MEIRSS
Middle East Institute
For Research
And Strategic Studies

Negating Privacy under the Pretext of Security:
Rising Trends of Mass Surveillance in the Middle East

June 2016

Jimmy Matar

The internet has reached over 2.5 billion people in its first 20 years of existence, and this reach extends to detailed aspects of personal, governmental, and corporate lives. Due to the lack of concrete legal standards regulating the use of the internet, as well as the huge rise in smartphone demand, has made the internet one of the most disruptive inventions of the 20th century especially in terms of free speech. Widely perceived as a tool which has given a voice to the voiceless, specifically in authoritarian countries, the upcoming years will pose a significant challenge to the protection of personal privacy online which if breached could be life-threatening in many cases.[1] On the other hand, it has also posed a danger to the public through groups which used the internet to plan and coordinate their attacks without being traced. This led to mass surveillance programs which theoretically aim to counter these actions. This paper aims to study the Snowden leaks, the degree of success of these surveillance programs, the dangers of negating online privacy, the sale and use of such programs by authoritarian regimes, and the policies adopted by Lebanon, Egypt, and Turkey; in addition to attempting to find the much needed balance between privacy and security going forward.

The documents leaked by former NSA analyst Edward Snowden in June 2013 put the spotlight on the surveillance programs adopted mainly by the United States and other major countries such as the United Kingdom. The leaks highlighted the access that governmental agencies have to phone records, text messages, servers of technology giants such as Apple, Google, and Microsoft through a program called Prism, global internet data flow through tagging fiber optic cables by the GCHQ (Government Communication Headquarters (British Intelligence Agency) in an operation called Tempora, and encryption backdoors; furthermore, the NSA also has hacking teams in case surveillance comes up short such as in China and Hong Kong, as well as spying on

[1] Gorodyansky, D. (2015) Privacy and Security in the Internet Age, Wired, Retrieved from http://www.wired.com/insights/2015/01/privacy-and-security-in-the-internet-age/

embassies, foreign leaders such as German Chancellor Angela Merkel, and European Union officials.[2]

Intelligence agencies stated that these programs are subject to oversight, are necessary for stopping terrorist attacks, and that the public should not be so concerned. The phrase “if you have nothing to hide, you have nothing to fear” was repeatedly used to justify this overreaching interception of data. Even tech companies, fearing from a consumer backlash, claimed that they were forced to cooperate by the law. In response, civil liberties groups indicated that this vast collection of data through phones, laptops, and social media… all lead to the building up of a “pattern of life” of someone targeted or even associated with them. The number of people who are included is huge. For example, there are three degrees of separation from the suspect being monitored. So, if the average user has 190 friends in the first degree, he would have 31,046 friends of friends in the second degree, and would finally have 5,072,916 friends of friends of friends in the third degree.[3]

Even though intelligence agencies assert that surveillance programs play a great role in preventing terrorist attacks, critics point out that the NSA has not been able to provide a single serious example of the success of these programs in stopping a major attack. This was corroborated by a member of the White House review panel established to study the NSA surveillance program. He stated that he was surprised that the agency did not have any proof of the success of this bulk collection of data, and the panel eventually mentioned in its report that

[2] Franceschi, L. (2014) The 10 Biggest Revelations from Edward Snowden’s Leaks, Mashable, Retrieved from http://mashable.com/2014/06/05/edward-snowden-revelations/#mbKJqgOWEiqd; BBC (2014) Leaks that Exposed US Spy Program, BBC News, Retrieved from http://www.bbc.com/news/world-us-canada-23123964

[3] Macaskill, E. & Dance, G. (2013) NSA Files Decoded What the Revelations Mean for You, The Guardian, Retrieved from http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

the program was "not essential in preventing attacks".[4] The report also specified that the telephone records collection program made "only a modest contribution to the nation's security", and "there has been no instance in which NSA could say with confidence that the outcome of a terror investigation would have been any different".[5] Furthermore, former head of the NSA's global intelligence gathering operations, Bill Binney, believes that mass surveillance leads to an overwhelming amount of data and thus obstructs the ability of analysts to properly go through it all. For example, according to Binney, the NSA had the information which could have prevented 9/11 but did not know that it was in their databases. This was before the bulk collection even began. He indicates that targeted surveillance for specific suspected individuals is a much better way of operating. This is validated by media reports stating that the San Bernardino shooters were in contact with people already under investigation by the FBI.[6] The same issue was also highlighted by a French counterterrorism expert who pointed out after the Paris attacks that the problem was not in the lack of data, but the failure to act on already-acquired information.[7]

