

KADIR HAS UNIVERSITY  
GRADUATE SCHOOL OF SOCIAL SCIENCES



RESISTANCE FROM WITHIN HEGEMONY:  
RISE OF SEMI-ANONYMOUS RESISTANCE IN TURKEY'S  
NEW MEDIA ENVIRONMENT

SARPHAN UZUNOĞLU

RESISTANCE FROM WITHIN HEGEMONY:  
RISE OF SEMI-ANONYMOUS RESISTANCE IN TURKEY'S NEW MEDIA  
ENVIRONMENT

SARPHAN UZUNOĞLU

Submitted to the Graduate School of Social Sciences  
in partial fulfillment of the requirements for the degree of  
Master of Arts in New Media

KADIR HAS UNIVERSITY

December, 2013

KADIR HAS UNIVERSITY GRADUATE SCHOOL OF SOCIAL SCIENCES

RESISTANCE WITHIN HEGEMONY:  
RISE OF SEMI-ANONYMOUS RESISTANCE IN TURKEY'S NEW MEDIA

SARPHAN UZUNOĞLU

APPROVED BY:

(Yrd. Doç. Dr. İrem İnceođlu) (Kadir Has University)

\_\_\_\_\_  
(Thesis Supervisor)

(Yrd. Doç. Dr Eser Selen) (Kadir Has University)

\_\_\_\_\_  
(Yrd. Doç. Dr Burçe Çelik) (Bahçeşehir University)

APPROVAL DATE: 10/December/2013

HEGEMONYA İÇİNDE DİRENİŞ:  
TÜRKİYE'NİN YENİ MEDYA ORTAMINDA YARI-ANONİM DİRENİŞİN  
YÜKSELİŞİ

**Özet**

Türkiye'de İnternet ve ifade özgürlüğü üzerine yapılan araştırmaların çoğu gözetim teknolojileri ve ülkedeki sansür politikalarına ilişkin çalışmalardır. Tüm bu çalışmalarda genel olarak yeni medyada ortaya çıkan politik iradelerin geleceğine ilişkin pesimist ifadeler vardır. Oysa burada söz konusu olan hegemonik bir süreçtir ve tüm bu baskı mekanizmaları tıpkı Raymond Williams'ın (1977, 110) belirttiği üzere hegemonyanın dinamik yapısı dahilinde direnişe de sürekli olarak, istemeksizin, alan sağlar. Bu direniş türlerinden biri de kullanıcıların kendi güvenliklerini sağlamak için kullandıkları profillerin anonimlik seviyeleri olarak görülebilir. Tez boyunca, anonim kullanım olarak kabul gören kullanım biçimleri tahlil edilerek, anonimliğin tam gereksinimlerini karşılayamayan aktivistlerin profilleri çıkarılarak, yarı-anonimlik durumu kavramsallaştırılmakta, yarı-anonimlik tecrübelerinden yola çıkarak, yarı-anonimlerin kimliklerini gizleme motivasyonları kategorik olarak incelenmekte, anonimlik, yarı-anonimlik ve görünürlük tanımları üstünden İnternet alanındaki kimliklerin görünülürlüğü gruplandırılmakta, dijital aktivistlerin anonimliğe ihtiyaç duymasına neden olan çeşitli motivasyonları ve yarı-anonim ve anonim kullanımın gelecekteki politik avantajları araştırılmaktadır.

**RESISTANCE FROM WITHIN HEGEMONY:  
RISE OF SEMI-ANONYMOUS RESISTANCE  
IN TURKEY'S NEW MEDIA ENVIRONMENT**

**Abstract**

Most of the studies over freedom of expression and thought in Turkey's new media sphere focus on surveillance technologies and related legal constraints in the country's new media sphere. Taking hegemony as a dynamic process just as Raymond Williams (1977, 110) did, hegemony is perceived as a structure within which resistance can still be available despite all the constraining policies of governments and companies in our lives. Anonymous, semi-anonymous and non-anonymous or real identity based resistance actions are considered as three different forms of resistance based on identifiability preferences. This thesis analyses the conjunctural anonymous uses of Internet by activists by analysing their profiles. Anonymity and semi-anonymity are conceptualized based on the users' experiences while necessity of being anonymous are studied categorically. This study conceptualizes forms of identifiability/ anonymity as anonymity, semi-anonymity and identifiability, it also focuses on different motives that resulted in the necessity of anonymity for digital activism. Thesis ends with a proposal about possible political uses of anonymity and semi-anonymity in the future for a radical democracy model.

## Table of Contents

**Özet**

**Abstract**

**Table of Contents**

<b>1 Introduction.....</b>	<b>1</b>
<b>2 Theoretical Background of Anonymity and Semi-Anonymity.....</b>	<b>7</b>
2.1 Layers and Definitions of Anonymity.....	7
2.2 Control Mechanisms in Turkey's New Media Environment.....	10
2.3 Deep Packet Inspection: Control For Everyone.....	13
2.4 Legitimacy of Surveillance.....	15
2.5 Perceptions of Anonymity.....	17
2.6 Social and Technical Methods Used For Providing Anonymity.....	19
2.7 Semi Anonymity versus Pseudonymity.....	22
<b>3 Political and Philosophical Background of Anonymity.....</b>	<b>24</b>
3.1 New Debates, New Politics, New Communities.....	25
3.2 Resistance and Hegemony.....	27
3.3 Political and Legal Necessity of Anonymous Use Of Internet.....	30
3.4 Semi-Anonymity as a Proactive Resistance Method.....	31
3.5 Technology as a Political Instrument.....	33
3.6 Identification of Semi-anonymity.....	34
3.7 Motives of Semi-anonymity.....	35
<b>4 Methodology.....</b>	<b>39</b>
4.1 Research Model.....	39
4.2 Research Context.....	41
<b>5 Experiencing Various Forms Anonymity and Identifiability.....</b>	<b>45</b>
5.1 Interviewees' Perceptions of Anonymity.....	45
5.2 Weaknesses of Semi-Anonymity.....	45
5.3 Reasons of Semi-Anonymous Use.....	46

5.4 Hacker Culture and Anonymity.....	49
5.5 Advantages / Disadvantages Of Anonymity.....	49
<b>6 Conclusion.....</b>	<b>52</b>
6.1 Semi-Anonymity: A Social Preference.....	51
6.2 Semi-Anonymity: Technical and Theoretical Proposal .....	53
6.3 Political Future and Use of Anonymity and Semi-Anonymity.....	54
<b>References .....</b>	<b>57</b>
<b>Appendixes.....</b>	<b>60</b>

## **Chapter 1**

### **Introduction**

Starting with 1990s, the Internet became an extraordinarily important actor in organizing and forming the political actions on the web. From Zapatista movement in South America to protests in Cairo, Tehran and Istanbul year by year Internet started to be used more effectively by political activists and choreography of the political organizations had changed. Like Belarus and Thailand, different countries regarded the Internet as a political instrument; from election campaigns to surveys, the Internet is used by political organizations. Yet, the most significant aspect of new media use has been its position within mass movements as a tool for mobilization. Anti-war and anti-globalization movements used the Internet for communicating within their own groups as well as for promoting their ideas to others. Yet, all these political developments are not limited with the NGOs' (Non-Governmental Organizations) or political groups' existence on the Internet. The Internet changed both the nature of democracy within these groups and activists' methods of protesting all over the world. Scrutinizing the way anonymity influences in-group democracy practices and public politics, this thesis tries to propose secure and anonymous new media usage as a method for replacing the existing under-surveillance democracy practices.

This study covers the conceptualization of anonymity with its varieties since anonymity itself has been a political strategy in both conventional and digital activism experiences in contemporary world. The Internet became a leading instrument in so called leaderless revolutions in 21<sup>st</sup> century. Thus, the newly emerged form of leaderless and less competitive forms of political activism and

resistance are analysed based on the personal and collective experiences of activists who use the Internet for political aims. Besides proposing anonymity as an instrument for radical democracy, social conditions and technical layers of anonymity are clarified in order to surpass the misperceptions of activists about their levels of anonymity.

Fuchs (2008, 272) states that, “while industrial capitalism surveillance is more oriented towards direct social contacts and the monitoring of activities (e.g., of factory workers) by overseers and punishment in the case of misbehaviour, electronic surveillance is more anonymous, indirect, invisible, and technologically mediated”. Discussions on control mechanisms have accelerated within the last decades as their effects have become more visible. Yet, there are still numerous people who have a positive perception about surveillance as a form of security in urban life. Citizens mostly demand surveillance for the security of their daily lives and properties.<sup>1</sup> However, this study hypothesizes that day by day there are more people who feel that they are threatened by the surveillance and try to create some measures against it. From pseudonymity to anonymity or preserving personal information on the web, these people started to create individual solutions against the control which will be described and explained in the coming pages.<sup>2</sup>

---

1

<http://www.haberler.com/mermer-diyari-iscehisar-da-halk-mobese-istedi-4215252-haberi/> [29/09/2013]

2

The word anonymous is used as a term with reference to the levels of identifiability rather than the transnational hacker organization called *Anonymous*. The ones mentioned in the study as anonymous users are not necessarily within the organization called *Anonymous*. But studies of Gabriela Coleman, who is known well with her articles about *Anonymous*, is utilized for revealing political potential of anonymity and its further impacts free from the organization called *Anonymous* (See

For proposing semi-anonymity as a new form of anonymity, experiences of pseudonymous users are examined and a layering construction is built for anonymity in Chapter Two. Softwares used and network structures created for providing anonymity that I cover in this chapter are used for stating technical layer of the anonymity, while anonymity of network became the social layer, and intentions and motives became the third layer and lastly, content produced by users became the last layer of anonymity. After stating conditions and motives of anonymity, surveillance methods are covered in that chapter for defining the hegemonic environment since surveillance as a government tool became a part of public policy and as civil libertarian critics point out much of information and communication technology developments that are said to be bringing about a quantum extension in government's powers to detect and punish as these new developments are open to be monitored (Hood, 2006, 472).

Having stated technical conditions of both anonymity and control, which can be stated as resistance and hegemony, third chapter includes philosophical and political background of anonymity as a form of resistance and contemporary debates over digital activism and its non-hierarchic characteristics. As Morozov (2011, 27) states; the nature of the Internet is reshaping the very nature and culture of anti-government resistance and dissent, shifting it away from real-world practices and toward anonymous virtual spaces, it will also have significant consequences for the scale and speed of the protest movement, not all of them positive. That chapter defines technical, social and theoretical layers of anonymity which resulted in the difference between various forms of identifiability and anonymity.

---

Coleman, 2011).

These changes starts with individuals' practices of using the Internet for protesting and, anonymity as a both individual<sup>3</sup> and collective<sup>4</sup> identity making process has been one of the most preferred methods of digital activism.

Relying on these changes in forms of activism, shift in methods and important role and existing definitions of anonymity, Chapter Three observes anonymity politically and philosophically while it also covers the social processes of communication which have evolved and have been completely impacted by this evolution of interactivity, sociability and communicational hierarchy of daily life by the nature of Web 2.0 or social media networks . Castells defines contemporary era the era when “the fastest and most autonomous, interactive, reprogrammable and self expanding means of communication in the history appeared” (Castells, 2012, 15); taking his emphasis on the less hierarchical characteristic of organization and participatory nature of occupy movements with reference to discussions over conventional and new types of activism in England, the relationship between individual, network and anonymity is analysed in Chapter Three.

Chapter Three will start with a discussion about the new media as a hegemonic sphere and terminology of new media as a hegemonic environment. This chapter, benefiting from Raymond Williams' theory of hegemony, and anonymity's

---

<sup>3</sup> In Turkey's Twitter environment, some figures such as @Eksihabermas or Angelopouloos have ten thousands or hundred thousands of followers while most of the deputies or party leaders in Turkey have less than ten thousand followers.

<sup>4</sup> Today, hacker groups such as Anonymous or Redhack are thought to be morally and ideologically more effective on voters in terms of opposition parties and Non-Governmental Organizations over the world. For instance, Redhack's number of followers are much more than conventional leftist parties in Turkey.

definition as a resistance from within hegemony, centralizing the user as a resistant figure, as the one who prefers anonymity as a strategy of resistance, anonymity's role in groups or individual practices will be stated. Besides these theoretical aspects the chapter includes some cases about Turkish users who used social networks for their political aims or political activism, the legal background of anonymity and identifiable use of the Internet in Turkey's new media sphere will be analysed with its social aspects.

Since anonymity is a legally controversial term, which is often perceived to be used only by hacktivists, methodology chapter includes social and legal rationale for the methods used during the design of the research ethically. New media tools used during the interviews and rationalization of their use is made in that chapter as well. Chapter Four also includes the details of participatory online research method used during the study.

Following methodology in Chapter Four, which gives details about the construction of this new media field research Chapter Five includes the information gathered throughout this study. Moreover an analysis of semi-structured online interviews with the users can be seen in this chapter. In these interviews users' experiences of various forms of anonymity or identifiability are questioned technically, socially and in a motive based way as well for detecting impact of various motives on various levels or forms of anonymity. Weaknesses of semi-anonymity are covered in this chapter for proposing the differences between anonymity and semi-anonymity. Semi-anonymity's position in hacker culture is also questioned by the expressions of semi-anonymous users and their technical preferences as well. Chapter Five finally covers anonymity's advantages

and disadvantages by the expressions and experiences of users.

In the conclusion, three main attitudes of new media users against control relying on their anonymity preferences is defined based on the results of the research: Anonymity, semi-anonymity and identifiability. Moreover, anonymity's position as a digital activism strategy and semi-anonymity's distinctive position will be defined in that chapter. Finally, academic and political future of the study as an opportunity for utopic new media and politics environment will be explained. Taking new media as a new and large sphere of control, this study provides non-techno determinist approach to the nature of the democracy in new media environment and how new media environment effected political representation of human beings or their 'avatars' on social networks. Regarding this impact, the thesis suggests an utopic sphere where direct and radical forms of democracy are institutionalized by the existence of new media tools.

## **Chapter 2**

### **Theoretical Background of Anonymity and Semi-Anonymity**

There is a need for clarifying technical, practical and theoretical definitions of anonymity, semi-anonymity and identifiability. Starting from layers and conditions of anonymity, this chapter covers surveillance mechanisms in Turkey's new media sphere and various technical and social methods used for providing anonymity for users. Based on technical and social methods and theoretical background, a distinction between anonymity, semi-anonymity and pseudonymity is proposed.

