

Piskopani, A., and Mitrou L., (2009) 'Facebook: Reconstructing Communication And Deconstructing Privacy Law?.' *4th Mediterranean Conference on Information Systems*, Greece.

Albrechtslund, A., (2008) 'Online social networking as participatory surveillance. *First Monday*, Vol. 13, No. 3.

Van Dijck, J., (2009) 'Users like you? Theorizing agency in user-generated content.' *Media, culture, and society*, Vol. 31, No. 1, pp. 41.

Castells, M., (2013) '*Communication power'* Oxford University Press.

Marwick, A., (2012) 'The public domain: surveillance in everyday life.' *Surveillance & Society*, Vol. 9, No. 4, pp. 378-393.

Fuchs, C., (2011) 'New media, web 2.0 and surveillance.' *Sociology compass*, Vol. 5, No. 2, pp. 134-147.

Farinosi, M., (2011) 'Beyond the panopticon framework: privacy, control and user generated content.' *Toward Autonomous, Adaptive, and Context-Aware Multimodal Interfaces. Theoretical and Practical Issues*. Springer, pp. 180-189.

Lampe, C., Ellison, N., and Steinfield. C., (2006) 'A Face (book) in the crowd: Social searching vs. social browsing.' 20th Anniversary Conference on Computer supported cooperative work, ACM.

Lange, P., (2007) 'Publicly private and privately public: Social networking on YouTube' *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, pp. 361-380.

Nevrla, J., (2010) 'Voluntary Surveillance: Privacy, Identity and the Rise of Social Panopticism in the Twenty-First Century.' *Commentary - The UNH Journal of Communication Special Issue*, pp. 5-13.

Jurgenson, N., (2011) 'Review of Timoner's We Live in Public.' *Surveillance & Society*, Vol. 8, No. 3, pp. 374-378.

Tokunaga, R., (2011) 'Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships.' *Computers in Human Behaviour*, Vol. 27, No. 2, pp. 705-713.

Marwick, A., (2012) 'The public domain: Surveillance in everyday life.' *Surveillance & Society*, Vol. 9, No. 4, pp. 378-393.

Whitaker, R., (1999) '*The end of privacy: How total surveillance is becoming a reality'*, The New Press.

Amichai-Hamburger, Y., Vinitzky. G., (2010) 'Social network use and personality.' *Computers in Human Behaviour*, Vol. 26, No. 6, pp. 1289-1295.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., and Gritzalis. D., (2010) 'An insider threat prediction model.' *Trust, Privacy and Security in Digital Business*. Springer, pp. 26-37.

Mylonas, A., Kastania, A., and Gritzalis. D., (2013) 'Delegate the smartphone user? Security awareness in smartphone platforms.' *Computers & Security*, Vol. 34, pp. 47-66.

Mylonas, A., Meletiadis, V., Mitrou, L., and Gritzalis, D., (2013) 'Smartphone sensor data as digital evidence.' *Computers & Security*, Vol. 38, pp. 51-75.

Shaw, E., Ruby, K., and Post. J., (1998) 'The insider threat to information systems: The psychology of the dangerous insider.' *Security Awareness Bulletin*, Vol. 2, No. 98, pp. 1-10.

Kandias, M., Galbogini, K., Mitrou, L., and Gritzalis. D., (2013) 'Insiders trapped in the mirror reveal themselves in social media.' *Network and System Security*. Springer, pp. 220-235.

Kandias, M., Stavrou, V., Bozovic, N., Mitrou, L., and Gritzalis. D., (2013) 'Can we trust this user? Predicting insider's attitude via YouTube usage profiling.' *10th IEEE International Conference on Autonomic and Trusted Computing*. IEEE.

Gritzalis, D., Stavrou, V., Kandias, M., Stergiopoulos. G., (2014) 'Insider Threat: Enhancing BPM through Social Media.' *6th International Conference on New Technologies, Mobility and Security*. IEEE.

Kandias, M., Stavrou, V., Bozovic, N., and Gritzalis. D., (2013) 'Proactive insider threat detection through social media: The YouTube case.' *12th ACM workshop on Workshop on Privacy in the Electronic Society*. ACM.