The parliamentary assembly in the Council of Europe issued a report which says that the scale of surveillance employed by intelligence agencies such as the NSA and GCHQ infringes upon the right to privacy, freedom of expression, and right to a fair trial. The fact that all this happens without sufficient judicial control threatens the cornerstones of democracy.[8] In the US, government surveillance requests are handled by a secret court which is the FISA (Foreign Intelligence Surveillance Act) court that constantly reinterprets the laws to allow broader

[4] Isikoff, M. (2013) NSA Program Stopped No Terror Attacks Says White House Panel Member, NBC News, Retrieved from http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588

[5] Ibid.

[6] Washington's Blog (2015) California Terror Attacks Proves Mass Spying Doesn't Keep Us Safe, Washington's Blog, Retrieved from http://www.washingtonsblog.com/2015/12/california-terror-attack-proves-spying-doesnt-keep-us-safe.html

[7] The Editorial Board (2015) Mass Surveillance Isn't the Answer to Fighting Terrorism, The New York Times, Retrieved from http://www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html

[8] Harding, L. (2015) Mass Surveillance is Fundamental Threat to Human Rights Says European Report, The Guardian, Retrieved from http://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe

surveillance, and the number of cases that have been made available to the public is incredibly limited. This greatly impedes the public's ability to hold the government accountable. Mass surveillance without proper political and judicial oversight could have very negative consequences. For instance, the large scope of surveillance enables the use of "big data" techniques which rely on complex algorithms to store a lot of data for later use when needed. Even if the domestic population is not specifically targeted, the fact that Internet communications pass through international routes leads to the search of domestic data without a warrant. Furthermore, since copies of this data are stored for years at a time, even though there is no reason to suspect any wrongdoing by a member of the population, allows the government to search through this data whenever it deems necessary without even obtaining a warrant.[9]

This well-built surveillance architecture could be used to crack down on dissent, profile people based on race or religion, and impair the ability to associate freely… This has already happened on a smaller scale such as people being placed on the "no fly list" without even giving them the chance to clear their names.[10] It has also had an effect in in the US where Muslim communities, for example in New York, preferred to "lay low", avoid political involvement, and think twice before posting something online because they know that the NYPD was monitoring them.[11] A second concern is the treatment of the whole population as criminals since the mass nature of surveillance abandons the principle that surveillance should be targeted based on sufficient evidence of wrongdoing and issued by an independent judicial authority. A third concern is the threat that surveillance and invasion of privacy has on the freedom of expression of an individual

[9] Toomey, P. (2015) Caught in the Internet, Foreign Affairs, Retrieved from https://www.foreignaffairs.com/articles/2015-08-20/caught-internet

[10] Ibid.

[11] Arastu, N. & Shamas, D. (2013) Surveillance and Its Impact on American Muslims, Al Jazeera, Retrieved from http://www.aljazeera.com/indepth/opinion/2013/03/201331311231826 7349.html

especially on the internet which has been considered for years as a free space for ideas.[12] A fourth concern is the imbalance of power created between the people and the government especially if the agencies collecting and analyzing this information are insulated to a certain extent from public accountability.[13] A fifth concern is the possible creation of a police state where citizens live under the constant threat of surveillance, and this could lead to a form of self-censorship and collective conformity. Even if there are internal rules regulating the use of this data, the fact that we have no control over how it is used or when the rules might change has an impact on human behavior by making us more compliant and reducing liberty and freedom.[14]

This was proven with a study conducted by Elizabeth Stoycheff, a journalism professor at Wayne State University, and published in *Journalism and Mass Communication Quarterly*. The study examined whether social media users would behave differently if they were under government surveillance. Two-thirds of the participants, even though they believed that they had nothing to hide, altered their behavior especially regarding issues they have different opinions about than the majority of society, while those remaining either refrained from posting at all or spoke their minds regardless.[15] Another study conducted by Jon Penney from Oxford showed that after the Snowden leaks there has been a 20% decline in searches related to "Al Qaeda" and "car bombs" as well as issues they believed would put them in trouble with the government. This shows the self-censorship people engaged in out of fear of being targeted, and the reluctance to search for important political topics could negatively impact the ability of the public to engage in