#### **2.1 Layers and Definitions of Anonymity**

Anonymity is the condition of both user and the communication type. Therefore, there are various forms and definitions of anonymity. The terminology regarding anonymous use of new media should be covered to categorize the forms of anonymity. First term to be covered is the anonymous. The English word anonymous is derived from the classical Greek stem onyma (name), combined with the prefix a- (the absence or lack of a property) (Clark et. al, 2005, 12-13). It is possible to interpret anonymity as the opposite of being identifiable. Baggio and Beldarrain (2011, 2) stated that "deciding to trust in cyberspace is not without risk, as anonymity protects those who are honest as well as those who intentionally deceive." This statement reveals that anonymity has both positive and negative connotations. Therefore, being anonymous should be observed not only as a form of resistance, but also as an individual or a collective action. Even if anonymity means namelessness in Greek, it is defined in a more detailed way in this research.

Palme and Berglund (2004) state that anonymity is possible when the real author of a message is not shown and anonymity can be implemented to make it impossible or very difficult to find out the real author of a message. They state that anonymity is sometimes thought to be synonym with pseudonymity when another name rather than the real one becomes visible. Anonymity should not be limited to the preservation of detailed data about user as the Internet is composed of different structures and in new media environment people disseminate different information about themselves in different media applications or networks. According to Hansen et. all (2001, 2) “anonymity is the state of being not identifiable within a set of subjects.” They recognized anonymity as a situation in transmission of the message and divided it in two different subcategories which are sender anonymity -the properties that a particular message is not linkable to any other-, recipient anonymity - a particular message and relationship anonymity means that it is untraceable who communicates with whom. In other words, sender and recipient (or recipients in case of multicast) are unlinkable. The relationship anonymity is a weaker property than both sender anonymity and recipient anonymity. Because it may be traceable who sends which messages and it may also be possible to trace who receives which messages, as long as the relationship between sender and recipient is not known.

There are three possible categorization of layers for defining anonymity. First one is sender and receiver anonymity. Second one is the connection and message anonymity and the third one is the anonymity set and the third one is the unlinkability. For defining the anonymity, this research focuses on these four categories that are proposed by Joss Wright, Susan Stepney, John A. Clark and

Jeremy Jacob (2005,14). Hansen et. all (2001, 33-34) starts new discussion over some other terms such as unlinkability and unobservability which refers to information hiding in terminology. Also, according to them, unlinkability of two or more items (e.g., subjects, messages, events, actions, ...) means that within this system, these items are no more and no less related than they are related concerning the a-priori knowledge (Hansen et. all, 2002,1-3). Connection between social media accounts or links between senders of different messages on the Internet can be considered as a linkability while unobservability may refer to today's coding and encryption technologies, by which senders of messages are completely stay anonymous but the relationships themselves do not. The terminology mostly depends on the conditions existing in Web 1.0 environment where interactivity had not that much penetrated into people's lives. But the terminology they provide can be still used for explaining 'complete' anonymity of relationships in terms of sender receiver interactions. According to them sender's anonymity is a precaution of relationship's anonymity but for them recipient's anonymity is another issue that provides anonymity to the relationship.

In contemporary world, a complete anonymity can be considered as a really 'radical' condition where relationships are no longer anonymous as receivers are not and observability is higher than ever because of the technologies mentioned above. Their relationship's observability is based on some technical applications such as dummy traffic, steganography which can be defined as hiding the messages in a way that can not be sensed; and spread spectrum (Hansen et. All, 2002,5).

The technical and interaction based definitions of the term, "anonymity" provides

users some certain advantages. For instance anonymity allows masking handicaps and accentuating certain individual characteristics, which might lower inhibition (Doering 2003, 460) One can create an identity for himself/herself free from all biases and legal constraints within society. Fuchs (2008, 322) states “anonymous identity is not free from social past of a human being as social experiences and the individual history of an individual influence and shape his or her online behaviour.”

Fuchs (2012) also states that "we need to observe both control mechanisms and the reactionary liberation movements and actions." To get a better understanding about the terms such as anonymity, semi-anonymity and identifiability, existing oppression and control mechanisms must be covered. In this part, surveillance mechanisms in Turkey used by financial corporations and government and their impact range is analysed in order to understand how users with different anonymity levels are positioned against corporate surveillance mechanism.

## **2.2 Control Mechanisms in Turkey's New Media Environment**

In Turkey's new media environment, surveillance processes are practiced by states and companies for their common aims and the sustainability of static governance policies. Hegemonic control of the new media is not different from controlling the streets of a country with typical surveillance mechanisms or such practices.

The difference is the lack of security of privacy and individuality. From ID cards to registered Internet connections, registered computers and cell phones, capitalist industry and state established a “wall of security” which is the key concept for understanding state’s relationships with citizens and capitalist institutions. Internet users mean more than users or consumers of the computer

mediated communication technologies or new media; but it does not completely save us from being the product or the object of the new surveillance environment.

Users are under the control of both the state and capital. Today, capitalism and state are agencies of surveillance for each other since the centralized controlling mechanisms need a collaboration of those two sides in informational society where internal and external networks provide the new sphere for both intellectual and fiscal production. Since the power holders would like to control what individuals do in their leisure times, on their work hours and even when they are not connected, surveillance mechanisms are getting much stronger day by day. Since focus point of the thesis is the rising resistance mechanisms in new media sphere, and the way their level of effectiveness and radicalness change according to ideological, social and technical factors differing from user to user, in order to make a good mapping of resistance mechanisms, the hegemonic control mechanisms of the state on new media environment must be studied the first.

In Turkey, while number of houses with the Internet connection increases, so does the usage of the Internet. Connections from the Internet cafes decrease as household connections increase. There is computer in 51% of the households in Turkey while 42% of the households have connection to the Internet. However this is not a “clear” data since the Internet connection cannot be limited to the personal computer connections. People, by using computers, mostly prefer to connect to the Internet from their households. In terms of security, the most important data obtained is that, people use the Internet mostly for social

networks and mailing. (IPIS KMG, 2012).

Rural Internet penetration is 27.3% while it is 55.5% in urbanized areas. 70% of household usage of the Internet is an important factor since it is an opportunity for government to get better and more reliable surveillance results (TÜİK, 2012). Webster (2006, 215) states that “information war no longer requires the mobilisation either of the citizenry or of industry for the war effort. It relies instead on capturing only the leading edges of industrial innovation for military purposes – for instance, electronic engineering, computing, telecommunications and aerospace.” As the Internet usage increases, Turkish state today develops its controlling mechanisms which are established in collaboration with international companies and well known typical softwares produced by the state. The informational war is not going on only between secret agencies of the states but also among some libertarian organizations and completely independent individuals at the same time. As it happened to trade unions, nuclear disarmament activists, educationalists and media personnel in 1990s England, surveillance is possible for individuals to be targeted by government surveillance. Regarding that, limiting surveillance to a model of controlling only works for the political individuals is a kind of delusion since all the phone calls are recorded and most of the Internet packages are controlled by different softwares within network structure. Investments on security and surveillance is so high that it should not be considered as a regular unit of consumption for the state. Rather than a war jet, it is more common for governments to buy surveillance services including recording all phone calls [etc.](#) (Appelbaum et. All, 2012).

### **2.3 Deep Packet Inspection: Control For Everyone**

For understanding the hegemonic uses of control mechanisms by state in Turkey, some of the surveillance mechanisms and cases they are involved in and the level of surveillance, censorship and legal restrictions on new media environment in that country should be observed. Deep Packet Inspection and Internet Provider Services are the key terms to be focused for understanding state surveillance better. In Turkey, there is a crisis of privacy for the Internet users because of the Phorm case and surveillance strategy of Turkish government in cooperation with TTNET and Phorm companies. Phorm in Turkey is claimed to be one of the controlling systems government used for surveillance of daily Internet usage of TTNET –an Internet Provider Service- users or clients. Phorm is announced to be illegal by the decision of European Parliament which is involving Turkey as well. Phorm’s function is defined as personalizing the user experience much more by themselves. Sites visited, ads clicked on, videos that are watched and forms that have been filled by users are used by Phorm for creating a profile of them. By redirecting TTNET users to a website<sup>5</sup> Phorm system forces users to be involved in a surveillance system and once you login to the system you are not allowed to sign out that easily. To better understand this surveillance process the term DPI should be understood well. DPI (Deep Packet Inspection) service is used for several reasons such as, presenting ads relying on behavioural targeting strategies, slowing P2P sharing and such activities, and finally surveillance for governments and intelligence agencies of them . Data Phorm collects include “political opinions, sexual proclivities, religious views, and health.” (Fuchs, 2012, 20) This is a kind of data that semi-anonymous users hesitate or try to prevent sharing with their employers and local or national

---

<sup>5</sup> <http://www.gezinti.com>

governance.

This kind of profiling may provide governments about political organizations, religious groups and subcultures a lot at the Because of the proclaimed illegitimacy of the information collected Fuchs (2012,21) states about Phorm that “Users should have to opt in to such a system, not merely be given an opportunity to opt out,” and it is required under European data protection law. “Heavy use of DPI by ISPs may undermine trust that users have in the network and ISPs and this can result in self and inhibition of users.” (Cooper, 2011, 147) In Turkey, Phorm is still claimed to be continuing its activities through different opt-in methods that force users to be involved in system according to Alternative Informatics Association. Certainly, Phorm is not the only company which serves to the interests of the governments, according to report by Fuchs (2012, 8-10) IPS, NETI, Ultimaco Safe-Ware, Group 2000, Gamma Group, Telesoft Technologies, Ipoque, Elaman, Amesys, Alcatel-Lucent and Aqsacom are some of the other companies whose serves to the governmental agencies have been revealed by Wikileaks reports. Google can be questioned in terms of privacy of the content, but different from Phorm it has a different characteristic. “Google may track your searches, your travel (Google Maps), and your appointments (Google Calendar), but the company’s ability to do so is limited by the number of different Google services of which you avail yourself. If you object to Google’s privacy policies, you can choose to use other services. By contrast, your ISP knows everything you do online. [...] A single ISP will know what you are browsing, what your email says, VoIP, and so on. In a matter of days, possibly even hours, an ISP using DPI can develop a remarkably detailed dossier on a person” (Landau 2010, 220). DPI, different from an ISP, Phorm is a

greater threat for the users' privacy and use of web. It includes the analysis of all the segments of the data no matter what bandwidth exactly is. The unencrypted texts sent by DPI are going to be observed if intended unlike ISP which superficially analyses the content of the data.

#### **2.4 Legitimacy of Surveillance**

Another important aspect of the surveillance in Turkey is its legitimacy preserved by laws and constitution. Turkey is one of the few countries which do not have a regulation or law for preservation of data. Because of that, it is identified as an insecure country in international area (Alternative Informatics Association, 2013). Even if freedom of expression and freedom of thought is guaranteed by the constitution, still there are no enough regulations to preserve these liberties as restrictions are also preserved by Turkish Criminal Law and Antiterrorism Laws that are built by Turkish governments. Recently, criticizing the government has been named as an activity to "weaken" the government on social media. Some people have been penalized with money or prison for their statements in social media. Additionally, people are taken away from their official duties because of their activities of recommendation and share in social media.

There is a problem experienced between financial corporations and consumers especially during the electronic commerce processes. It is known that people are expected to give much more information than needed for e-commerce activities. There is a principle called "limitation of the aim" and the person who collects information via a net activity or contract can only use the data he/she obtained for that issue, nothing else. This principle is in run only according to the

preferences of the users, there are still some companies which serve the information they obtained as a financial meta to other companies and make profit on the information they gathered from you (Alternative Informatics Association, 2013b, 8). Another problem in this issue is the consent of the users. According to Alternative Informatics Association data must be preserved with the consent of the users and this consent must be taken with the free will of the users/consumers etc. (Alternative Informatics Association, 2013b, 9).

This is a great economy that is mentioned here as all the security systems and digital surveillance mechanisms. Google, as a global company acts as a surveillance and control mechanism as well. According to their statistics, since 2010 July, 12% of the demands of removal are about aspersions, 22% of them are about official corporations, 11% of them are about adult content, 2% of them are about secrecy and security, 6% are about religious offence, 3% are about copyright, 1% is about violence, hate speech is 1% and there are other titles. Atatürk as a "sensitive theme" is used for these bans and google removal requests at the same time (Google Transparency Report, 2013). Here the main point is not only about the state policies but also about the policies of the companies and the [corporations](#). Corporations in Turkey are ought to pay their taxes for their financial interests and legitimacy of their economical activities. Moreover, Google's head squad's visits to Turkish President and possible cooperations between state and the company can be understood as primary reasons of their cooperation in censorship and surveillance.

All of the corporate surveillance mechanisms listed above are part of our daily life practices. From paying our bills via the Internet to walking in the streets

people are not really away from these surveillance mechanisms. From using a Gmail account to use a social media account enabling the system or the corporate mechanisms identify name registered on their ID card given to people by the state, new media is multi dimensionally under surveillance. It does not mean that people are ‘completely’ under the control of the government, since there is a ‘big data’ around and as seen during Gezi protests occurred in Turkey millions of tweets should be observed by states to gather a concrete data about identities of the users who are claimed to have committed a crime through new media.<sup>6</sup> Having recognized control of new media in Turkey as a threatening factor for digital activism, now I’ll observe technical and social methods which are often used by users with different experiences and different levels of anonymity. Firstly I will focus on softwares and other applications that provide anonymity for users. Later, I will cover social methods of providing anonymity. Lastly, I will clarify the differences between anonymity, semi-anonymity and pseudonymity with reference to the various methods used for anonymous use.

## **2.5 Perceptions of Anonymity**

Anonymity is a complex issue especially in social networks. People do not use anonymity only for political aims, but also used it as a method of entertainment. So, as this study focuses on political use of forms of anonymity as a strategy of resistance, we also have to define semi-anonymity's most well known form: Trolling.

Trolling is a critical issue in new media environment as trolling is

---

6

<http://www.hurriyet.com.tr/gundem/23509447.asp> [15/07/2013]

contemporarily being discussed in both political and academic environments in terms of its so called destructive characteristics. Semi-Anonymous and Anonymous personalities are possibly recognized as trolls and the term troll has no positive connotation in social networks. Except one who said "I am rarely a troll" none of the the interviewees stated themselves as trolls. This has several reasons such as interviewees political claims and their necessity to be politically recognized. However a Troller can be defined as a computer mediated communication user who constructs the identity of sincerely wishing to be part of the group, e.g. by professing or conveying pseudo-sincere intentions , but whose real intention(s) is/are to cause disruption and/or to trigger or exacerbate conflict for the purposes of their own amusement/entertainment (Hardacker, 2010).