Chen, Y., Nyemba, S., Zhang, W., and Malin. B., (2011) 'Leveraging social networks to detect anomalous insider actions in collaborative environments.' *IEEE International Conference on Intelligence and Security Informatics*. IEEE.

Kandias, M., Virvilis, N., Gritzalis, D., (2013) 'The insider threat in Cloud computing.' *Critical Information Infrastructure Security*. Springer, pp. 93-103.

Skues, J.L., Williams, B., and Wise, L., (2012) 'The effects of personality traits, self-esteem, loneliness, and narcissism on Facebook use among university students.' *Computers in Human Behaviour*, Vol. 28, No. 6, pp. 2414-2419.

Steele, R.D., (2007) 'Open source intelligence.' *Handbook of intelligence studies*, pp. 129-147.

Buffardi, L., and Campbell, K., (2008) 'Narcissism and social networking web sites", *Personality and Social Psychology Bulletin*, Vol. 34, No. 10, pp. 1303-1314.

Mehdizadeh, S., (2010) 'Self-presentation 2.0: Narcissism and self-esteem on Facebook *Cyberpsychology, Behaviour, and Social Networking*, Vol. 13, No. 4, pp. 357-364.

McCallum, A., and Nigam. K., (1998) 'A comparison of event models for naive Bayes text classification.' *AAAI-98 workshop on learning for text categorization*, Vol. 752, pp. 41-48.

Joachims, T., (1998) '*Text categorization with support vector machines: Learning with many relevant features'* Springer.

Anderson, J., (1982) 'Logistic regression.' *Handbook of Statistics.* North-Holland, USA, pp. 169-191.

Manning, C., Raghavan, P., and Schütze. H., (2008) '*Introduction to information retrieval'* Vol. 1. Cambridge: Cambridge University Press.

Council of Europe Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

Kosinski, M., Stillwell, D., and Graepel. T., (2013) ‘Private traits and attributes are predictable from digital records of human behaviour.’ *Proc. of the National Academy of Sciences*, Vol. 110, No. 15, pp. 5802-5805.

Kandias, M, Mitrou, L., Stavrou, V., and Gritzalis. D., (2013) ‘Which side are you on? A New Panopticon vs. Privacy.’ *10th International Conference on Security and Cryptography*, pp. 98-110.

Keber, T., (2014) “Rechtskonformer Einsatz von Social Media im Unternehmen, Recht der Datenverarbeitung 4/2014,” pp. 190-199, 191 with reference to a survey among USA based companies (http://www.go-gulf.ae/blog/ social-media-pre-employment-screening/)

Sánchez A., Avner, P., and Del Riego. A., (2012) ‘Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee.’ *American Business Law Journal*, Vol. 49, No. 1, pp. 63-124.

Fazekas, C., (2004) ‘1984 is still fiction: Electronic monitoring in the workplace and US privacy law.’ *Duke Law & Technology Review*, pp. 15-15.

Mitrou, L., and Karyda. M., (2006) ‘Employees’ privacy vs. employers’ security: Can they be balanced?.’ *Telematics and Informatics*, Vol. 23, No. 3, pp. 164-178.

Broughton, A., Higgins, T., Hicks, B., and Cox, A., (2009) ‘Workplaces and social networking-The implications for employment relations.’ *Institute for Employment Studies, Brighton*.

Hull, G., Lipford, H. R., and Latulipe, C., (2011). ‘Contextual gaps: privacy issues on Facebook’. *Ethics and Information Technology*, Vol. 13, No. 4, pp. 289-302.

Strahilevitz, L. J., (2005). ‘A social networks theory of privacy.’ *The University of Chicago Law Review*, pp. 919-988.

Nissenbaum, H., (2004) ‘Privacy as contextual integrity.’ *Wash. L. Rev*,. Vol. 79, pp. 119-157.

Davison, H., Maraist, C., and Bing, M., (2012) ‘To screen or not to screen? Using the internet for selection decisions.’ *Employee Responsibilities and Rights Journal*, Vol. 24, No.1, pp. 1-21.