[12] Amnesty (2015) Five Reasons to Care about Mass Surveillance, Amnesty International, Retrieved from https://www.amnesty.org.uk/blogs/ether/five-reasons-care-about-mass-surveillance-edward-snowden-gchq-nsa-citizenfour

[13] Kendzior, S. (2013) The Danger of Data Not the Information but the Interpretation, Al Jazeera, Retrieved from http://www.aljazeera.com/indepth/opinion/2013/09/20139995624545872.html

[14] Amnesty (2015) Five Reasons to Care about Mass Surveillance, Amnesty International, Retrieved from https://www.amnesty.org.uk/blogs/ether/five-reasons-care-about-mass-surveillance-edward-snowden-gchq-nsa-citizenfour; Greenwald, G. (2016) New Study Shows Mass Surveillance Breeds Meekness Fear and Self-Censorship, The Intercept, Retrieved from https://theintercept.com/2016/04/28/new-study-shows-mass-surveillance-breeds-meekness-fear-and-self-censorship/

[15] Waddel, K. (2016) How Surveillance Stifles Dissent on the Internet, The Atlantic, Retrieved from http://www.theatlantic.com/technology/archive/2016/04/how-surveillance-mutes-dissent-on-the-internet/476955/

a proper democratic debate.[16] More direct examples of the dangers of surveillance where the internet is abused as a tool for state control are China and Russia. The "Great Firewall" of China prevents access to certain websites especially if they contain certain keywords such as human rights and Tiananmen. Page content is also scanned so that if it contains undesired content, it is blocked for a period of time. While in Russia, the SORM, System of Operative-Investigative Measures, captures phone communications, internet traffic, and information from all forms of communication within Russia; in addition, this includes recordings and locations of calls, and the data is stored for a long period of time. This is done under the guise of combating terrorism, but critics and activists point out that this is used to control and eliminate opposition.[17]

The advancement in surveillance technology and the collection of personal information by governments and tech companies alike poses a big challenge especially with the ability of government hackers to access your computer and install malicious software which aims to steal data. For example, in 2011, an Iranian hacker broke into the Dutch certificate authority, DigiNotar, which enabled him to impersonate major organizations such as Google, Facebook, Microsoft, and the CIA… Consequently, this gave him the authority needed to spy on the users of these services. The more important fact is that this ability was passed on to the Iranian government which was able to access more than 300,000 Iranian Gmail accounts. Another example is a malware called GhostNet that was found on the computers of the Dalai Lama. This surveillance network was found to be controlled from China and was also installed on computers of many political, economic, and media organizations in 103 countries that are Chinese espionage targets. Many similar programs reportedly installed by governments have been

[16] Greenwald, G. (2016) New Study Shows Mass Surveillance Breeds Meekness Fear and Self-Censorship, The Intercept, Retrieved from https://theintercept.com/2016/04/28/new-study-shows-mass-surveillance-breeds-meekness-fear-and-self-censorship/

[17] Herman, A. (2016) The Road to Internet Serfdom, Hudson Institute, Retrieved from http://www.hudson.org/research/12271-the-road-to-internet-serfdom

discovered such as Flame which was installed by the US and Israel to spy on Iranian networks, and Red October which is a Russian surveillance system…[18]

There has been a huge rise in the market for surveillance tools in the past decade as the value increased from virtually nothing to about $5 billion dollars annually in 2011[19]. For example, Ricardo Martinelli, former President of Panama, purchased a monitoring tool from NSO Group Technologies, an Israeli intelligence firm, to tap into phones and emails. Another example is Verint, a US-Israeli firm, which sold advanced surveillance systems to Columbia's security apparatus. The same scenario repeats itself in different repressive states such as Uzbekistan and Kazakhstan where surveillance techniques are used as an additional tool for police brutality.[20] The lack of comprehensive regulation for the trade of such tools could have devastating effects on the freedom of millions of people.