This statement involves two key terms: Disruption and triggering a conflict. Those two terms act as trolls' main function in social media. Rather than organizing a political action, they are providing collective or interpersonal crisis in social media for entertainment rather than a political motive. Trolling involves some attitudes such as "impoliteness", "rudeness", "face-attack", "conflict". However these attitudes are easy to turn into "racism" and "sexism".<sup>7</sup> The disruption and dissemination of false information by them probably caused the interviewees not to state themselves as trolls. Since these politically active interviewees present a 'serious' identity which has the claim of recognition,

---

<sup>7</sup> E.G. Turkish rock singer Aylin Aslım and Journalist Ece Temelkuran had been targeted by trolls because of their statements on their Twitter accounts and collective troll account is perceived seriously by some groups and they became one of trend topics of the day for the days they are attacked by trolls. Ece Temelkuran is threatened with death through tweets.

As they differentiate themselves from trolls and they are not perceived as trolls by others, a problem of identification occurs for these users. There are some shared characteristics of semi-anonymous users with trolls such as their policy of not revealing their real names and photos, not associating their content produced to their revealed officially recognized identity's content productions. Several motives made interviewees keep their identities secret but they experience problems about defining their anonymity levels.

Taking trolls aside, semi-anonymous use of the Internet has other and mostly reactive motives, which we define as resistance.

## **2.6 Social and Technical Methods Used For Providing Anonymity**

There are some softwares and physical needs for being anonymous. The first focus point of anonymity is dividing your social networks from each other. A person who needs to be anonymous is expected for every new network that he/she adds to create new aliases. A person should create many aliases to communicate since the more aliases are possible the easier it is to manipulate and this can not be figured out that easily. For local security there are several sharewares for a person to keep himself/herself away from physical control. However, in terms of surveillance, the methods of avoiding control are different. For being totally anonymous, one should know that technology itself won't make a person fully anonymous or secure. There are certain anonymity types deployed which are categorized as Type-0 (anon.penet.fi), Type-I (Cypherpunks), Type-II (MixMaster), Type III (MixMinion), JAP, TOR and FREENET. As seen above there are different softwares and methods used for providing anonymous connection to the Internet, sending and receiving messages anonymously such as

HTTPS everywhere, OTR and TOR. Here are some of the explanations for the programs and systems used for providing anonymous usage of the new media.

**HTTPS everywhere:** This Chrome and Firefox extension provides encrypted browsing while encrypting communications with many major websites. While it does not protect users' identities nor hide the sites they are visiting, it provides people encrypted browsing. It is created as a result of collaboration between The Tor Project and the Electronic Frontier Foundation. (EFF.ORG)<sup>8</sup>

**Type-I (Cypherpunks):** The Cypherpunks remailer system, still in use today (APA-S, 2004), uses reply blocks to allow anonymous replies to emails. A reply block is a series of routing instructions that allow the message to be delivered to a pseudonym. These data are included in an anonymous message when sent, and then allows the recipient to reply, despite not knowing the identity of the sender. (Clark et. All, 2005, 34)

**Type-2 (MixMaster):** While Type-1 is thought to be open to the attacks of powers out of the network, type-2 is believed to be a more persistent way of communication. Just as it introduces fixed-length messages, with shorter messages being padded up to the message length and larger messages being broken up into multiple messages, this form defeats the trivial attack of following a message from sender to receiver by the size of the message. (Clark et. All, 2005, 34)

**OTR:** Encrypted chat (off the record) encrypts the communication, hiding it

---

8

<https://www.eff.org/https-everywhere>

from the network provider. Don't click verify if you have not actually verified. You do not necessarily know whom you communicate with even if it is verified.

**JAP:** JAP (2004) is an anonymizing proxy server developed and hosted at the Technical University of Dresden, with certain nodes on the network hosted by other Universities. The JAP software uses a mix cascade approach to provide anonymity, however the application of the network is geared towards low-latency requirements such as web browsing (Clark et. All, 2005, 35)

**TOR:** A browser that provides encrypted network address, anonymous network address and anonymous publishing. TOR (The Onion Router) has a gateway noise and output noise. Basically a user can see the entire TOR network as a link of routers. When a user enters the TOR network, TOR network will know who his/her identity but not what content it creates and or which links one wants to visit. TOR itself is not a sufficient form of using web safely if there are some social networks that you use dependent on the former accounts that aren't created in TOR. The details given through social media and all other content productions are the factors that TOR can not prevent you from doing. TOR only creates a 'relatively' secure model of browsing. (9 July 2013, Secure Internet Workshop at Kumbara Sanat)

Besides these technical and social methods of providing anonymity, advantages and disadvantages of anonymous use of the Internet must be taken into account. Wright and Stepney (2008) state advantages of Anonymity as preventing the formation of cliques in a network, or the exploitation of such cliques if formed outside the network and its well-known censorship-resistant properties. Adversely,

there are some limitations (disadvantages) caused anonymity. For instance, ability of a small set of users to identify themselves may not be enough to ruin the overall fairness of the network. The most important disadvantage of anonymous use is the lose of it, while "the loss of anonymity could have serious effects for a network that relies on anonymity for its overall behaviour" (Wright and Stepney, 2008: 5)

## **2.7 Semi-Anonymity versus Pseudonymity**

Semi-anonymity may be defined as, being included in a social network through different names and images rather than real names, locations and registered e-mail addresses of the users. Manipulation of an IP is not necessary for them, but IP manipulation is still considered as type of semi-anonymity as anonymousness not only prevents being found by [the](#) state or corporations but also it prevents them from seeing or obtaining the content derivated by them. What differentiates a semi-anonymous user from an anonymous user is the success of IP manipulation methods which are thought to be used by both groups. First of all, anonymity needs to be available in the network and the content created should be anonymously sent and received to be completely anonymous. For instance, Turkish Hacker group RedHack's connections to the some specific news channels such as Hayat TV, Ulusal TV and Halk TV are non-anonymous as one receiver's common details are available.

People using nicknames and avatars which do not reveal their own names on social networks that are not established by them can be considered as semi-anonymous users as they are still detectable by the state but they took [accuses](#) for being directly recognized by corporations and states through their profiles.

Semi as a prefix is used for this preference of anonymity or identifiability since people using such profiles show different characteristics such as trolling or political activity. However this research is focused on political individuals with semi-anonymous profiles rather than trolls whose aims are not avoiding social or political pressure but creating personas that do not reflect their own identities or political aims directly.

It is possible to define semi-anonymity as a way of political behavior rather than a preference about the name, avatar etc. What is the difference between semi-anonymity and pseudonymity? There is no simple and unified definition of anonymity. Pseudonymity is just a subcategory of semi-anonymity while it is a subcategory of anonymity at the same time. It is a preference based on giving away some types of information to users.

## Chapter 3

### **Political and Philosophical Background of Anonymity**

Since many academic studies focus on the control systems and their influences on society, most of the resistance based articles and studies are based on hacker culture rather than daily political culture and its influences on online practices of individuals (see Alternative Informatics Association, 2013). This thesis is one of the primary works in Turkey taking Baym's (2010) term of networked individual as one of the primary motives of the study and studies the tendencies and preferences of activists using new media. Taking the individual as the pioneer of political process and proposing the anonymity as a key actor in claiming direct democracy in groups with various sizes, study's political focus is on how lack of anonymity impacted the practice of democracy in people's relationships with each other, the NGOs or political parties they are members of and the state.

Without ignoring the term hacktivist, which means the activist that expresses himself/herself with hacking as a political action, the study is more interested in people who use social media for expression of ideas and organizing their political activities. Hierarchic mechanisms within activist groups even if they are integrated to web and how networked individuals are used for spying on behalf of the political organizations and how denunciator tradition of countries like USA and USSR emerged once again after decades in a so-called free new social movements. From McCarthyism (Freeland, 1985) to NKVD (Conquest, 1985) in-party control had always been used by governments and parties just as in today's political organizations. Not only in political groups or organizations, but also from families to companies, partners to roommates, many people utilize methods of surveillance. Defining anonymity as a resistance form against all the

sources of repression above not only political activists but regular pseudonymous users are involved in this research.

### **3.1 New Debates, New Politics, New Communities**

This Study does not perceive a member of counter culture as a neutralized figure, based on group hierarchy and discussions of radical democracy in new social movements between traditional socialist groups represented by Alex Callinicos and radical democracy defenders such as Laurie Penny (Gerbaudo, 2012, 18), it tries to reveal in-group control and in-group resistance within new social movements. This debate is more likely to be the conflict between old politics and new politics, which can be understood as a conflict between authoritarian scheme of Leninist organization model and new radical democracy. Laurie Penny's emphasis is more on leaderless 'multi-headed hydra' student movement, which resembles the organization models appeared in May-June protests in Turkey in 2013, while Callinicos' model represents the traditional action model. Both Penny's and Callinicos' statements are not that clear as long as we try to see these protests as protests coming from 'no where' as Thomas Nail (2013, 20) comes against as coming from no where means being nothing at all.

For Nail, the Occupy movement and all similar resistances have their roots in anti-globalization movements and in the cultures of the NGOs included in such protests even if the Occupy movements seem to be isolated, ephemeral and spontaneous and free from the previous resistance forms experienced. Nail (2013, 21) states that the Occupy Movement had borrowed three main characteristics of the Zapatistas: (1) Horizontalism, (2) consensus decision-making, and (3) the

political use of masks. As all these three practices signify both resistance against outsourced control and inner hierarchial mechanisms, these might be understood as the reasons of the necessity of the 'anonymity' in contemporary political practices.

Even if this debate had been more about the way protests on streets, it is actually based on formation of the political organizations and the way discussions are made. Hierarchial and leaderless formations are subjects of political and ethical debates in terms of in-group control and authoritarian mechanisms of social contracted groups. So in-group control should be examined as well. In-group control and global surveillance mechanisms are examined together, since thesis focuses on semi-anonymous user as a 'reliable' and 'free' Internet figure, who is relatively more liberated than a party militant or an activist with organic or inorganic connections and detected on social networks with his/her own identity by corporations, government or the hierarchial group he/she belongs to. As Penny argues (Guardian, 2010), "the new wave of activists has no interest in the ideological bureaucracy of the old left". What should be understood from this sentence should not be only about the demands of the old left but about the preferences of British youth such as not wanting to take orders and pay even a penny for a vacillating, pro-business party to be "voice of voters". It is a valid discussion for most of the representative democracies around the world.

The term self-organization is also used for understanding how new media reflects the preferences and structure of daily life as it is the re-creation or self-reproduction of society. By this approach, it will be possible to understand self-

organizing structure of new social movements and their members preferences that impact the nature of the new media environment.

Different from neoliberal hegemonic view, self-organization should be understood as an alternative method of building the society once again while instrumentalizing the new media. The last group of users are examined as the users who are under the control of the relationships they had in their private lives such as family connections or love-based relationships. So the categorization of control mechanisms will be under 4 main topics which are i) state, ii) company, iii) non-governmental organization and iv) private life. This new categorization will bring control to a new understanding which may create a new perspective for the understanding of hegemony in daily life as these are all parts of modern daily culture.

### **3.2 Resistance and Hegemony**

To get a better understanding of contemporary political new media environment, nature of the conflict within needs to be analysed. There are various definitions of hegemony. Gramsci is the first intellectual who completely conceptualized the hegemony for interpreting daily life and political practices. For him, education, political parties, working unions and all similar institutions were established for being resources of consent. His originality in hegemony studies is based on his extended definition of hegemony which not only involves administrative, executive and coercive apparatus of government, but also the underpinnings of the political structure in civil society. Gramsci is thought to have provided analytical usefulness for the categories of civil society and state (Cox, 1983, 52). His studies of hegemony has a qualitative difference between the operations of

hegemony by regressive, authoritarian groups on the one hand, and progressive social groups on the other. For him where a regressive hegemony involves imposing a set of non-negotiable values upon the people, chiefly through use of coercion and deceit, a progressive hegemony will develop by way of democratically acquired consent in society. This meant not only empowering the various unions by bringing them together, but also involving all of society's opposition strata in the movement, drawing out the connections between all forms of "political oppression and autocratic arbitrariness" (Brown, 2009). Gramsci's understanding of hegemony is not limited to the understanding of power and control of ruling class.

While Martin Clark (1977, p. 2) defines hegemony as "how the ruling classes control the media and education"; Lenin (1963, 86-87) states "the Bolsheviks needed to come to occupy a hegemonic position within the struggle against the Tsarist regime". His emphasis of hegemony was about the political leadership of the working-class in a democratic revolution. Gramsci's conception of hegemony is different from Lenin's and Clark's understanding of hegemony with its civil, daily and more comprehensive basis. The more contemporary, politically benefitable and Gramscian definition of hegemony was proposed by Raymond Williams. Williams (1977, 110) defined hegemony not only as "the articulate upper level of 'ideology', nor are its forms of control only those ordinarily seen as manipulation or indoctrination" but also "a whole body of practices and expectations, over the whole of living: our senses and assignments of energy, our shaping perceptions of ourselves and our world."

Following Gramsci and Williams' accounts on hegemony we can conceptualise the new media as a hegemonic environment, a sphere where dynamic nature of hegemony

can be observed. According to him; "hegemony equates consciousness with the articulate formal system which can be and ordinarily is abstracted as ideology" (Williams, 1977, 109-110). According to him:

“a static hegemony, of the kind which is indicated by abstract totalizing definitions of a dominant 'ideology' or 'worldview', can ignore or isolate such alternatives and opposition, but to the extent that they are significant the decisive hegemonic function is to control or transform or even incorporate them” (Williams, 1977, 112).

He emphasises that any hegemonic process must be especially alert and responsive to the alternatives and opposition which question or threaten its dominance (Williams, 1977, 113). Williams states hegemony has to reconstruct itself continuously like the men/women shape and change themselves accordingly. This is a positive factor that can provide opportunity for resistance from within hegemony and this is the reason why Williams' definition of hegemony was used while defining the political struggle from within hegemony or the new media environment.

Williams' focus on struggle between lower and higher classes is the base of his thesis that hegemony is not determined by the high class culture or state understating but a mutual process in which all of the actors are included in.

For his non-technodeterminist approach, culture as a network does not take technology as the primary power that can be used for foreseeing or inspecting all the things going on completely. However, Williams still insists on the advantageous uses of it (Williams, 1977). It can be stated that technology itself is limited to be a way of surveillance in today's academic environment but there

is still hope for technology to be used for the good and resistance of the people against the governance mechanisms. Williams' understanding of hegemony provides a theoretical basis for handling new media environment with a less pessimistic perspective as focus of contemporary new media studies are mostly based on surveillance and security systems enabled by corporations and governments in around the world and most of the academic studies focus on the geography or country that study is run in (See Alternative Informatics Association, 2013; Aytar and Çavdar, 2013). However, there are also studies which focus on on-going forms of resistance in terms of users' activism strategies (See Akin and Zıraman, 2013).