Sobkowicz, P., Kaschesky, M., and Bouchard, G., (2012). ‘Opinion mining in social media: Modeling, simulating, and forecasting political opinions in the web.’ *Government Information Quarterly*, Vol. 29, No. 4, pp. 470-479.

Bennett, C., (2013) ‘The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies,’ *First Monday*, Vol. 18, No. 8.

Bennett, C., (2015) ‘Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications.’ *Surveillance & Society*, Vol. 13, No. 3, pp. 370-384.

Tufekci, Z., (2014) ‘Engineering the public: Big data, surveillance and computational politics.’ *First Monday*, Vol. 19, No. 7.

Buttarelli, G., (2014) ‘The EU Data Protection Reform: Updated Perspectives and the Challenges posed by Big Data.’ *Speaking points at Inet Istanbul. Internet: Privacy and Digital Content in a Global Context*.

Rubinstein, I., (2012) ‘Big Data: The End of Privacy or a New Beginning?.’ In: *New York University School of Law Public Law & Legal Theory Research Paper Series*, Working paper no. 12-56.

Thorburn, M., (2012). ‘Identification, Surveillance, and Profiling: On the Use and Abuse of Citizen Data.’ Hart.

van Otterlo, M., (2014). ‘Automated Experimentation in Walden 3.0: The Next step in Profiling, Predicting, Control and Surveillance.’ *Surveillance & Society*, Vol. 12, No. 2, pp. 255-272.

Cumbley, R., and Church, P., (2013) ‘Is “Big Data” creepy?.’ *Computer Law & Security Review*, Vol. 29, No. 5, pp. 601-609.

Podesta, J., (2014) ‘Big data: Seizing opportunities, preserving values.’ *Executive Office of the President. Report.*

Farrell, H., and Newman, A., (2016) ‘Transatlantic Data War: Europe Fights Back against the NSA’, *The. Foreign Affairs*, Vol. 95, No. 124.

Čas, J., (2011) ‘Ubiquitous Computing, Privacy and Data Protection: Options and limitations to reconcile the unprecedented contradictions.’ *Computers, privacy and data protection: An element of choice*. Springer, pp. 139-169.

Schermer, B., (2011) ‘The limits of privacy in automated profiling and data mining.’ *Computer Law & Security Review*, Vol. 27, No. 1, pp. 45-52.

Solove, D., (2006) 'A taxonomy of privacy.' *University of Pennsylvania Law Review*, pp. 477-564.

Harvard Law Review, (2014), 'Data Mining, Dog Sniffs, and the Fourth Amendment.' Harvard Law Review, Vol. 128, No. 691.

LaFave, W., (2012), Search and seizure: A treatise on the Fourth Amendment (Vol. 5).' West Group Publishing.

Rubinstein, I., Lee, R., and Schwartz, P., (2008) 'Data mining and Internet profiling: Emerging regulatory and technological approaches.' *The University of Chicago Law Review*, pp. 261-285.

Dempsey, J., and Flint, L., (2003) 'Commercial data and national security.' *G. Washington Law Review* 72, pp. 1459.

Hildebrandt, M., (2009) 'Who is profiling who? Invisible visibility.' *Reinventing Data Protection?*. Springer, pp. 239-252.

Andrejevic, M., (2005) 'The work of watching one another: Lateral surveillance, risk, and governance.' *Surveillance & Society*, Vol. 2, No. 4, pp. 479-497.

Brin, D., (1999) '*The transparent society: Will technology force us to choose between privacy and freedom?*' Basic Books, USA.

Dumortier, F., (2010) 'Facebook and Risks of "De-contextualization" of Information.' *Data Protection in a Profiled World*. Springer, pp. 119-137.

Simitis, S., (1999) 'Reconsidering the premises of labor law: Prolegomena to an EU regulation on the protection of employees' personal data.' *European Law Journal*, Vol.5, No. 1, pp. 45-62.

Gritzalis, D., Kandias, M., Stavrou, V., and Mitrou, L., (2014) 'The Social Media in the History of Information: Privacy violations and security mechanisms,' In: *History of Information Conference*, Greece.