Due to the role that the internet and social media played in the mobilizing and reporting in the Arab uprisings, activists came to rely on this technology as seen in Tunisia and Egypt where citizens used YouTube to disseminate what is happening on the ground to world media after the failure of traditional journalists to get access. Over time, activists also realized the harm that this technology can do especially with dozens of companies from North America and Europe selling technology to authoritarian regimes in the Arab World so that they can crack down on opposition movements. These tools could intercept communications of activists, listen to their phone calls, read their text messages, scan their emails, pinpoint their locations, monitor their movements, and exploit security flaws in their devices… This has translated many times into the arrest,

[18] Schneier, B. (2015) What's Next in Government Surveillance, The Atlantic, Retrieved from http://www.theatlantic.com/international/archive/2015/03/whats-next-in-government-surveillance/385667/

[19] Bamford, J. (2016) The Espionage Economy, Foreign Policy, Retrieved from http://foreignpolicy.com/2016/01/22/the-espionage-economy/

[20] Bamford, J. (2016) The Espionage Economy, Foreign Policy, Retrieved from http://foreignpolicy.com/2016/01/22/the-espionage-economy/

torture, and even death of individuals, and in most cases, the public didn't even know about what happened. Several Arab regimes dealt with surveillance companies as seen with the Ben Ali regime in Tunisia which received discounts from firms that wanted to use the country for testing, the Bahraini regime which purchased technology from the Germany-based Trovicor and allowed security officers to access text messages and emails of political activists, the Qaddafi regime which spied on journalists and activists using programs made by the French company Amesys[21], and the Syrian regime to monitor user activities by using devices from the California-based Blue Coat Systems as well as Hewlett-Packard, AreaSpA of Italy, and Dublin-based Cellusys… All of these trades have caused a lot of controversy about companies selling surveillance technology to authoritarian regimes.[22]

Due to the fragile state that the Middle Eastern region is going through, and the high probability that surveillance laws could be negatively used, three countries with different political systems and varied degrees of freedom will be examined in terms of the law and practical application.

The first example is Lebanon which has a relatively democratic system with a high degree of political freedom compared to the region's countries. The Lebanese Constitution protects the privacy of an individual's place of residence, individual liberty, and freedom of expression. This is interpreted to include the secrecy of different forms of communication. In addition, Law No.40 protects the secrecy of communications, whether wired or wireless, and cannot be subject to surveillance or tapping except in specified cases specified by Article 98 of the Lebanese Code of Civil Procedures. Lebanon has a legal framework for the interception of communications which

[21] Timm, T. & York, J. (2012) Surveillance Inc How Western Tech Firms are Helping Arab Dictators, The Atlantic, Retrieved from http://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/; Elgin, B. & Silver, V. (2011) The Surveillance Market and Its Victims, Bloomberg, Retrieved from http://www.bloomberg.com/data-visualization/wired-for-repression/

[22] Mackinnon, R. (2012) Containing Weapons of Mass Surveillance, Foreign Policy, Retrieved from http://foreignpolicy.com/2012/04/24/containing-weapons-of-mass-surveillance/

was introduced in 1999 and adopted in 2009. The Telecommunication Interception Act (Law 99/140) restricts the interference in communications to cases of urgency and based on a judicial or administrative order. Both cannot exceed a 2 months period: the judicial order must be based on the suspicion of a crime committed by the targeted individual while the administrative order must be specific and based on combating terrorism, organized crime, and crimes against state security. It is authorized by the minister of interior or minister of defense and must gain approval of the Prime Minister. Even these administrative decisions are subject to judicial oversight to safeguard against abuse; however, in spite of the protection that the law aims to offer, systematic abuse of the law is practiced.[23]

Before March 2014, security services were granted access to the telecommunications data of a specific area based on a request due to the occurrence of a security incident or the possible location of wanted suspects; however, this no longer happens and security services have been granted full access to all data following a decision of the Telecommunications Minister that was subsequently approved by the cabinet. This decision is subject to renewal every 6 months; even though the law clearly states that it cannot exceed 2 months. Another violation is the PM approving surveillance requests even before the judicial panel studies them rendering them as only a symbolic advisory body. High-level judicial and parliamentary sources also reportedly stated that all security branches illegally operate wiretapping divisions without any oversight. This is exacerbated by the fact that the different security branches do not trust each other and pursue different goals away from national interests. Furthermore, the Information Branch requested a couple of years ago, in addition to the telecommunications data, the contents of