### **3.3 Political and Legal Necessity of Anonymous Use Of Internet**

“The Revolution Will Be Tweeted” is the first in a series of blog posts published by the Atlantic's Andrew Sullivan a few hours after the news of the protests broke in Iran. (Morozov, 2011, 1) And in Turkey's Gezi Protests one of the most common graffitis read as “the Revolution Will Not Be Televised.” Both approaches promote a ‘competition’ between the television and new media (specifically Twitter). Therefore, the possibility of scientific statement decreases and understanding of convergence and alternative media is completely ignored.

From corporate accounts to personal accounts, or from one personal account to another, what really matters in revolutionary processes is not only the media used, but also the way users or organisations used it. So we cannot evaluate a new media application as revolutionary. Likewise, television is a counter-revolutionary device just as government's initiation towards banning the broadcasts of Hayat TV, a television channel available on satellite and is

appreciated by protesters and followed by thousands of people during the resistance. Rather than the revolutionary character of the medium, hacker abilities of users and the way they construct their methods of personal or organizational security through their identifiability or anonymity preferences of new media is focused.

Returning to the role of new media in social movements, even in democratic countries people claim that the certain political opinions are persecuted, as it is clear from the existing oppression mechanisms used by Turkish Government which are stated above as well. There are numerous examples of use of new media for political activism, but each new media activism has different nature. Failure and success can be two possible outcome of the social media movements. Failure of the new media based protests in Belarus is an important example of how anonymity may prevent users from being sentenced by regime. Arrestments and sentences given to people in Turkey because of their messages on social media can be the example of how important anonymity can be for the new media activists or ordinary new media users.

In order to analyse political use of semi-anonymity and propose it as a method of resistance, we can rely on Zapatista movement, whose members identify themselves with a common mask used by them and which by the time became the symbol of the movement itself.<sup>9</sup> Subcomandante Marcos' famous statements about his identity can provide an understanding of semi-anonymity in today's political culture based on egocentric decisions of individual, as he identified himself with all the exploited, marginalised and oppressed minorities in capitalist

---

9

<http://www.heureka.clara.net/gaia/zapatistas.htm> [07/11/2013]

modernity.<sup>10</sup> Rather than choosing who he exactly is, his focus is more on the political struggle. During the research process, besides this aim of representation of oppressed minorities it is found out that semi-anonymous users' preferences also rely on their personal concerns caused by the daily control mechanisms.

### **3.4 Semi-Anonymity as a Proactive Resistance Method**

To understand semi-anonymity's use as a resistance artefact, it is necessary to understand the use of new media as a resistance tool. The information age is probably remembered with new production systems and methods it created, but it is also important to underline how it changed the social and political relationships within new media environment and daily life. With the rise of debates about Arab Spring, the new media technologies started to be named as the primary actors of especially Egyptian revolution. Conversely, documentation as a guide is distributed in [Egypt](#) in 2011. This guide is starting with the note "do not use Twitter or Facebook for distributing this note" and it is ending with the same note too (Madrigal, 2011). It is still a question that how effective social media is in Arab Spring, but it is visible that rise-up against the Mubarak is enforced by the time he cut off the Internet, as people had to go out on the street to know what is really going on.

According to Appelbaum, et. al. (2012), contemporary revolutions became successful and whoever used Twitter or Facebook have not been victims of their social networking activities yet. But, such a case is experienced in Belarus in 2006. After the street protests mostly organized by mailing ended after their

---

10

<http://www.goodreads.com/quotes/259994-yes-marcos-is-gay-marcos-is-gay-in-san-francisco> [07/10/2013]

failure President Alexander Lukashenko became more determined to control social media. The Red Shirt uprising in Thailand experienced such a failure, which ended with the death of dozens as well (Shirky, 2011). Anonymity of identities is a key actor for the security of the rebellions and resistance processes as developed control mechanisms create risks.

### **3.5 Technology as a Political Instrument**

At that point where new media is admired or cursed for its successes or its failures, Gerbaudo (2013, 8) suggests that "when social media are turned into a 'fetish' of collective action; in other words, when such media are endowed with mystical qualities that only obscure the work of the groups and organisers using them, ... the techno- visionary discourse on social media appears as the reflection of a neoliberal ideology, incapable of understanding collective action except as the result of some sort of technological miracle fleetingly binding together egotistical individuals." His criticism here depends on that technology is not only the instrument of the neoliberal system, but also people are capable of using technology for different reasons.

Gerbaudo's thesis mostly depends on collective action and how collectivity of the masses are mobilized through new media while Baym suggests the opposite. According to Wellman (cited in Baym, 2010, 90) a crucial social transformation of late modernism is a shift away from tightly bonded communities towards increasing networked individualism in which each person sits at the centre of his or her own personal community. Baym (2010,90) suggests that as the only messages that can be seen by all users are the ones sent by the sites themselves, none of the social networks are identical and all of them are

egocentric as we (people) prefer who we are following and who or what can follow us. By the way, according to Castells (2001, 54) "As virtual communities expanded in size and reach, their original connection to the counterculture weakened." Baym (2010, 91) is approving Castells' approach by saying that "Communities organized through multiple sites do not feel like places. Shared practices are less likely to develop when groups are spread throughout sites, " Baym's approach criticizing the so called necessity of Internet to be perceived as a way of building community is important as communities differ in terms of the content created on them even if they are produced by same users.

Users may prefer to be identifiable with different identities in different networks, just as in the cases of trolling or semi-anonymity. Before starting the discussions about the anonymity types, we need to continue discussing the nature of today's networks. Today's social networks are thought to be decentralized. Castells (200:15) states that apart from the rise of new technologies, the 'networking paradigm' is informed by the libertarian and participatory culture inaugurated by new social movements such as environmentalism, feminism and student movement. His emphasis on the lack of centres in networks is important as democratization of social movements resulted in a libertarian understanding where traditional hierarchical structures of social movements are broken.

### **3.6 Political Identification of Semi-anonymity**

From ethnical to ideological, political groups emerge on the basis of some easements. They even share profile pictures, source of news and a particular

language, some of them even still identify themselves as member of typical Leninist organization model or any other hierarchical model. But, their easements in shared values of the group does not result in barren discussions or monotype discourses. Semi-Anonymity provides them a security even within the democratic organizations they are involved in rather than the state they are opposed to. Here we see that, ID cards or registered names of the users are not only used by governments or companies for identifying the citizens but also by political organizations, working unions and such groups that use real names for surveillance of their users and put a totalitarian understanding into the practice.

This is a way used by most of the people for preservation of their positions in daily life. It is also possible for people who have been previously expelled from some political groups social in media networks to use these networks with new accounts only letting people they trust know their identities. This aspect is really important as it signifies the authoritarian structure of the new media groups no matter they are political or not.

### **3.7 Motives of Semi-anonymity**

Rather than professional concerns, it is possible for users to avoid using visible profiles for not revealing their privacy to their parents or other family members. So, taking family, state, professional life and political activism as some of the categories, cases below are going to be analysed to gather categorical data about attitudes of interviewees.

Bodle (2013,22) states that "Democratic and totalitarian alike nations-states monitor citizens' online communication and a mass big data on citizens. Law

enforcement agencies seek to lower the legal threshold to use information technology to track and convict criminals (e.g., GPS-enabled ubiquitous surveillance)." In this aspect, it is clear that communication in totalitarian or democratic states is a risky attempt. Even if it is still possible to communicate anonymously, day by day the powerful ad funded Internet industry advocates for real name only policies that are shaping an online environment that prohibits anonymous, non-identifiable communication by design. For instance, today it is difficult to create mail accounts via your personal computers without confirming your phone number or some other information which can be used as a reference to your citizenship ID. Observing Facebook's services such as face recognition and its relatively new service called Open Graph it can be stated that, users are connected to the Facebook all our web interactions are recorded by our Facebook accounts which are mostly registered on our names written on our id cards or the emails which are registered based on our officially registered cell phone numbers and accommodation information.

“Studies about anonymity systems typically assume that the anonymous users wish to be anonymous. This assumption is partially due to the natural view of anonymity as a method of somehow protecting users, and partially due to the sheer number of sources of information leakage in all but the most restrictive systems” (Stepney and Wright, 2008,3-4). This study focuses on the anonymity as a user preference rather than a 'forced condition' of Internet use, since the study handles the anonymity as a resistant model of Internet use.

It is known that anonymity and pseudonymity are expressly prohibited on the site with Facebook Terms of Use suspending and deactivating accounts based on

its strict real-name only policy. And this is not limited with Facebook as a social network. Google plus, is known to be the other company that avoids users from using pseudonyms in their accounts' registration processes (Markmann and Scott, 2005, 23). While restrictions of Facebook prevent users from providing false personal information or creating account for somebody other than one's self, also a person cannot create more than one personal profile, it is also impossible to create another account for a person if his/her account is disabled by Facebook. However, users can still create 'pseudonymous accounts' as Facebook still provides the opportunity of creating anonymous profiles. However, in any situation regarding Facebook administration, as no formal document can be presented regarding the anonymous name that you use, you won't be given service.

Zuckerberg -founder of Facebook- finds positives in Facebook's counter-anonymity approach. He states that Facebook's counter-anonymity approach disables the differentiation between working life and daily life. Zuckerberg is accused of being privileged since he is a wealthy, white, heterosexual male — in other words, someone who has nothing to fear from being transparent about his life, and no need to maintain two different identities (Ingram, 2010). This statement seems to be right as even legal political parties' Facebook fan pages are disabled by Facebook <sup>11</sup> and many individuals have been sentenced over their messages shared. Sentences an surveillance practices are not limited to the use of corporations. In Turkey, during the Gezi Resistance, Tekin Beyaz, who used to work for Kocaeli Municipality, reacted to the police violence which effected his mother through writing a message on Facebook, and he is firstly

---

<sup>11</sup> <http://www.etha.com.tr/Haber/2013/07/13/guncel/bdpnin-facebook-hesabi-kapatildi/>

demoted from his position in municipality and then got fired.<sup>12</sup> Also, Alev Toprakođlu, who is a scriptwriter, is fired from the copywriting team that she is involved in because of her messages in Facebook regarding the policies of the prime minister.<sup>13</sup> In all these examples, it is seen that Facebook's transparency and counter-anonymity policies are for the advantage of controlling mechanisms of both states and the companies. So, through social networking experiences, it is easy to state that deanonymization of the social network profiles can be defined as a systematic attempt to block any political activism movement that can rise through these networks and from political parties to less political citizens, everyone without anonymous profiles are controlled by these social or technical mechanisms in Turkey. Besides the disadvantages of visible or non-anonymous uses of social networks, methods and advantages of using social media anonymously should be focused.

---

<sup>12</sup> <http://www.Internethaber.com/facebookta-gezi-mesaji-isinden-etti-556149h.htm> [Access Date: 08/11/2013]

<sup>13</sup> <http://www.hurriyet.com.tr/magazin/televizyon/23598748.asp> [Access Date: 08/11/2013]

## **Chapter 4**

### **Methodology**

#### **4.1 Research Model**

In this research, 13 twitter users tweeting mostly in Turkish are included in an online ethnography in order to understand why do people, that create content in social networks in Turkish, prefer profiles that do not reveal personal information about themselves and what are the motives lying behind their non-visible use of social networks. Besides online participatory observation, secondary sources are used to create theoretical basis for research and some semi-structured interviews are designed and made with 8 of the users whose nicknames are @kafa\_radyo, @Przykazan, @Myriamonde, @KuntaKinteden, @kafa\_radyo, @\_kullanici\_adi, @13melek, @xisor\_yasoo on Twitter. These methods are chosen for not to hurt users' preferences of identity through physical, face-to-face contact; for becoming objective while observing their judgements of themselves and for being able to observe the content they produced in public mode. Online participation model is preferred as being in the same social community with these users would make it easier for research to detect weaknesses of anonymity layers for users and analysing users in their networks. Secondary sources are used for gathering explanatory information about theoretical background of anonymity and collecting more data about technical forms of providing anonymous use of computers.

For stating the technical conditions of anonymity, I met with a hacker, whose positions are assumed to be illegal by states. Meeting is arranged by other hackers. During the meeting, he did not give away any information about his identity including his name, nationality, occupation, nickname etc. He made some

statements about the softwares that hackers use for providing anonymity. I benefited from his technical methods while collecting detailed information about both social and technical tactics used for being anonymous.

Eight users whom I supposed as semi-anonymous, have directly attended the process through semi-structured interviews which are done through Google Hangout and E-mail. The reason why Google Hangout and E-mail are used during the research because this is a new media research over users who try to provide a kind of invisibility for themselves and their identities in social networks. Face to face interview is not preferred as a method since it is assumed to create a negative effect towards the answers of the interviewee and research's nature as a new media field research. None of the interviewees are asked for face-to-face interviews. Because of the advantages of online questionnaires such as including their ease of storage, retrieval, and qualitative analysis interviews are done through e-mail. Also, e-mail interviews are known to be advantageous for reaching the users who could possibly hesitate face-to-face interview for various reasons (Murthy, 842). Semi-structured interviews are mostly composed of open-ended questions. Since "meanings are constructed by human beings as they engage with the world they are interpreting. Qualitative researchers tend to use open-ended questions so that participants can express their views" (Crosswell, 2003, 9). Therefore, open-ended questions have been used through the interviews. A list of identical questions are asked to all interviewees in addition to which some extra questions are asked to the respondents in order to get further details of cases they are involved in. Open-ended nature provides the chance of getting more detailed information about the inquiries of users.

One of the users observed refused to answer questions for interviews. Accordingly, data obtained from online participatory observation is used for one of the case studies covered as this case is inspirational for studying forms of anonymity. There are two important cases regarding three of the interviewees which is the revelation of their identities through Twitter and Ekşi Sözlük. Rather than analysing security of the social networks mentioned, security of the social network and users' network building processes is analysed for theorizing the forms of anonymity and identifiability together. Softwares used by interviewees are also questioned regarding defining the level of anonymity for users.

As a part of this research in order to get an overview, I followed the users included in the research for 4 months before the interviews and analysed the tweets they sent since they began tweeting for determining their loyalties to the necessities of anonymity. One specific case is experienced regarding revelation of the personal data of the users involved in research.