[23] Privacy International (2015) The Right to Privacy in Lebanon, Privacy International, Retrieved from https://www.privacyinternational.org/sites/default/files/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission.pdf

phone calls, text messages, and passwords for social media sites. The issue caused controversy and then died down without determining whether they got the information or not.[24]

It has also been reported by Citizen Lab at the University of Toronto that PacketShaper, a surveillance technology that monitors users' interaction on Facebook, Twitter, and Google Mail…, had been installed in Lebanon. Even though they could be used for legitimate purposes such as controlling bandwidths costs, they can also be used for censorship and surveillance. This discovery came at a time when the government was drafting a regulation that controls online content under the guise of public morals but later abandoned the regulation.[25] Another report by Global Voices Advocacy, based on leaked documents by WikiLeaks, states that the Lebanese Army purchased Hacking Team's Galileo Spy Software while the Internal Security Forces, General Security, and Cybercrime Bureau all had contact with the same company. The Cybercrime Bureau also contacted Gamma, another leading surveillance technology company, and the creator of FinFisher, a spyware product.[26] The fact that each security agency in Lebanon has made contact with renowned spy companies and have access to the communications of the population raises a high degree of concern to the way that this data might be used especially since each agency is believed to be close to the political leadership of a specific Lebanese sect, rather than being fully impartial and serving the general interest of the government and all citizens.

[24] Nazzal, M. (2014) The Surveillance State No Privacy for the Lebanese, Al Akhbar, Retrieved from http://english.al-akhbar.com/node/19751

[25] Privacy International (2015) The Right to Privacy in Lebanon, Privacy International, Retrieved from https://www.privacyinternational.org/sites/default/files/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission.pdf

[26] Quino, Z. (2015) Hacking Team Leaks Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices, Global Voices Advocacy, Retrieved from http://www.smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

Another area of concern for Lebanon is the ability of powerful non-state actors such as Hezbollah to monitor communications themselves through informer networks and telephone monitoring to obtain information about individuals they deem as their adversaries. This is even more worrying due to the complete absence of judicial or political oversight by the government or elected officials.[27]

A second case from the region is Egypt which has an authoritarian regime with a negative record of cracking down against opposition, whether Islamic or secular. The previous Mubarak regime had established a wide range of surveillance policies which were not halted after he stepped down. The same trend seems to have continued after the uprising as well. The 2014 Egyptian Constitution, in articles 57 and 58, guarantees the right to privacy and specifically mentions electronic, communications, and home privacy. Article 113 of the Egyptian Penal Code no.58/1937 even imposes criminal penalties in case unlawful violation of an individual's privacy occurred. Surveillance is usually linked to the imposition of a state of emergency which had been applied frequently since 1958 but lifted since November 2013, with the exception of the Sinai region in which it was reinstated in October 2014 due to the presence of militant groups. The surveillance law allows the state to monitor letters of any type, impose censorship, and seize publications. Based on Law 58 of the Egyptian Criminal Code and Law 150 of the Criminal Procedures Code, judges can issue warrants authorizing the interception of communications possibly related to a crime, and the period is limited to 30 days which can be renewed only once; however, a warrant can also be issued by an authorized member of the armed forces or security agencies who are not subject to proper oversight and whose actions are not explicitly regulated by the law. This is coupled with the 2003 Telecommunication Regulation Law which prevents

[27] US State Department (2013) Lebanon 2013 Human Rights Report, US State Department, Retrieved from http://www.state.gov/documents/organization/220575.pdf

encryption unless a written consent is acquired from the National Telecom Regulatory Authority, the Armed Forces, and National Security Entities and forces communication companies to cooperate with security agencies and the armed forces.[28]