## **4.2 Research Context**

Nine of eight users observed in this research are selected as they are pseudonymous activists on Twitter, who ordinarily send political messages. The reason why they are chosen as interviewees is the fact that some of these users meet and act together in daily life for political events and they all have political identities that they do not completely 'define' as troll and they are not named as trolls by others and their existence and actions on new media can be perceived as political activism. Trolls, who are often defined as manipulators of regular flow of content production in social media, are defined through the answers of the

interviewees. Their tendency of manipulating a content flow for joy, as defined in the analysis chapter, and their use of language are the other factors that made the study exclude them from being taken as samples.

In order to analyse users' attitudes towards staying anonymous, different and previously stated categories of motives that brought about the necessity of anonymity are covered.

The users that are involved in research are not 'twitter phenomenons' or the ones that previously gave interviews to digital or hardcopy magazines. None of them have been on conventional media with their 'twitter identities' and they have never revealed their own names or photographs in their profiles.

The user that did not respond any of the interview demands are analysed regarding the content he/she produced and cases he/she is involved in. These are neither 'twitter celebrities', who are believed to create content for cyber prestige which we can define with number of followers and high levels of interaction, nor figures that are physically identifiable with their nicknames or their profiles on social networks in conventional media. He/she is not troll either. He/she does not intentionally create manipulative contents regarding the profile they created. They are politically active figures as well.

Different types of information is sought during the research. To understand the users' ability to use the Internet technologies 'anonymously' and create a kind of measure for the anonymity levels of the users. Their preferences of softwares and freewares are made focusing on the use of Internet anonymously. This

information is planned to be used afterwards for drawing the lines of distinction between anonymity and semi-anonymity. Also users' statements about themselves are taken into consideration for identifying possible 'trolling' activities that could impact presumptions about users political situations and their relationship with the hegemony.

Resistance from within hegemony does not necessarily mean that users are supposed to use artefacts of oppression that targeted them. However, hacker culture is a part of information society and it is directly related to computer culture and cyber culture's backlog. Besides these, digital activism's most popular form is hacking as seen in the examples of RedHack or Anonymous. Hacker is a widely discussed term in terms of digital activism in Turkey especially because of the Redhack case. There are several types of hacktivists and there are several dimensions of hacking. Therefore, users definition of themselves as 'hackers' has been questioned to understand the possible similarities assumed between types of anonymity and hacker culture.

Political, familial, interpersonal and economical concerns are four categories used for understanding main motives that made people use their profiles anonymously. While asking the interviewees the questions interviewees have been given opportunity to choose more than one of these categories as hegemonic is available in different parts of life and different levels. Since the focus point of the research is the safe use of the Internet and 'anonymity' of the users, anonymity and identity revelations have been the key points of the research. Rather than people's personal 'feelings', their experiences are taken into consideration while preparing semi-structured interview and observing twitter

profiles of users selected.

In next chapter, observing the interviews made, semi-anonymous and non-anonymous uses of Internet will be analysed. Starting from users' own perceptions of anonymity, taking philosophical and practical characteristics of anonymity with reference to Chapter Two and Chapter Three, a new perception for the forms of anonymity will be proposed with the users self-experiences of anonymity and semi-anonymity.

## **Chapter 5**

### **Experiencing Various Forms Anonymity and Identifiability**

#### **5.1 Interviewees' Perceptions of Anonymity**

All of the interviewees involved in this study are all aware that, their identities can be found through several ways such as company-state cooperation and finding out linked social media accounts of themselves. Most of the users define themselves 'partially' anonymous as they are aware about control and surveillance mechanisms over their Internet use and their lack of security in connecting to others. Only one of the interviewees stated himself as anonymous in terms of using a nickname rather than real one. Others have different definitions of anonymity for themselves such as 70% anonymous, quarterly anonymous, used to be anonymous, and semi-anonymous. But except one, they all have worries about the privacy of their accounts and their security against estates of repression. And as it will be seen below, these estates of repression reveal weaknesses of semi-anonymity.

#### **5.2 Weaknesses of Semi-Anonymity**

A complete anonymity that is provided by network anonymity is not also possible for the interviewees as it is experienced in @demet\_kuzey case who used to be a semi-anonymous user who only used to use her first name without profile picture or any similar revealing information, before Melih Gökçek, Mayor of Turkish Capital, revealed her real identity after reaching her real identity information through people that she followed. This revelation of identity is a result of political discussion. This brings about the problem of anonymity of networks.

Another example is the case of @Narlaincir. @Narlaincir is one of the effective pro-Kurdish militant figures in Twitter as her tweets and statements create 'agendas' and she is also one of the interviewees involved in this research. She is one of two interviewees whose names are revealed by their 'political rivals'. Ceng Sağıncı, a pro-Kurdish politician living in Israel, is firstly criticized by Narlaincir and the community she belonged to. After such criticisms, Ceng Sağıncı revealed Narlaincir's name and surname, and her position in political organization she is part of (see p. 89). This is not the first time her real identity is reported. Another example of revelation of 'real identity' for her is experienced in 15 March 2013 by another user, @AybikeHatemi (See p. 90). She is also reported to the other people that she is organizationally responsible to in 2012.

### **5.3 Reasons of Semi-Anonymous Use**

@Narlaincir states she is not 'semi-anonymous' nor 'anonymous' any more as her identity is revealed. She defines her anonymity type as a position that dignifies the content created rather than whoever stated it. She states that, the main reason that made her stay anonymous is the political pressure of the organization that she belongs to. She states that after her real identity is revealed, she opened a new and protected anonymous account to be more secure. But she is still worried about revelation of the tweets that she sent through this account.

Another source of repression is the social pressure that is result of the relationships with family, [neighbours](#) and friends or partners. @Przykzn as a female user, defines her motive of anonymity with social pressure category. She states that, she would have also been fired if she did not use the Internet

anonymously. For her people need one more social media account to keep themselves anonymous from their primary friend and family circles that surround them in social media.

@AugustusHill is another interviewee who defines the primary reason of his anonymity as state pressure which is enforced with surveillance systems such as DPI and censorship. He became actively involved in social media as a semi-anonymous user after he faced some problems with his family members because of his political ideas. He also defines his anonymity's unique advantage as hiding the tweets he sent from his parents as he faced both warning of the security forces and their pressure on his family. He states that anonymity is much more popular in pre-Facebook era and he links neoliberal transformation of daily lives with revelation of 'real data' on Internet. Returning to the oppression that made him use 'semi-anonymous' profile he tells about two main cases. The first one is the time his family is warned by police by the time his tweets are recognized by state forces. This is the first time he is warned by his family. The second is also about his family but also about mostly 'political' and 'impolite' messages that he sent through twitter.

@Kuntakinteden is an another semi-anonymous user who defines his anonymity motive as the pressure caused by commercial links but he states that his concerns are linked to other categories as well. His name is revealed through Ekşi Sözlük and he is threatened and insulted by the users revealed his nickname. Because of these insults and threats, he defines the advantage of being semi-anonymous and not having been known by other users physically as not having been attacked by someone. He also states that his semi-anonymous

personality is much more brave than him. It creates a capability of action for him. The other example of commercial links' pressure on users is @13melek who is a semi-anonymous activist. While not defining himself as a Hacker, he used Hotspot Shield during Gezi protests. He states that he is not anonymous as his accounts are linked to e-mail accounts that are revealing his name and surname. He defines his 'primary' reason for using an anonymous name as commercial links that are results of his relationship with the establishment he is working for. His secondary reason is his demand to stay anonymous against his family members. He perceives the state-driven pressure as the one feeding all these pressures. His identity information has never been revealed before. He is an active 'citizen journalist' in Gezi process and he states that his semi-anonymous identity relaxed him while tweeting or broadcasting.

Some of the users defined the sources of pressure that made them use semi-anonymous profiles with all categories which are commercial, political, social and state based stating that put pressure on them. @Kafa\_radyo is one of these users. He states that he never faced a problem regarding the content he semi-anonymously created. Some of the methods he assumed to provide his anonymity are HotSpot Shield and Google Public DNS. His definition of himself as 70% anonymous reveals his suspects about his anonymity.

@\_kullanici\_adi\_ revealed his reason of staying anonymous as state pressure on him. Never facing a problem about content created semi-anonymously, he mentions the liberating potential of semi-anonymous identities.

#### **5.4 Hacker Culture and Anonymity**

None of the interviewees defined themselves as hackers while one of the users confessed 'hacking' a MSN account earlier by the well known methods which are published on forums. So they do not call their activities on web 'hacking' activities, so they can not easily be named as hacktivists as they do not define their activities on web as hacktivists. Regularly accepted rules of hacker society involve the necessity of anonymity. However the research revealed that except three of ten interviewees, none of these users have access to softwares and applications that are used for anonymous connection either.

One of the most important issues in today's academic discussions is the surveillance systems used for controlling and designing new public sphere. While some of the users 'contemporarily' used softwares for keeping their identities anonymous, majority of the users included in this research revealed that they did not use any of this programs. Some of the programs used by interviewees are HotSpot Shield, Google Public DNS, and Spotflux. None of these are sufficiently designed for keeping the identities of users anonymous. Also, network anonymity rules are not provided by any of these users. DPI or in-agency softwares used by companies are able to control the contents created and submitted easily. From IP detection to detection through 'e-mail links', many different methods might be used for controlling their Internet browsing activities.

### **5.5 Advantages / Disadvantages Of Anonymity**

1991 is a milestone for a message that expanded the discussion of autonomous, anonymous culture zone in Internet. Message is written by Hakim Bey:

In the face of contemporary pecksniffian anaesthesia we'll erect a whole

gallery of forebears, heroes who carried on the struggle against bad consciousness but still knew how to party, a genial gene pool, a rare and difficult category to define, great minds not just for Truth but for the truth of pleasure, serious but not sober, whose sunny disposition makes them not sluggish but sharp, brilliant but not tormented. Imagine a Nietzsche with good digestion. Not the tepid Epicureans nor the bloated Sybarites. Sort of a spiritual hedonism, an actual Path of Pleasure, vision of a good life which is both noble and possible, rooted in a sense of the magnificent over-abundance of reality. <sup>14</sup>

His thesis of a so-called soul of Nietzsche with good digestion did not realize itself in daily life. Today, all the positive connotations of anonymity have been terrorized by states and other parts left are somehow politically or interpersonally discredited by trolling activities under these identities. So today; anonymity has both advantages and disadvantages while it is still a gray area for users.

According to interviewees, several advantages of semi-anonymous identities are:

- Avoiding the necessity of self-censorship.
- Helping them use a name in their native language, rather than the one they are forced to.
- Meeting new people in easier way.
- Avoiding outsourced pressures and providing freedom of expression.
- Being able to follow or unfollow people in social networks regardless of daily relations.
- Behaving liberated from the norms of public sphere.

---

<sup>14</sup> [http://canopycanopycanopy.com/15/anonymity\\_as\\_culture\\_\\_treatise](http://canopycanopycanopy.com/15/anonymity_as_culture__treatise)

- Being able to behave liberated from the concerns that statements on social media would affect family members.
- Being able to express one's self without the concern of financial interests such as employment etc.
- Not being attacked physically by other users or people because of his/her ideas.

There are no 'serious' disadvantages of anonymity according to users. But while some of the users state that it made it 'harder' to meet with new people, some stated otherwise. But especially as @Narlaincir stated, even if people are semi-anonymous, they might have to create new 'semi-anonymous' accounts for themselves to provide a more liberated area.

## **Chapter 6**

### **Conclusion**

Three main focuses of this study are unconsciousness about unclear motives of anonymity, technical practices and terminology of anonymity. Concluding these three themes using the findings of the research, the thesis finalizes with a proposal of anonymity as a new medium for organizing direct democracy in various sizes of communities.

#### **6.1 Semi-Anonymity: A Social Preference**

Starting from the idea, resistance from within hegemony, covering Twitter as the space of resistance and oppression at the same time, social media had been covered without denigrating nor subliming the media itself. Rather than characteristics of web 2.0 and controllers' methods of controlling, indomitable users' preferences are the focus point of the article. This thesis assumes a categorization of the motives that revealed the necessity of anonymity, the interviewees did not seem to confirm this hierarchic structure while the categories chosen are sanctified by interviewees.

Economic, in-group (NGOs, political parties etc.), family/private life based and legal or state based pressures can be regarded as dominant forms of repressions that caused need of resistance. Moreover, several different forms of motivation such as habits from 1990s' Internet and need of collective identity should be added to the categorization of semi-anonymity motives. So these categories of motives should be expanded in further studies in a more detailed framework.

## **6.2 Semi-Anonymity: Technical and Theoretical Proposal**

The other focus point of the study is the terminology of anonymity and necessity of a new category. None of the interviewees feel themselves completely anonymous and their definition of their 'anonymity' status is defined as half anonymous, quarterly anonymous, 70% anonymous or "not anonymous any more" etc. While users do not have the unique description of anonymity, their statements about their 'lack of complete anonymity' or their insufficient level of anonymity proved the necessity of a new category. Network anonymity seems to be the most critical layer of anonymity as most of the discloses are caused by network anonymity weaknesses as seen in the cases of @demet\_kuzey and @narlaincir.

Describing a new category is not possible based only on the statements of the interviewees. For conceptually designing anonymity and semi-anonymity, some layers should be defined for both. Users' definitions of themselves, programs and applications used, users' network anonymity are three main categories that can be used for defining layers of anonymity. Most of the interviewees and most of the users with pseudonyms are aware that they are not anonymous. To clarify anonymity there is a necessity of another layer of anonymity: Softwares and programs used for anonymity which means technical background of anonymity. While case studies and interviewees made revealed that, more than 'technical' anonymous hunting, social forms of chasing are used for identifying pseudonymous users, it is still important to provide necessities of anonymous use for creating totally anonymous use of anonymity.

Interviewees rarely know about these 'technical' methods of providing anonymity

and users of such programs are seen to be temporary users for politically active periods. Research revealed that, use of semi-anonymity is caused mostly by need of contemporary anonymity or invisibility, and most of the users experiencing semi-anonymity are aware that their positions in controlled societies are not safe regarding existing methods of surveillance. Users rarely know about these 'technical' methods of providing anonymity and the ones using such programs are temporary users for politically active periods.

So, this study has provided a red line between the anonymity and semi-anonymity in a technical and theoretical background in order to avoid possible political failures of activists as seen in the examples of Egypt, Thailand and Turkey.

### **6.3 Political Future and Use of Anonymity and Semi-Anonymity**

The debate about anonymity is also debate about the clarity of new political structure and how the communicational structure will be influenced by the new media technologies. In order to conclude anonymity's and semi anonymity's political aspects, it is necessary to use the terms of new politics as well. With reference to new social movements, Michael Hardt and Antonio Negri published a book, which is thought to be the communist manifest of our age by numerous intellectuals. Their focus on opacity of relationships and formation of leaderless communities create the necessity of non-hierarchic communicational and political structures and this study proposes its communicational methods to the service of new democracy. At the end of their text, "Declaration" Hardt and Negri (2012) state that:

“We need to empty the churches of the Left even more, and bar their doors, and

burn them down! These movements are powerful not despite their lack of leaders but because of it. They are organized horizontally as multitudes, and their insistence on democracy at all levels is more than a virtue but a key to their power.”

Their statement has been a political motivation for this study as anonymity and semi-anonymity should be perceived as methods for providing horizontality, which is defined as one of the political outcomes of anonymity.

Social networks are spaces of expression and organization rather than spaces of action. Activists come together, organize and discuss through new media. However, new media is an instrument which reorganizes the forms of relationships between the activists. The leaderless movement term, which is associated to new social movements is mostly because of this Web 2.0 evolution, which is thought to be a democratic communication based revolution. Anonymity's role in establishment of these relationships is the elimination of biases, prestige advertisements, image cultivation, hierarchic statuses. Therefore, after establishing a collectivist, horizontal and secure definition of anonymity, it is necessary to define commoners, which is the key term that the study uses for establishing a connection with anonyms or semi-anonyms. “Commoners’ task is not only to provide access to the fields and rivers so that the poor can feed themselves, but also to create a means for the free exchange of ideas, images, codes, music, and information” according to Hardt and Negri (2012) and it is not limited to the access to and self-management of shared wealth but also the construction of forms of political organization.

Here, anonymity is provided as a way to common, which can be regarded as a

form of making the experience of political communication more collective and participatory. Through the elimination of biases, a more liberated form of decision making will be possible. Based on this study, it is understood that people eliminate many forms of control in their lives through their semi-anonymous use of the Internet. From voting to discussions in forums, anonymity's uses always helped people express themselves more directly and free from the manipulations or directions of the control mechanisms in their lives.

The forms and definitions of anonymity provided here are not proposed only for the use of activists but also daily political practices of states and citizens. As seen on Gezi Resistance, plebiscite had been proposed by governments as a way of political and collective decision making. However, in Turkey, it is well known that voting behaviours of citizens are controlled by political parties and voting is proposed as a condition of being served by local governance or the government in major level.

Most of the people feel under pressure because of voting statistics' possible impacts on their daily life. This is not limited to behaviour of voting. Self-expression is another problematic aspect of capitalist modernity that we experience today. While making a discussion over a topic, interpersonal or economical relations create a pressure over people. The main paradox of capitalist democracies, which might be defined as the conflict of political interests and economic interests should be solved by putting anonymous expression and voting services into practice. Anonymous or semi-anonymous users, as commoners, are anticipated to participate as the role models of ideal participatory and radical democracy models, and their use of Internet will not be

limited to forms of activism, hacking or security protocols.

Anonymity and semi-anonymity would provide citizens' access to political decision making processes in a secure, unlinkable and unobservable way, which will eliminate the conflicts that capitalist structure of the states caused in political or non-political decision making processes that people experience regularly.

Therefore use of anonymity and semi-anonymity within and from hegemony is expected to create a new and more democratic environment for both resistance and contemporary daily politics. This environment is not anticipated to be identified just with illegal resistance forms any more. Moreover, anonymity and semi-anonymity as forms of political self-representation are expected to get more reputation, interest and popularity among the users.

## REFERENCES

- Alternatif Bilişim Derneği, 2013. *Türkiye'de İnternetin Durumu – 2013*. [online]  
Available at: <<http://bit.ly/14Sxjcd>> [Accessed on: 12 May 2013]
- Alternatif Bilişim Derneği, 2013. *Veri Korumaya Giriş*. [online] Available at:  
<[http://ekitap.alternatifbilisim.org/files/veri\\_korumaya\\_giris\\_edri\\_paper\\_06\\_tr.pdf](http://ekitap.alternatifbilisim.org/files/veri_korumaya_giris_edri_paper_06_tr.pdf)> [Accessed on: 12 May 2013]
- Akin, A., Zıraman, E. "Türkiye Çevrimiçi Alanında Güç Mücadelesi Ve Üç Tarz-I Muhalefet: Redhack, Alternatif Bilişim Derneği Ve Youtube Yasağı Karşıtı Bireysel Girişimler." Karaburun Bilim Kongresi: Sosyal Medyada İktidar ve Dayanışma Oturumu. 5 Eylül 2013.
- Appelbaum, J., Assange, J., Muller-Maughn, A., Zimmermann J., 2012,  
*Cyberpunks - Freedom and the future of the Internet 2012*.
- Arslantaş Toktaş, S., Binark, M., Dikmen, E. Ş., Fidaner, I. B., Küzeci, E.,  
Özaygen, A., 2012. *Türkiye'de Dijital Gözetim: TC Kimlik Numarasında E-Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi*. İstanbul: Alternatif Bilişim Derneği yayınları.
- Aytar, Volkan; Çavdar, Ayşe. 2013. *Medya ve Güvenlik Sektörü Gözetimi: Sınırlar ve İmkanlar*. [online] Available at:  
[http://www.academia.edu/207440/Medya\\_ve\\_Guvenlik\\_Sektoru\\_Gozetimi\\_Sinirlar\\_ve\\_Imkanlar](http://www.academia.edu/207440/Medya_ve_Guvenlik_Sektoru_Gozetimi_Sinirlar_ve_Imkanlar) [Accessed on: 10 May 2013]
- Brown, Trent (2009). be
- Castells, Manuel (2012). *Networks of Outrage and Hope*. Cambridge: Polity Books.
- Clark, M. (1977). *Antonio Gramsci and the Revolution that Failed*. New Haven: Yale University Press.

- Clark, John A.; Jacob, Jeremy; Stepney, Susan; Wright, Joss (2005). *Designing Anonymity: A Formal Basis for Identity Hiding*. . [online] Available at: <http://bit.ly/16eQmNw> Reach date: 29<sup>th</sup> July 2013.
- Coleman, Gabriela (2011). *Anonymous: From the Lulz to Collective Action*. [online] Available at [http://www.rezoanonymous.eu/IMG/pdf/anonymous\\_from-the-lulz-to-collective\\_action.pdf](http://www.rezoanonymous.eu/IMG/pdf/anonymous_from-the-lulz-to-collective_action.pdf) (Accessed on: 24th August 2013)
- Conquest, Robert (1985). *Inside Stalin's secret police: NKVD politics, 1936-1939*. Hampshire: Macmillan.
- Cooper, Alisa (2011). [online] Available at: <http://www.alissacooper.com/wp-content/uploads/2011/10/DPIchapter.pdf> (Accessed on: 29th June 2013)
- Cox, Robert W. (1983). "Gramsci, hegemony and international relations: an essay in method." *Millennium-Journal of International Studies* 12.2 162-175.
- Crosswell, John W. (2003). *Qualitative, Quantitative, and Mixed Methods Approaches*. London: Sage Publications
- Doering, Nicola. 2002. Studying online-love and cyber-romance. In *Online social sciences*, ed. Bernard Batinic, Ulf-Dietrich Reips, and Michael Bosnja, 333–356. Goettingen: Hogrefe
- Freeland, Richard (1985). *The Truman Doctrine and the origins of McCarthyism: Foreign policy, domestic politics, and internal security, 1946-1948*. New York: New York University Press.
- Fuchs, Christian. 2012. *Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society*. [online] Available at: <http://bit.ly/NwosT4> [Accessed on: 24 2013]

Fuchs, Christian. 2009. Information and Communication Technologies. *European Journal of Communication* 24.

Google Transparency Report, 2013. Available at:

<http://www.google.com/transparencyreport/removals/government/TR/>

[Accessed on: 12 May 2013]

Gramsci, A. (1971). *Selections from the Prison Notebooks of Antonio Gramsci*, Q. Hoare & G. N. Smith, eds. & trans. London: Lawrence and Wishart.

Hansen, Marit; Köhntopp, Marit; Pfitzmann, Andreas. *Anonymity,*

*Unobservability, Pseudonymity, and Identity Management – A Proposal for*

*Terminology*. [online] Available at: <http://dud.inf.tu->

[dresden.de/literatur/Anon\\_Terminology\\_v0.18.pdf](http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.18.pdf) [Accessed on: 20th

August 2013]

Hardacker, C. (2010). Trolling in asynchronous computer-mediated

communication: From user discussions to academic definitions. In *Journal of Politeness Research* 6 (2010), 215 X 242.

Hardt, M., and Negri A. (2012). *Declaration*. Melanie Jackson Agency.

Hood, Christopher 2006. The Tools of Government in the Information Age in *The*

*Oxford Handbook of Public Policy*. Eds. Goodin, Robert; Moran, Michael;

Rein, Martin. New York: Oxford University Press.

Ingram, M. (2010) Are Facebook's Views on Privacy Naive and Utopian?.

*GigaOM*, [online] Available at: <http://gigaom.com/2010/06/01/facebooks-views-on-privacy-are-naive-and-utopian-prof-says/> [Accessed on: 10

December 2010]

IPIS KMG, 2012. *Türkiye'nin İnternet Kullanım Haritası*.

- Landau, Susan E. 2010. *Surveillance or security? The risks posed by new wiretapping technologies*. Cambridge: MIT Press.
- Lenin, Vladimir I. (1963). *What is to be Done?* S.V. Utechin & P. Utechin, trans. Oxford: Oxford University Press.
- Lyon, David 2009. *Identifying Citizens: ID Cards as Surveillance*. : Polity Press.
- Madrigal, Alexis C. 2011. Egyptian Activists' Action Plan: Translated. *The Atlantic*. [online] Available at < <http://bit.ly/XXFQGz>> [Accessed 08 March 2013]
- Marcuse, Herbert 1972. *Counterrevolution and Revolt*. Boston: Beacon Press
- Markmann, Kris M.; Scott, Craig R. (2005) *Anonymous Internet? Examining Identity Issues in Email Addresses*. [online] Available at <http://bit.ly/18JBIOz> [Accessed on: 20 August 2013]
- Morozov, Evgeny 2012. *The Net Delusion: The Dark Side of Internet Freedom*. Public Affairs; Reprint edition.
- Murthy, D. 2008. Social Research Digital Ethnography : An Examination of the Use of New Technologies for Social Research for *Sociology Volume 42 Number 5*.
- Nail, Thomas. “Zapatismo and **the** Global Origins of Occupy,” in *Journal for Cultural and Religious Theory* vol. 12 no. 3 (Spring 2013): 20-35.
- Shirky, Clay. 2011. The Political Power of Social Media. *Foreign Affairs* vol. *January/February*.
- TÜİK, 2012. *Hanehalkı Bilişim Teknolojileri Kullanım Araştırması*. [online] Available at: <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880> [Accessed on: 27 March 2013]
- Webster, Frank. 2006. *Theories of the Information Society*. York: Routledge.
- Williams, Raymond. 2012. *Marxism and Literature*. York: Oxford University

Press.

Penny, Laurie. *Guardian*. Out with the old politics. <http://bit.ly/18HtgPa>

[Accessed on: 20 August 2013]

TÜİK, 2012. Hanehalkı Bilişim Teknolojileri Kullanım Araştırması. [online]

Available at: <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880>

[Accessed on: 20 August 2013]

## APPENDIXES

### Various Softwares and Freewares Used For Anonymous Identity

#### Profiles of Semi-Anonymous Twitter Users Involved in This Research:

**@Narlaincir:** With 1727 followers and 375 accounts followed; @Narlaincir as a twitter user demonstrates a mixed profile. Her account is time by time protected and time by time public. She does not reveal her real picture and real identity that much. She has made 7894 updates in Twitter so far. She dominantly prefers tweeting in Turkish. She has tweets in Kurdish and Arabic as well. She has not revealed any personal information on her twitter bio and in her tweets observed since December 2011.

**@Myriamonde:** She tweeted over 57 thousand times so far. She is an activist who is one of the well known reporting figures in #occupygezi process. She tweets in two languages which are English and Turkish.

**@AugustusHill:** With 428 followers and 464 people that he follows, AugustusHill has a public profile that represents a 'political' identity. Except his 'location information' he did not reveal any private information about him on his tweets.

**@PrzyKazan:** With 375 followers and 459 people she followed, PRZYKAZAN tweeted over 11000 times so far. She uses Turkish, Kurdish and English in her tweets.

**@KuntaKinteden:** Sending 120.759 tweets so far, and being follown by 2580 people, @kuntakinteden is a well known figure in Twitter. He did not reveal any information about his identity so far.

**@13melek:** This user sent over 15000 tweets so far. Being follown by over 5000 people he has not revealed any personal information on his twitter bio and in his tweets observed since September 2011.

**@\_kullanici\_adi** 91 followers, 476 people that he followed, 1040 tweets. Never revealed his e-mail until today.

@kafa\_radyo 3895 followers, 220 people followed.

@xisor\_yasoo 1526 following, 1821 followers

@KuntaKinteden 2580 followers, 2892 following

### **Records of Answers by People Included in Research**

Interview with @kuntakinteden is made on 8<sup>th</sup> October 2013 through e-mail.

**Kaç yıldır Internet kullanıyorsunuz?**

10 yıl

**Kendinizi bir hacker olarak tanımlar mısınız?**

Hayır

**Cinsiyetiniz?**

Erkek

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri neler?**

Hayır

**Hangi sosyal ağlarda hesaplarınız var?**

Facebook, twiter, ekşisözlük

**Facebook'unuzun ve Twitter'inizin kayıtlı olduğu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Evet

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Anonim değil IPS'ten tespit edilebilir

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Evet

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

Ticari bağlardan oluşan baskı (Şirket vs.)

Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)

Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)

Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)

Hepsi ile bağdaşıyor

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Devletle değil ama şahıslarla kısmen (kimliğim ifşa edildi) Bir kaç kere tehdit edildim, hakaret edildi.

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Dayak yememek:)

**Kimliği saklı profil sahibi olmanın avantajları nelerdir?**

Oto sansür ihtiyacını ortadan kaldırması

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Tam olarak değil, o daha cesur

**Kendinizi troll olarak tanımlar mısınız?**

Bazen:)

Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?

Kesinlikle bir mahalle baskısı oluşturuyor

**@xyasino0**

Interview with @xyasino0 is made on 12<sup>th</sup> October 2013 through e-mail.

**Kaç yıldır Internet kullanıyorsunuz?**

13 yıldır Internet kullanıyorum

**Kendinizi bir hacker olarak tanımlar mısınız?**

kendimi hacker olarak tanımlamam mümkün değil tabi ilk zamanlarda ele geçirdiğimiz MSN adreslerini saymazsak :)

**Cinsiyetiniz**

Erkek

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri neler?**

Hayır

**Hangi sosyal ağlarda hesaplarınız var?**

Facebook, Twitter, instagram, wechat, youtube

**Facebook'unuzun ve Twitter'inizin kayıtlı olduğu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Facebook hesabımın kayıtlı olduğu mailde isim-soyisim geçiyor ama twitter hesabımda yok

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Anonimlik zaten genel olarak yaratıcısı bilinmeyen olarak bakarsak Nick ile hesaplarımızı kullandığımız için profilim anonim diyebilirim

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Öyle bir bakışta isim ve profil fotoğrafından tespit edilen birşey olması mümkün değil çünkü isim ve fotoğraf gerçek kişi değil

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

- a) Ticari bağlardan oluşan baskı (Şirket vs.)
- b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)
- c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)
- d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)

Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Profil Saklı dahi olsa paylaşımlar öz düşünceleri yansıtıyor zaten ve görüş

farklılıklarından dolayı kimi zaman tartışmalar oluyor bu bazen sorun yaratabiliyor.

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Tek avantajı anadilimde profil ismi kullanmam oldu

**Kimliği saklı profil sahibi olmanın avantajları nelerdir?**

yarı- anonimliğin benim için dezavantajı yok ki olsa zaten gerçek kimlik kullanımım

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Gerçek kimlikten kasıt devletin verdiği ise hayır ama gerçek düşünce ve yaşantıma göre gerçek kimliğimle paralel

**Kendinizi troll olarak tanımlar mısınız?**

Tam olarak kendimi troll olarak tanımlayamam ama eğlence amaçlı trollük yaptığım zamanlar oluyor

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Cemaatler her yerde tehdit unsuru ve sosyal medyada da düşüncelere müdahale ederek tehdit oluşturmaya başladı.

**@kafa\_radyo**

Interview with @kafa\_radyo is made on 12<sup>th</sup> October 2013 through e-mail.

**Kaç yıldır Internet kullanıyorsunuz?**

18 yıl

**Kendinizi bir hacker olarak tanımlar mısınız?**

Anlamam etmem yani hayır

**Cinsiyetiniz?**

Erkek

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz?**

Kullanıyorsanız bunların isimleri neler?

Pc'de kullanmıyorum ama ipad'e spotflux diye bir vpn programı yükledim.

**Hangi sosyal ağlarda hesaplarınız var?**

Ekşisözlük, twitter, friendfeed, tumblr, 4square, instagram, feysbuk

**Facebook'unuzun ve Twitter'ınızın kayıtlı olduğu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Biri evet diğeri hayır

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Kafa radyo ile açık olan hesapların çeyrek anonim olduğunu düşünüyorum. Bir kere vpn kullan ve/ya kullanma ip adreslerini tespit etmek mümkün (bazı ağlar ipleri vermiyorum dese dahi). Ayrıca bu mahlasla da olsa gerçek hayatta tanıştığım iNsalar olduğu için anonoimlik o noktada bitiyor. Hasılı isteyen kimin kim olduğunu bulabilir.

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Feysbuk hesabım adım ile açık ve fotoğraflarım var.

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

- a) Ticari bağlardan oluşan baskı (Şirket vs.)
- b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)
- c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)
- d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)

E hepsi

Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?

Hayır

Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?  
Yeni insanlarla tanışmak.

Kimliği saklı profil sahibi olmanın avantajları nelerdir?

Pek yok aslında

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Kısmen

**Yarı anonim olmadan sosyal medya kullansaydınız bunun iş/siyaset/özel/günlük hayatınıza ne tür etkileri olurdu?**

Bambaşka bir profil olacağı için daha vasat olacaktı.İş hayatında zorluk yaşamam kaçınılmaz olurdu

**Kendinizi troll olarak tanımlar mısınız?**

Çok ender anlarda trollük yapıyorum

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Evet. Yaratılan personanın etkisinde kalıp yazmak istediği türden yazıları yazamadıklarına şahit oluyorum. Sosyal medyada eylemler için atıp tuttuğundan eyleme gitmek zorunda kalanlar da var ahahah

**Daha önce hiç bu tür bir kimlik kullandınız mı?**

Yıllardan beri kullanıyorum yahu

Interview with @\_kullanici\_adi is made on 06<sup>th</sup> September 2013 through e-mail.

**Kaç yıldır Internet kullanıyorsunuz?**

15 yıl

**Kendinizi bir hacker olarak tanımlar mısınız?**

Hayır

**Cinsiyetiniz?**

Erkek

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri neler?**

Evet, bilgisayarımda HotSpot Shield kullanıyorum ve Google public DNS adreslerini kullanıyorum.

**Hangi sosyal ağlarda hesaplarınız var?**

Sadece Twitter

**Facebook'unuzun ve Twitter'inizin kayıtlı olduğu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Hayır

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Anonimlik bence gerçek kimliğimle, yaşadığım çevreyle, veya yakın arkadaşlarımla ilgili herhangi bir bilgi veya ipucunu mevcut profilimde veya paylaşımlarımda kullanmamaktır. Bu durumda Twitter profilimi %70 anonim olarak tanımlayabilirim.

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Hayır yok.

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

- a) Ticari bağlardan oluşan baskı (Şirket vs.)
- b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)
- c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)
- d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)**

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Hayır

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Hayır bir bariz avantajı olmadı yalnızca bana daha özgür bir ifade alanı ve olası baskılardan korunma imkanı sağladı.

**Kimliği saklı profil sahibi olmanın avantajları nelerdir?**

Ben şu ana kadar bir dezavantajını görmedim ancak bu olmadığı anlamına gelmez.

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Evet kendinden kopamıyorsun sonuçta.

**Yarı anonim olmadan sosyal medya kullansaydınız bunun iş/siyaset/özel/günlük hayatınıza ne tür etkileri olurdu?**

Paylaşımlarımda daha sınırlı olma gerekliliği hissederdim, daha şiddetli bir oto-sansür hali olurdu.

**Kendinizi troll olarak tanımlar mısınız?**

Hayır

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Evet, insanlardan oluşan bir topluluğun zaman zaman örgütlülüğünden gelen gücünü eylemin haklılığını sorgulamadan kullanabileceğini ve bunun bazı mağduriyetlere sebebiyet verebileceğini düşünüyorum.

**Daha önce hiç bu tür bir kimlik kullandınız mı?**

Hayır

Interview with Narlincir is made on 26<sup>th</sup> September 2013 from 18:30 to 20:00 through Google Hangout in Turkish.

@Narlaincir

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri neler?**

Hayır kullanmıyorum, haberim bile yok.

**Hangi sosyal ağlarda hesaplarınız var?**

Facebook ve twitter.

**Facebook'unuzun ve twitter'mızın kayıtlı olduğu e-mail adresi adınız Ve soyadınıza dair bilgi veriyor mu?**

Hayır

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Bence "artık" anonim değil. Çünkü anonim kalmak istediğimi anlayanlar beni incitmek için deşifre ettiler. Bence anonimlik söyleyeni değil, söyleneni öne çıkaran bir şey. O yüzden anonimliği tercih etmiştim

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Foto yok. Ben olduğum anlaşılmaz diye düşündüğüm şeyleri paylaşıyordum fakat 8 yıl önceki sevgilim o profili takip etmeye başlamış ve ortak arkadaşımıza "sanırım bu bizim x" diye mesaj atmış.ben ne kadar sanmasam da, anlaşılıyor olabilir

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

A) ticari bağlardan oluşan baskı (şirket vs.)

b) siyasi bağlardan oluşan baskı (parti, stk, siyasi örgütlenme)

c) sosyal bağlardan oluşan baskı (aile, arkadaş, eş, sevgili, komşu)

d) devlet politikalarından kaynaklanan baskı (gözetim, phorm, dpi, sansür)

B

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Hayır

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı Avantajlar oldu mu? Olduysa nelerdir?**

Onun olmadı ama 2. Hesabımda seçerek insan takip ettiğim ve kabul ettiğim için çok daha rahatım

**Kimliği saklı profil sahibi olmanın avantajları nelerdir?**

Bilmiyorum :)

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Evet

**Kendinizi troll olarak tanımlar mısınız?**

Hayır

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Evet

**Geçtiğimiz günlerde bir kullanıcı Internette adınızı ve soyadınızı Teşhir etti. Bu durum sizi tedirgin etti mi? Bunun gerekçeleri neler?**

Daha önce 2 kere yazdıklarım yuzunden partililerle sorun yaşadım. Birisi partiden biriyle ilgiliydi, diğeri ise bülent arınç-vajina konusuyla ilgiliydi. Nasıl hem bir kurumda çalışıp hem de ulu orta vajina yazarım diye eleştirildim ve tartışma çıktı. Beni tedirgin etti çünkü deşifre eden kişi kürttü ve partiden çok takipçisi vardı. Bilmeyen

duymayan partililer de bu sayede öğrenecek diye tedirgin oldum. Nitekim o deşifreden sonra baya bir kürt takipçi daha geldi. Artık başıma iş açacak şeyleri (gerek geyik-gerek ciddi) 2. Hesabımdan yazıyorum

### **ikinci bir Saklı profil açtın. Sebebi neydi?**

Yukardaki soruda yazdım. Kurumlardan bir kadın arkadaş beni itibarsızlaştırmak için "o kadın twtrda vajına yazıyor ahlaksız" diye deşifre etti. Olay \*\*\*\*'e gidecek kadar büyüdü. Hem o hesaptaki takipçileri kontrol edemediğimden, hem de "daha çok tanıdığım ve rahat olabileceğim" insanları seçebileceğim başka bir hesap açtım. Hem parti yuzunden hem de diğer hesapta yazdıklarım yuzunden dedikodumu yapan bir kısım hevallere ve gündelik hayatta da "arkadaşım" olan insanlar yuzunden. Biraz onların baskısından kaçtım :)

### **@Myriamonde**

Interview with Myriamonde is made on 2<sup>nd</sup> October 2013 from 15:00 to 15:24 through Google Hangout in Turkish.

Buradaki bilgiler tamamen akademik amaçlı istenmektedir ve şahsın kimliğinden çok Internet kullanım biçimine ilişkin bilgi edinilmesi amaçlanmaktadır.

Kaç yıldır Internet kullanıyorsunuz?

1997'den beri, 16 yıldır

Kendinizi bir hacker olarak tanımlar mısınız?

Hayır

Cinsiyetiniz?

Kadın

Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz?

Kullanıyorsanız bunların isimleri neler?

Değil

Hangi sosyal ağlarda hesaplarınız var?

Facebook, twitter,

Facebook'unuzun ve Twitter'inizin kayıtlı olduđu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?  
Facebook evet, twitter hayır

İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?  
Yakın zamana kadar anonimdi ama artık deđil sanırım. İsim veya profil fotoğrafı kullanmıyorum, doğrudan kimliğime bağlanabilecek detayları (genelde) paylaşmıyorum

Yarı anonim profiliniz hariç sizin olduđu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?  
Facebook profilim fotoğraf ve detay içeriyor, twitter içermiyor

İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?  
a) Ticari bağlardan oluşan baskı (Şirket vs.)  
b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)  
c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)  
d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)  
Hepsi - baskı'dan ziyade "gerek yok" ekseninde gerçi.

Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?  
Ekşi sözlük'te yazarken kimliğimi araştırıp tehdit edenler oldu.

Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?  
Aileme zarar vermeden istediğim gibi davranabilme, işverenlerin ismimi arattığında hakkımda kontrol edemediğim kadar bilgi edinmemeleri gibi faydaları oldu.

Kimliği saklı profil sahibi olmanın avantajları nelerdir?  
Yok bence, belki gerçekten ne kadar anonim olduğundan emin olamamak olabilir.

Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?  
Kesinlikle.

Yarı anonim olmadan sosyal medya kullansaydınız bunun iş/siyaset/özel/günlük hayatınıza ne tür etkileri olurdu?  
İş ilişkilerimin zedeleneceğini düşünüyorum, siyaseten gerçek bir etki olacağını sanmam, gündelik hayatta sadece insanların hakkınızda edindiği bilgiyi, dolayısıyla intibayı, kontrol altında tutabilmeyi sağlıyor.

Kendinizi troll olarak tanımlar mısınız?  
Hayır

Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?  
Peer pressure her yerde, ama deşifre olmak haricinde çok gerçek bir tehdit var diyemem.

Daha önce hiç bu tür bir kimlik kullandınız mı?  
Ne tür? Ay kullanmadım. Kullandım mı? Kullanmadım. Kullandıysam da kullandı bu ya ben biliyorum diyiver :)

### **@Przykazan**

Interview with Przykazan is made on 24<sup>th</sup> September 2013 from 21:30 to 22:40 through Google Hangout in Turkish.

Kaç yıldır Internet kullanıyorsunuz?

12 yıl

### **Kendinizi bir hacker olarak tanımlar mısınız?**

Hayır

### **Cinsiyetiniz?**

Kadın

### **Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz?**

Evet, bazen.

### **Kullanıyorsanız bunların isimleri neler?**

lahana

### **Hangi sosyal ağlarda hesaplarınız var?**

Twitter-facebook-ff

**Facebook'unuzun ve Twitter'inizin kayıtlı olduđu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Evet

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Hayır

**Yarı anonim profiliniz hariç sizin olduđu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

evet

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

- a) Ticari bağlardan oluşan baskı (Şirket vs.)
- b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)
- c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)
- d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)

C

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Hayır

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Evet, söylediklerimin ardında durmam gerekmiyor. Bir kişilik olarak canlanmıyor sosyal medyada ismim. sadece bir kullanıcı olarak görülüyor. bu yüzden sorumluluğum olmuyor, ben de istediğim şekilde cümleler kurabiliyorum.

**Kimliđi saklı profil sahibi olmanın avantajları nelerdir?**

İkili ilişkilerde, gerçek olmadığını bildiđin için karşınızdaki arkadaş/dost/sevgili/partner'in de gerçekliğinden şüphe ediyor, güvensizleşiyorsunuz.

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Evet.

**Yarı anonim olmadan sosyal medya kullansaydınız bunun iş/siyaset/özel/günlük hayatınıza ne tür etkileri olurdu?**

Kovulurdum.

**Kendinizi troll olarak tanımlar mısınız?**

hayır.

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Evet. Orada yaratılan sanal dünyada artık birer bireyler, bir sosyal ortamları var. yine bu sosyal medyada ikinci bir hesapla ancak anonimliklerini sağlayabilirler.

**Daha önce hiç bu tür bir kimlik kullandınız mı?**

Evet.

**@AugustusHill**

**Kaç yıldır Internet kullanıyorsunuz?**

8-9

**Kendinizi bir hacker olarak tanımlar mısınız?**

Hayır

**Cinsiyetiniz?**

Erkek

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri neler?**

Hayır, kullanmıyorum

**Hangi sosyal ağlarda hesaplarınız var?**

Facebook, Twitter, Instagram, Vine

**Facebook'unuzun ve Twitter'inizin kayıtlı olduğu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Evet

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Yarı anonim diyebiliriz sanırım. Anonimliğin tam olarak ifade ettiği ise "sahibi asla bilinmeyen" İnternetteki karşılığı ise "tam güvence"

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Sadece ilk bakışta adımlı vermiyor fakat detaylı incelemek isteyen birisi olduğunda adıma soyadıma ulaşacaktır.

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden**

**hangisiyle bağdaştırabilirsiniz?**

- a) Ticari bağlardan oluşan baskı (Şirket vs.)**
- b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)**
- c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)**
- d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)**

Cevapta "hepsi" diye bir seçenek yoksa "d" seçeneği.

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Kendi kimliğimle hesap kullanırken yaşadım ancak yarı anonim olduğumdan beri problem çıkmadı

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Aile üyelerim bu twitleri benim attığımı bilmiyor. Başka da bir avantajımı hatırlamıyorum.

**Kimliği saklı profil sahibinin avantajları nelerdir?**

Yarı anonim olduğumdan beri twitterdan daha az kadınla tanıştım :)

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Gerçek hayatta tanımadığım kişilere sataşmıyorum bunun dışında paralel.

**Yarı anonim olmadan sosyal medya kullansaydınız bunun iş/siyaset/özel/günlük hayatınıza ne tür etkileri olurdu?**

Daha önce 2-3 defa ailemle bu konuda problem yaşadım. Hatta bir keresinde istihbaratta çalışan bir polis tanıdığım annemi arayıp twitlerimden bahsetmiş "Anıl'ı izliyorlar,

zaten fişlenmiş kendine dikkat etsin" demiş.

**Kendinizi troll olarak tanımlar mısınız?**

Evet.

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

"Sosyal medyada oluşan cemaatler" hakkında bir bilgim yok.

**Daha önce hiç bu tür bir kimlik kullandınız mı?**

Anonim kimlik eskiden daha popülerdi sanırım. pre-Facebook sitelerde anonim olarak takılırdık. Benim de facebooktan önceki sitelerde anonim hesaplarım vardı. Ancak neo-liberal dönüşümün bizi "evlerimize hapseden" bir tarafı var. Ve "var olma" ihtiyacımızı İnternet üzerine taşıyor. O yüzden artık anonimlik tercihinin azaldığını düşündüğümü de ekleyeyim.

**Daha önce anonim olmadan önce yani ne tür sorunlar yaşamıştınız twitter'da yazdıklarınızdan ötürü? Sence bugün kimliğiniz açığa çıksa ne tür sorunlar yaşarsınız?**

"Anadilde eğitimi konuşuyoruz sürekli de Kürdistan'ın köylerinde hala öğretmenin okula uğramadığı okullar var. Biraz da 'eğitim'i konuşalım." gibisinden bi twit atmıştım. Bu twitin üzerinden bi süre geçti. Açlık grevlerinin olduğu dönem bir bildiri yayınladık okulda Uludağ Üniversitesi Psikoloji Öğrencileri diye. Dekanla falan problemler olmuştu. Sivil polis de isimlerimizi almış. Okulda bu bildiriye şikayet eden hocalar olmuş yani. Sonra babamın eski bir arkadaşı annemi aramış. Polis. "Yenge, abiyi aramak istemedim senin haberin olsun. Anıl böyle işlere bulaşmış, bildiri falan. Twitterına da Kürdistan yazmış." demiş. Ailemle birinci vakam bu oldu.

İkincisi de geçtiğimiz 1 Mayıs'ta HDK kortejindeydik. En çok polis bizim kortejin yanında geziyordu. "Kortejimizi bir an olsun yalnız bırakmayan Emniyet Teşkilatımıza

teşekkürler." diye bir twit attım. Yine aynı dönem sevdiğim bir müzisyen öldü "Böyle dünyanın amına koyayım" yazdım. Babamın da tam bu dönemde adımı google'da aratası tutmuş :) Biraz kavga gürültü de oradan yaşadık. Baktım olmuyor hesabımın tamamen yeniledim. Yani kısacası polisin fişleme meselesinden falan öte ailevi problemlerimin hesabımı kapatmama sebep oldu. Sonrasında da bu şekilde twitter kullanmanın daha eğlenceli olduğunu gördüm. Kimliğim açığa çıksa diye bir şey de yok aslında. Birazcık detaylı profilimi inceleyecek olan birisi zaten profilin bana ait olduğunu görecektir. Ama google gibi bağlantılardan kolaylıkla ulaşılmasının zor olması işime geliyor. Sonuçta artık işverenlerin bile iş başvurusu yapan kişilerin adını googledadığını biliyoruz. Ee kendim için yaratabildiğim ve keyifle kullanabildiğim bir alan twitter. Bu bozulsun da istemiyorum. Bu şekilde işler harikulade gidiyor yani :)

**@KuntaKinteden**

**Kaç yıldır Internet kullanıyorsunuz?**

10 yıl

**Kendinizi bir hacker olarak tanımlar mısınız?**

Hayır

**Cinsiyetiniz?**

Erkek

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri neler?**

Hayır

**Hangi sosyal ağlarda hesaplarınız var?**

Facebook, twiter, ekşisözlük

**Facebook'unuzun ve Twitter'inizin kayıtlı olduğu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Evet

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

Anonim değil ISP'ten tespit edilebilir

**Yarı anonim profiliniz hariç sizin olduğu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı?**

Evet

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

1. Ticari bağlardan oluşan baskı (Şirket vs.)

b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)

– Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)

1. Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)

Hepsi ile bağdaşiyor

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayı sorun yaşadınız mı?**

Devletle değil ama şahıslarla kısmen (kimliğim ifşa edildi). Bir kaç kere tehdit edildim,

hakaret edildi.

**Yarı anonimliğin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Dayak yememek:)

**Kimliği saklı profil sahibi olmanın avantajları nelerdir?**

Oto sansür ihtiyacını ortadan kaldırması

**Yarı anonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Tam olarak değil, o daha cesur

**Kendinizi troll olarak tanımlar mısınız?**

Bazen:)

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskı ya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Kesinlikle bir mahalle baskısı oluşturuyor

**@13melek:**

Kaçıldır Internet kullanıyorsunuz?

15 senedir.

**Kendinizi bir hacker olarak tanımlar mısınız?**

Hayır

**Telefonunuzda ya da bilgisayarınızda anonim kalmanızı sağlayacak yazılımlar kurulu mu? Bu yazılımları kullanıyor musunuz? Kullanıyorsanız bunların isimleri**

**neler?**

Gezi direnişinin ilk iki ayında Hotspot Shield kullandım.

**Hangi sosyal ağlarda hesaplarınız var?**

Twitter ve Facebook (Facebook hesabında tamamen pasifim, paylaşımında bulunmuyorum)

**Facebook'unuzun ve Twitter'inizin kayıtlı olduđu e-mail adresi adınız ve soyadınıza dair bilgi veriyor mu?**

Evet.

**İnternetteki profiliniz sizce anonim mi? Sizce anonimlik ne anlama geliyor?**

başka bir sosyal medya kullanıcısının Twitter profilim üzerinden kimlik bilgilerine ulaşması kolay değıl. Ancak isim üzerinden olmasa da email adresi üzerinden sosyal medya şirketleri aracılığıyla tespit edilebilirim. Bu yüzden anonim olduğumu düşünmüyorum.

**Yarı anonim profiliniz hariç sizin olduđu profildeki isim ve fotoğraftan ya da içeriklerden tespit edilebilen bir profiliniz var mı? -**

Yok, bu konuda özenli olmaya çalışıyorum ama uğraşılırsa noktalaribirleştirebilenler olabilir.

**İnternetteki gizli kimlik kullanımınızı aşağıdaki seçeneklerden hangisiyle bağdaştırabilirsiniz?**

**a) Ticari bağlardan oluşan baskı (Şirket vs.)**

**b) Siyasi bağlardan oluşan baskı (Parti, STK, siyasi örgütlenme)**

**c) Sosyal bağlardan oluşan baskı (Aile, arkadaş, eş, sevgili, komşu)**

**d) Devlet politikalarından kaynaklanan baskı (Gözetim, Phorm, DPI, Sansür)**

İnternetteki siyasal paylaşımlarımın ya da dergi/radyo gibi uğraşlarıma dair bilgilerin işçevrem tarafından bilinmemesi gizli kimlik kullanımımın başlıca sebebi. Ancak üniversitede çalıştığımdan ticari bağlar sınıfına sokup sokulamayacağından eminim.

Onun dışında özel hayatım sebebi ile aileme ve akrabalarımaya karşı da anonim olabilmek istiyorum, sosyal medyadaki profil bilgilerimi onlarla paylaşmıyorum. Devlet

politikalarından kaynaklanan baskı ise bunları çerçeveleyen genel bir baskı ve geçerli.

**Saklı kimliğine rağmen yeni medyada ürettiğiniz içerikten dolayısırın yaşadığınız mı?**

Hayır.

**Kimliği saklı profilin (kimliği açık etmeden kullanım) size sağladığı avantajlar oldu mu? Olduysa nelerdir?**

Siyasal fikirlerimi, sokak eylemlerimdeki varlığımı, işten çalıp hobilerime harcadığım vakitlerin kanıtı olan paylaşımlarımı yakalanma, kınanma korkusu hissetmeden yapabiliyorum.

**Kimliği saklı profil sahibi olmanın avantajları nelerdir?**

Günlük hayatın içerisinde tanıştığım insanların beni bir mahlas üzerinden tanıması ancak gerçek kimliğimle bir bağlantı kuramaması tuhaf durumlara yol açabiliyor ancak bu seçici kimlik beyanı yaparak aşılabilen bir konu ve dezavantaj olarak sayılmayabilir.

**Yarıanonim kimliğinizin gerçek kimliğinizle paralel bir kimlik olduğunu söyleyebilir misiniz?**

Evet. Aradaki tek fark gerçek kimliğimin daha tedbirli ve gizci olması, anonim kimliğimin ise daha çekincesiz davranabilmesi.

**Kendinizi troll olarak tanımlar mısınız?**

Hayır.

**Sosyal medyada oluşan cemaatlerin yine bu alanda aktif bireyler için baskıya da tehdit unsuru olabileceğini düşünüyor musunuz?**

Cemaatler halihazırda bir baskı ve tehdit unsuru zaten, twitter'da linç vakalarına alıştık ama şu ana kadar bu baskı ve tehditlerin içi boş tehditler olduğunu gördüm. Ancak özellikle iktidarın sosyal medya timleri oluşturması bu durumun ciddileşmesi yönünde

endişe verici. Anonimlik bu açıdan da önemli, bir gün sokakta yolumuzun kesilmesi ihtimalini sıfırlamasa da azaltıyor.

### **Sosyal medyada kimliğinizin ifşa edilmesi sizi kötühissetirir miydi?**

Kesinlikle evet. En basitinden öğrencilerimle daha anonim bir ilişki kurmak istiyorum ve bu açıdan sıkıntıyaşardım. Bunun dışında aileden de, her ne kadar siyasal olarak çok ayırdüşmesek de güvenliğim adına baskı görebilirdim.

### **Gezi Direnişi sırasında aktif olarak yurttaşmuhabirliği yaptınız. Çektiğiniz fotoğraflar ve konularınız belirgin olduğundan, olası bir operasyona tabi tutulmaktan korkmadınız mı? Twitter kimliğinizde kendi isminizi kullanmamanız sizi güvende hissettirdi mi?**

Hayır, korkmadım zira sorumluluğun ve heyecanın korkuya galip geldiği bir dönemdi, yaptığım şeyin meşruiyeti korkuyu yendi. Ancak bu konuda Twitter kimliğimde gerçek ismim olmaması mutlaka rahatlatıcı bir unsurdu. Orada kendi adım ve soyadım olsa biraz daha endişe ederdim. Yine de bu endişenin çoğu devletin operasyonuna maruz kalmaktan dolayı sosyal çevrede maruz kalabileceğim baskılara yönelik.

### **3. SCREENSHOTS REGARDING DISCLOSES**



The screenshot shows a Twitter post from user Cng Sgnc (@cngsgnc). The post text reads: "Özge İspir diye biri. 16 yaşından beri pêşmerge olan Barzani'ye hain diyor Kürtler adına. Kürtler onunla dost. [twitter.com/narlaincir/sta...](https://twitter.com/narlaincir/sta...)". Below the text are options for "View translation", "Reply", "Retweet", "Favorite", and "More". The post has 3 favorites, with two profile pictures visible. The timestamp is "2:34 PM - 31 Aug 13".

<https://twitter.com/cngsgnc/status/373876581640306688>



**Aybike Hatemi-Teubes**

@AybikeHatemi



Follow

Kim diyor Ermenilere hakaret ettiğimi? Ayda Erbal mı, Özge İspir (Narla İncir) mi, yoksa Ayşe Özdemir mi? ;) @bingl\_yav

View translation

Reply Retweet Favorite More

1:47 PM - 15 Mar 13

### tolga mustafa kadioğlu

paylaş araştıır takip et yaz taşı başlıkta ara

1

çok büyük bir avukat ama bir bülent arınc değil..

paylaş favori

20.06.2011 16:10 [akiyor yesil](#)

şükela! çok kötü

[mesaj at](#) [diğer](#)

2

alın teri ile kazanılan ekme parasını aşağılamaya çalışan kafanın temsilcisidir. hatırlatma babında:

rıza efendi iki ekme bir süt!

karakter analizini yapmayacağım ama toplumdaki statü sevdalısı hali pek bir fena imiş..

paylaş favori

20.06.2011 16:21 [akiyor yesil](#)

şükela! çok kötü

[mesaj at](#) [diğer](#)

3

kompleks sahibi olduğunu iddia ettiği adamı gün yüzüyle bir kere görse bu hakaretlerinden tövbe-i istiğfar edip geri döneceğinden emin olduğum büyük icra avukatı.

paylaş favori

20.06.2011 16:25 [akiyor yesil](#)

şükela! çok kötü

[mesaj at](#) [diğer](#)

4

herkesin tc numarasıyla konuştuğu ortamlarda takma isimler kullanmakla çok ayıp ediyor doğrusu.

paylaş favori

20.06.2011 16:28 [dagny taggart](#)

şükela! çok kötü

[mesaj at](#) [diğer](#)

<http://eksisozluk.com/tolga-mustafa-kadioglu--2880207>