The fears of abuse of power by the security agencies are reportedly well-placed since it has been stated by Vodafone, one of the major phone and internet service providers in Egypt, that law enforcement agencies have unrestricted access to communications data.[29] The Technical Research Department (TRD) which has ties to the Ministry of Interior is also allegedly in charge of a monitoring center. The TRD has one of the largest budgets of the intelligence agencies and has recently purchased technologies worth around 1 million pounds from Hacking Team, as well as other equipment from Nokia Siemens Networks and Advanced German Technology. It is only accountable to the President, and its purpose is reported to be to spy on government officials and potential opponents.[30] Several examples of surveillance have come to light in the past years such as the systematic targeting of Muslim Brotherhood members and civil society activists by the Sisi government since the July 2013 coup. For instance, the emails of a human rights activist were reportedly printed and slipped under her door. Another example is the television program Black Box which broadcasted the phone calls of activists to show how they participated in "treasonous activities".[31]

Monitoring of online activity is also on the rise as seen in 2014 with the reported contracting of See Egypt (Systems Engineering of Egypt), which has strong ties to the State Security Services,

[28] Privacy International (2016) State of Surveillance Egypt, Privacy International, Retrieved from https://www.privacyinternational.org/node/739

[29] Ibid.

[30] Privacy International (2016) The President's Men, Privacy International, Retrieved from https://www.privacyinternational.org/sites/default/files/egypt_reportEnglish.pdf

[31] Privacy International (2016) State of Surveillance Egypt, Privacy International, Retrieved from https://www.privacyinternational.org/node/739

to provide surveillance services to the government.[32] The alleged contract comes months after leaked documents from the Ministry of Interior indicated that seven unnamed technology firms present proposals for a surveillance system regarding “anti-government sentiment, instigating unrest, terrorism, blasphemy, and other vague offences”.[33] Previously, security agencies have been able to loosely monitor local networks, but See Egypt has the technology which enables geo-location, tracking, and extensive monitoring of internet traffic. In addition, it can also penetrate WhatsApp, Viber, Skype, and other programs, and it is similar to the systems used by most Western governments – even though some doubt the ability of a program to perform all these actions. In spite of officials stating that monitoring online activity is to prevent terror attacks, the arrests of demonstrators, cracking down on dissenting voices, and observing LGBT Facebook groups indicate that the purpose of such programs is much broader.[34]

The third case is Turkey which is slowly moving towards more authoritarian practices. The Turkish Constitution, in articles 20 and 22, guarantees the protection of privacy, personal data, and freedom of communication; in addition, the articles 134, 135, 138, and 138 of the Criminal Code provide further protection for the right to privacy. In practice, there is a widespread belief that violations and mass surveillance is practiced. For example, mobile communications are monitored on a large scale as well as implementing mandatory SIM card registration which facilitates establishing detailed databases about individuals including location tracking and removal of communication anonymity. In addition, it has been reported by Citizen Lab that a

[32] Frenkel, S. & Atef, M. (2014) Egypt Begins Surveillance of Facebook, Twitter, and Skype on Unprecedented Scale, BuzzFeed, Retrieved from https://www.buzzfeed.com/sheerafrenkel/egypt-begins-surveillance-of-facebook-twitter-and-skype-on-u?utm_term=.bjXXAV9aO#.ypJlQ1Zny

[33] Beck, J. (2014) Egypt is Readying a Massive Surveillance Program for Social Media, Vice News, Retrieved from https://news.vice.com/article/egypt-is-readying-a-massive-surveillance-program-for-social-media

[34] Frenkel, S. & Atef, M. (2014) Egypt Begins Surveillance of Facebook, Twitter, and Skype on Unprecedented Scale, BuzzFeed, Retrieved from https://www.buzzfeed.com/sheerafrenkel/egypt-begins-surveillance-of-facebook-twitter-and-skype-on-u?utm_term=.bjXXAV9aO#.ypJlQ1Zny

program called PackageShaper has been detected in Turkey. It's used for internet filtering and possesses data-collection capabilities which could be used for surveillance. Spyware which provides the ability to observe and control a targeted computer has also been identified.[35]

A law amendment adopted in 2014 provides the Telecommunications authority with the ability to block any website within four hours without seeking a court ruling first; moreover, it forces internet providers to store the users' activities for two years and make them available to authorities when requested.[36] This has led to tens of thousands of websites to be blocked over the past years and also obstructed access to Youtube and Twitter for a period of time after the wiretaps of conversations between top officials were leaked through social media. Subsequently, the Constitutional Court annulled the proposed amendments, but the intent to increase the state's reach is clearly there.[37]

Furthermore, a law passed in April 2014 largely expanded the surveillance powers of the National Intelligence Agency by giving them powers to collect private data, personal information, and documents in all forms without needing to acquire a court order. This includes the ability to intercept, store, and analyze internet traffic, text messages, and mobile calls. Additionally, immunity is provided to employees of the intelligence agency in case a complaint was filed to the prosecutor. This immunity would be granted if the head of the intelligence agency stated that the actions undertaken were connected to the "duties of the agency".[38] More

[35] Privacy International (2015) The Right to Privacy in Turkey, Privacy International, Retrieved from https://www.privacyinternational.org/sites/default/files/UPR_Turkey.pdf

[36] Letsch, C. (2014) Turkey Pushes though New Raft of Draconian Internet Restrictions, The Guardian, Retrieved from https://www.theguardian.com/world/2014/feb/06/turkey-internet-law-censorship-democracy-threat-opposition; Stupp, C. (2014) Erdogan Tightens the Digital Screws on Free Expression, Index on Censorship, Retrieve from https://www.indexoncensorship.org/2014/09/turkeys-new-internet-restrictions-danger-user-privacy-access-information/

[37] Pamuk, H. (2014) Turkey's Top Court Annuls Part of Law Tightening Internet Controls, Reuters, Retrieved from http://uk.reuters.com/article/uk-turkey-internet-idUKKCN0HR20B20141002

[38] HRW (2014) Turkey Internet Freedom Rights in Sharp Decline, Human Rights Watch, Retrieved from https://www.hrw.org/news/2014/09/02/turkey-internet-freedom-rights-sharp-decline

recently in March 2016, a data protection law was passed which allows the extensive collection of information such as ethnicity, religious beliefs, political ideas, and outward appearance (headscarves)… It also forces third parties to hand over data they have to security agencies without having to obtain a warrant. In spite of stating that "sensitive personal data cannot be processed without the consent of the individual", the power given to governmental agencies with little oversight opens the door to exploitation of such data, especially with article 28 of the law relating to national security.[39] The expanded surveillance powers passed in this law are very similar to the amendments which were previously annulled in 2014 by the Constitutional Court.

In the three cases, there is a clear attempt to either ignore the law or try to amend it in order to increase the scope of surveillance being practiced by security agencies. The pretext of fighting terrorism and preserving national security is repeated constantly and without exception. This could be an attempt to fend off the rising threat from extremist groups in the region, but it could also put the rights and freedoms of the public at risk. Moreover, the reported presence of far-reaching surveillance programs developed by leading technology companies in the world sets a dangerous pattern to both the use of such technology by security agencies and its sales to states with questionable human rights records. The increased presence of such technologies in a region like the Middle East with its well-known history of political repression undoubtedly raises many concerns and should not be taken lightly especially since some of its effects are starting to show with the targeting of certain groups and arrests of activists... If such programs are causing huge controversy in Western countries that are considered democratic and respect the rule of law, then their spread in the Middle Eastern region should cause an equal if not larger reaction.

[39] Shaw, C. & Sentek, Z. (2016) Citizens will be Stripped Naked by Turkey's Data Law, Computer Weekly, Retrieved from http://www.computerweekly.com/news/450280254/Citizens-will-be-stripped-naked-by-Turkeys-data-law

Regardless of whether surveillance technology is being used to monitor the population and crackdown against opposition movements or to uncover terrorist attacks, the threat that this overreaching system poses is definitely there. The presence of such technology in the hands of a small number of people poses a danger to the freedom of the rest of the population, especially if opposition protests erupt against those in power. The technology created and developed with the alleged aims of combating terrorism and crime could later on be used as a tool of oppression. All of this should serve as a wake-up call to strengthen democratic institutions, ensure public accountability, enact legal regulations, and initiate social and political changes that protect the public from the possible abuse of this technology[40]; moreover, history has shown that oppression and authoritarianism are not the most successful tools in combating terrorism, especially on the long-run, since such tactics will generate more hate and radicalism. On the other hand constitutionally protected freedoms and judicially regulated monitoring remain prerequisites for any healthy sustainable security.

[40] Lempert, R. (2013) PRISM and Boundless Informant Is NSA Surveillance a Threat, Brookings Institution, Retrieved from http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert