CHARLES UNIVERSITY IN PRAGUE

UNIVERSITY OF KONSTANZ

Davit Petrosyan

Gustav-Schwab str. 10, apt 10

Konstanz, Germany, 78467

davitpetrosyan.edu@gmail.com

Master's Thesis

The Dilemmas of SurveillanceProfiling: The Case of the United States

Dual Master's Program

Fields of Study: MA in International Security Studies

MA in International Administration and Conflict Management

First supervisor: Dr. Vit Stritecky

Second Supervisor: Dr. Alexander De Juan

DECLARATION:

I hereby declare that this thesis is my own work, based on the sources and literature listed in the appended bibliography. The thesis as submitted is 115518 keystrokes long (including spaces), 52 manuscript pages.

Davit Petrosyan, 20.12.2017

Contents

Introduction to the Thesis and the Importance of the Topic

The sorting and the categorization of individuals and groups by their capacity and inclination to risky behavior or level of dangerousness has been and remains an essential function of security apparatus of the state and a vital component in state security. Practices of this kind became even more important in the age of international terror. The western world and specifically the United States has been the primary target of international terror suffering numerous terrorist attacks including the 9/11 attacks that became thedefining moment of how security functions in themodern world. While what we call 'western world' is dominantly defined by liberal democratic political order, many of its societies and specifically the US is also defined by atechnology-enabled environment that scholarship characterizes as 'surveillance society' (Gandy 1989, Lyon 2001, Lyon & Bauman 2012).

Withintechnology-enabled environments the technologization of security was inevitable (Ceyhan 2008), and the 9/11 generated even more intense and enhanced efforts ofspeeding this process up (Lyon 2004, Ball and Webster 2003). In the post 9/11 US war on terror, specifically surveillance technologies became central to security policies (Ceyhan 2006) as universal security enablers (Lyon 2003). All technologies that are at the core of security policies and are designed to be enablers of the pursuit of safe state entail surveillance in some fashion (Lyon 2007).In their pursuit of security, surveillance technologies and techniques such as data mining, for example, are potent to provide certainty not only about past and present but most importantly about future (Ceyhan 2008). Data mining or KDD (knowledge discovery databases) technique many times provides "with answers to questions" that the users of it "did not know to ask" in advance(Zarsky 2002-2003: 6). The aggregate data, collected and mined through technologies, brings together possiblyvast amount of information on targets. Such data includes not only conscious but also unconscious behaviors (Ceyhan 2008) that are stronger predictors of future and subject touncontrolled repetition (Lyon 2007) leading to certitude in expectations.It is the reason why in security in general and in thewar on terror particularly, the strategy of possibly close and best monitoring potential and actual sources of threats has no equally good alternative despite its problematic nature (Thorburn 2012). Among other components, it is enabling the intervention and the altering of the course of the events before they occur enabling adaptive pre-emptive and preventive security strategies (Brakel and Hert 2013).

Surveillancehas many definitions. Lyon defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007: 14). Another definition by Ceyhan is that surveillance is the "systematic attention to personal data with a view to manage, influence, discipline and monitor people" (Ceyhan 2008: 119). In terms of preventive and pre-emptivesecurity policies, surveillance processes and practices are aiming to create theprofiles of actual and potential sources of threats with high accuracy toproduce security. Profiling in the domain of security is conceptualized differently from other fields. The process of profiling for security and risk purposes as described by Lyon is the gathering of all sorts of data and manipulation of it to produce risk categories within "a fluid network" (Lyon 2007: 23). Marx and Reichmann define profiling as "systematic data searching" enabling to "correlate a number of distinct data items in order to assess how close a person or an event comes to a predetermined characterization or model infraction" (Marx and Reichmann 1984: 429). The nature of this sort of practice becomes more risk-oriented, meaning prioritization of assessment of potential risks in advance rather than focusing on existence or absence of danger (Ceyhan2008).

Because surveillance in thefight against terrormust be a covert action to achieve its goal (Kitrosser 2007), in this circle of knowledge production and its operational execution specifically in the USwar on terror, the knowledge and consequently the consent of profile owner is being excluded from the process (Lyon 2001). This kind of practices within liberal democracies has been found to generate negative influences, controversies, compatibility issues with the defining principles of political design of the liberal state (Kreimer 2004, Monohan 2010, Bigo 2012, Andersen 2016). Surveillance is "treated as inevitably infringing liberal conceptions of the rights of individuals and citizens" (Gilbert 2007: 11).While the simple view as Bigo puts it is that security safeguards democracy, it is important to study "how liberal states always try to exonerate themselves from accountability, transparency and general democratic practices in relation to their use of high policing, intelligence services and national security" (Bigo 2012: 280). According to Lyon, surveillance profiling practices of thestate is rather "form of organization of power through surveillance strategies" (Lyon 2007:4) while as Monohan states, surveillance "at its core is about control" (Monohan 2010: 91). Social control is defined as "mechanisms for ordering society through the regulation of individual and groupbehavior" (Monohan 2010: 96). Security surveillance that by nature not only demands secrecy but also

aims total inclusiveness is overcoming one of the last barriers to total social control (Lyon 2007: 5). In 2013 Edward Snowden revealed, that while the public in theUS has been heavily surveilled, the watchers themselves were exempted from surveillance signaling exactly the structures of social control.

As the minimization of risk has become to be the top priority for themodern state in general (Lyon 2007) and as already mentioned, for post 9/11 US, the use of surveillance technologies by the US government for security purposes also produced controversial consequences subject to examination in terms of their nature and influences. While the government in theUS as in any liberal democracy is constrained by "political, ideological and institutional factors" it has always been obvious that in the face of intensive threats to their national security (such as international terror for example) democratic governments "do not always measure up to their own stated ideals" (Rogerson and Milton 2013: 463). The executive branch of the US government enabled covert mass surveillance programs in an unconventional and out of order manner that did not necessarily fit well within structural checks and balances designed to prevent asymmetry among branches of the government and its accountability to the public. According to the Bush administration and the DoJ under Bush administration, the secrecy of secret mass surveillance programs is necessary to contain and control tremendous risk of exposure potentially leading to destruction and ultimately failure of missions of intelligence and security agencies (DoJ 2006). This would risk causing irreversible damage to the US national security. Bush administration believed that the norms of usual time are subject to being "outweighed by critical public interest" (white paper on sec. 215: 19) such as national security. The administration did not claim of having been completely guided by directives of FISA (Foreign Intelligence Surveillance Act) in its actions but tried to root the legitimacy of its actions within presidential power in emergencies and crisis (Kitrosser 2007) for defending the nation (Doj 2006). In the course of architecting adaptive and more reflective security apparatus in the post 9/11 US that deploys mass surveillance to counter threats, it has become clear that indiscriminate practices of this kind oppose and pose challenges for alist of US constitutional rights (Ballet. al 2009) including thepresumption of innocence of persons for example that is a vital legal entitlement for thecitizen of constitutional democracy (Thorburn 2012).

There isaconsensus in scholarship, governments, and public intellectuals in general that it is fundamentally imperative to examine the meaning and the influences of modern

surveillancetechnology on state and society. In 2013 President Obama ordered adetailed investigation to review the meaning and the impact of intelligence and communication technologies from the perspective of the US government. The task has been assigned to the Presidents Review Group on Intelligence and Communication Technologies. In the'Report and Recommendations of the Presidents Review Group on Intelligence and Communication Technologies: Liberty and Security in Changing World', the commission concludes, that the narrative of balance between security and liberty contains elements of truth but it is "also inadequate and misleading" because there are safeguards of liberty that cannot be and should not be subject to balancing (The Presidents Review Group report 2013: 16). At the same time surveillance programs and technology has been described many times as vital security enabler and tool in War on Terror both by scholars (Lyon 2003, Ceyhan 2006,TAPAC 2004) and importantly also practitioners including the former Director of Federal Bureau of Investigation James Comey and currenthead of National Security Agency Michael S. Rogers who very recently described those programs as "critical, indispensable, vital" to U.S. national security[1]. This means that such programs simply cannot and will not be eliminated.

While specifically security surveillance and profiling practices of liberal state are referred as undemocratic and even anti-democratic, the capacity of scholarship of studying this field of state activity empirically remains very limited. The reason is that the nature of state practices of this sort demands secrecy and denies access to outsiders. In post 9/11 period,however, in the process of the US waging war on terror, there has beenseveral remarkable events that coming together form a chronological chain with anavailable linked information on each of them. Those are leaked classified government materials, partly declassified government documents and adopted legal documents, open congressional hearings on this matter, interviews of whistleblowers, testimonies and statements of insiders of intelligence and government officials enabling studying the issue for the specific case of the US.

In this thesis, I am aiming to examine how the US government's security surveillance and profiling practices in the War on Terror have impacted the political system and the state of democracy in the US. My hypothesis is that US security surveillance programs in post 9/11

[1]20/03/2017 testimony of heads of FBI and NSA before Senate Intelligence Committee on alleged Russian interference in 2017 US presidential elections

period War on Terror had eroding negative influences on legal and political norms, demonstrated incompatibility with defining core principles of the design of the US political system as liberal democracy. The thesis is a case study.

Brief introduction to the methodology

As I am studying a process based on qualitative data where the cause leads to an outcome, the essence of theselected method must be the capacity to link the cause to the outcome. Because of this reason, process tracing is the best fitting methodological tool for conducting this research. Collier describes process tracing as"a fundamental tool of qualitative analyses" (Collier 2011: 1). Itis a toolenabling to take diagnostic evidence and through intensive static description and analysesdraw descriptive causal inference for which it is very important not specifically focus onchange itself but on series of specific moments (ibid). As Bennett and Checkel define "process tracing is analyses of evidence on processes, sequences and conjectures of events within a case for the purposes of either developing or testing ahypothesis about causal mechanisms that might causally explain the case" (Bennett and Checkel 2015: 7). Because of theinfluential configuration of theindependent variable (Seawright and Gering 2008), the case of the US qualifies as an influential case and the main mission of influential case analyze is the validation of general theory (Gerring 2007).

To examine thecertain type of materials such as statements and interviews of government officials, intelligence officers,and whistleblowers that represent interest from the perspective of this research, I will also use critical discourse analyses (CDA). CDA is "specifically interested in power abuse that is in branches of law, rules and principles of democracy, equality and justice by those who wield power" (Van Dijk 1993: 255).

The first part of the thesis focusing on the idea of surveillance and its meaning in liberal political order coversthe background of the topicby addressing it in the chapters on the state of the modern surveillance and technology, the meaning of it in liberal political order, the meaning of surveillance in terms of social control. It is followed by the discussion on the selection of methodology for studying the case of the United States. Following this, the analytical part addresses specifically the case of the United States and includes chapters on politics of surveillance in theUS, the relations in US government structure in terms of surveillance,

examination of thelist of events linked and referring to the US security surveillance programs in chronological order. Those events include the adoption of 2001 USA PATRIOT ACT and its influence, DARPA's Total Information Awareness Program, 2005 The Washington Post leaks on mass surveillance programs, 2007 secret Foreign Intelligence Surveillance Court orders, 2013 Snowden revelations and post period including very recent leaks from WikiLeaks in 2017 under code name Vault 7. The thesis ends with conclusions and bibliography. The thesis overall contains 55 pages, 110 name bibliography, including books, scholarly and journal articles, interviews etc.

The Age of Surveillance

In the process of identification and association of actual and potential threats technologies play avital role. The primary event over which there is aconsensus in scholarship as the cause of acceleration and intensification of both production and use of surveillance technologies has been 9/11 (Lyon 2004, Brakel and Hert 2013, Ball and Webster 2003). Since 9/11, risk assessment, surveillance, and identification technologies have become the "centerpiece" of security policies (Ceyhan 2008: 102) because in the war against terror technologies are considered as universal security enablers (Lyon 2003, Ceyhan 2006). Because security demands 'certainty' (Lipschutz 2000: 1), the environment with extended threats created necessity, popular support, and demand for high-security features aiming inclusive identification of all subjects. Certainty means "confidence attributed to particular knowledge" (Ceyhan 2008: 103). As Ceyhan formulates "in the realm of security what is at stake is not only the certainty about figures(s) of enemy and possible threats, but also certainty about present and future, certainty about the political economic, strategic and tactical tools that liberal society produces to be successful" (2008: 3). The necessity of developing and enhancing security tools and strategies is constant because security never can be total as it has no fixed boundaries and rather depends on the situational change in liquid reality (Lipshutz 2001). Threats can emerge at any time in any environment. Therefore, the kind of strategy that is built to face threats of this kind should be 'adaptive' in its nature (Brakel and Hert 2013). New emerging realities within globalized world challenge the capacity of state in remaining competent towards new threats and movement of possible sources of threat. It is no surprise that after 9/11 the rhetoric of securitization with an unclear distinction of internal and external threat has been dominant given the fact that unexpected terrorist attacks against many countries and specifically targeting the US and its citizens are rather 'expected unexpected'. In these terms, arguably, the traditional model of the liberal state is losing its capacity of successfully accommodating material realities on the ground due to the incompatibility of those realities with operating legal and political norms derived from defining principles and design of the liberal system (Weber 1947). Within this new environment, influenced and shaped by international terrorism among other factors, high tech has become to enable security agencies in the identification of risks, threats and sources of them with unprecedented certainty. Technologies such as biometrics, video-cameras, chips, smart cards, scanners, databases, computers etc. are central to facing internal and nontraditional external

threats (Ceyhan 2008). Not only technology is the tool enabling the identification and assessment of threats, but more vitally it is the one for "monitoring the future" (Ceyhan 2008: 107). Usage of digitalized profiling is pursuing one particular target which is the detection of threats, prevention of crime and violence before it would take place (Brakel and Hert 2013). After 9/11 US authorities determined that technological and electronic capabilities of state should become central for intercepting terrorists within and outside the borders of the US. Homeland Security Advanced Research Projects Agency has been established with the mission "to identify and develop revolutionary technologies, satisfy state, local and federal agencies operational needs for advanced technology".[2]

In modern times, the prime strategy of fighting threats and individuals posing it is to monitor them as best and close as possible and apply to pre-emptive measures to secure (Thorburn 2012). The main function of identification technologies is to "gather, process and disseminate" attributes of targets to identify and by doing so provide with documented evidence leading to "certitude who is who, and who does or did what" (Ceyhan 2008: 109). Using possibly maximum data as input, computers can create dossiers of a large number of subjects based on a vast amount of conscious and unconscious acts and moments of life (Ceyhan 2008). As an outcome of this process, the dossiers attach labels of potential risk or threat to owner becoming determiners of treatment the owner receives many times without even realizing it(Bigo 2012).

Lyon defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007: 14). Ceyhan defines it as "systematic attention to personal data with a view to manage, influence, discipline and monitor people" (Ceyhan 2008: 119). From the perspective of this research, those definitions go beyond the alternative definitions and provide with a complex description of what the surveillance represents as phenomena. The nature of this sort of practice becomes rather risk-oriented, meaning assessment of potential risks rather than focusing on existence or absence of danger (Ceyhan 2008). Security technologies enabling profiling can be classified into three groups. Technologies focusing on biological aspect measuring genetics, attributes of body etc., optical and electronic such as laser, glass etc. and information and communication technologies

[2]Homeland Security Subtitle G of the Title VIII of the Homeland Security Act of 2002: The Support of Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act).

(ICT-s) (Ceyhan 2008). They can be deployed in multiple forms ranging from “intelligence surveillance systems to DNA samples passing by USB keys, chips, sensors, cables, wiretaps, cameras, internet etc” (Ceyhan 2008: 108).

Profiling in the domain of security is conceptualized differently from other fields. The process of profiling for security and risk purposes as described by Lyon is gathering of all sorts of data and manipulation of it to produce risk categories within "a fluid network" (Lyon 2007: 23). Marx and Reichmann define profiling as "systematic data searching" enabling to "correlate a number of distinct data items in order to assess how close a person or an event comes to a predetermined characterization or model infraction” (Marx and Reichmann 1984: 429). From the perspective of national security, the ‘predetermined characterization or model infraction' are the risks and threats of committing a crime, producing violence and conducts of any kind that are potent or represent a threat to national security of the state. Some of the common features detected in process of profiling are “categorization...deduction from known knowledge to expected...the use of produced information" (Bosco et.al. 2013). Another definition of profiling is "profiling is a technique whereby a set of characteristics of a particular class of a person is inferred from past experience, and data holdings are then searched for individuals with a close fit to that set of characteristics" (Clarke 1993: 2). Because the process is done through data mining and statistical analytical correlation by computers, the risks are assessed based on variables in a profile that are also not criminal themselves but are types of oral and written signals, images, behavior correlated with risk (Lyon 2003). Consequently, profiles of subjects and groups are an aggregate type of knowledge based on mined data input (Fuster et. al. 2010, Fritsch 2008). This kind of knowledge is very probabilistic in its nature (Fuster et. al 2010). In this circle of knowledge production and its execution, the knowledge and consequently the consent of profiled subjects are being excluded from the process due to the very nature of security surveillance (Lyon 2001).

Profiling can be non-automated or organic, automated and autonomic (Bosco et. al 2013). In this case, specifically the second and the third one that is the most comprehensive and sophisticated form excluding human intervention to the production process (ibid) are addressed. Automated surveillance systems that by principle are binary frozen into codes classify as positive or negative with no negotiation (Norris in Lyon 2003 (ed): 276). This creates risks of negative discrimination also by mistakes which are unavoidable as computers make decisions based only on input

without making assumptions of any sort. From the perspective of targeting there are group, distributive group, non-distributive group and personalized or individual profiling (Bosco et. al 2013). "Group profiling focuses on one or more common attributes of people... distributive group profiling identifies certain number of people with one or more shared attribute...non-distributive profiling focuses on members of group that do not share all attributes of groups profile...and personalized profiling relying on set of attributes subscribed to particular subject" (Bosco et. al 2013: 7).

The most comprehensive technique that is used for profiling is called Knowledge Discovery in Databases (KDD) (ibid). This technique provides "with answers to questions" that the users of it "did not know to ask" (Zarsky 2002-2003: 6). KDD or otherwise data mining is defined as "nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data" (Fayyad 1996: 2). The use of large databases with this method can enable prediction of the behavior of all kinds from political preferences to personal preferences (Bosco et. al 2013). Processed data includes what people engage on a routine basis and more importantly also unconscious actions many times which are stronger predictors prone to uncontrolled repetition (Lyon 2007).

As mentioned above, identification of patterns is rather based on correlation and not causation and the aggregate profiles are not associated as single but through cross-examination of profiles through deductive and inductive logic (De Zwart 2014). Profiles created through algorithms may result in a product which in reality does not match to the behavior of an individual. The meaning of it in the current level of technological capacity is first of all the identification and assignment of the profiles to a certain class or category within which the accuracy of predicting the possible range of actions and reactions becomes much more accurate (Gilbert 2007). Creation of many positive cases of profiles from the security perspective that are negative in reality is unavoidable (ibid). The vital issue from the perspective of security, however, is the non-exclusion of positive profiles that would decrease the efficiency leading to violence and harm to the security of the state.

In process of identifying the targets with certainty, the most efficient and the "ultimate technology" (Ceyhan 2008: 101) is biometrics. The use of biometrics in fighting to insecurity has become security norm globally (Salter 2006). The word biometrics is derived from Greek words

‘Bios’ meaning life and ‘Metron’ meaning measure. The function of biometrics is the identification of an individual through "authentication of his/her identity by measuring his/her unchangeable body parts" (Ceyhan 2008: 3, Lyon 2003) transforming it into a source of information and readable text enabling to trace the movement and actions (Ceyhan 2008). But to be able to use physical biometrical profiling, the identity of the subject has to be determined earlier to be linked to the biometrical profile the data of which is either missing or is inaccessible many times. From the perspective of what is included in the profile, there are different types of profiling. Two of them called behavioral profiling and biometrical behavioral profiling are of interest of security dimension. Behavioral profiling “is the study of patterns of behavior and the consequent grouping of the subjects according to emerged behavior that emerges” (Bosco et. al 2013: 10). Biometrical behavioral profiling “measures human characteristics related to conscious and unconscious actions” without focusing on physical features of targets (Bosco et al 2013: 12). Both deductive and inductive principles are applied in this process.

Surveillance in Liberal Political Order

As a scientific field, one of the main tasks of surveillance studies in the context of surveillance and control within a nation state is to examine “how liberal states always try to exonerate themselves from accountability, transparency and general democratic practices in relation to their use of high policing, intelligence services and national security” (Bigo 2012: 280). A simple view as Bigo puts it is that security is what protects democracy (ibid). However, the rhetoric of going beyond normal politic in emergencies to assure the survival of political order can become more of a threat to the liberal political order itself (Bigo in Ball et al 2012). The difference between traditional state and the modern one in terms of strategic policy planning is that now states dominantly put the minimization of risk in the core as first priority replacing "the positive benefit for all" that traditionally occupied that role (Lyon 2007: 25). The powers that government of liberal state claims when going beyond what is considered to be a norm in usual times by warranting suspension of civil liberties and constitutional rights as reaction to emergencies, special times or for prevention of their occurrence (Bigo 2011) is justified with argument that it is a necessity for overcoming imminent and existential threats to national security (Andersen 2016). The process of legitimization of special measures in advance to prevent special occurrences is what lies in the argument for possibly more information gathering enabling extraction of actionable intelligence (Bigo 2012).

The value of information security in modern times for state and policymakers is critical. The overlapping concepts of safe state and surveillance society (Lyon 2007) are important ones when it comes to understanding the role of surveillance technologies in the creation of the new environment within which members of society operate. When mass surveillance programs are implemented as part of governments conduct aiming national security, the codes that are used for categorizing individuals and groups are classified as official secrets (Lyon 2007). It is imperative to notice that in a democratic system, governments not always can have total control over the implementation of all kinds of policies involving information secrecy legally just by linking it to national security. In liberal political order, governments are constrained by "political, ideological and institutional factors" (Rogerson and Milton 2013: 463). However, it is necessary to notice as well that threats make democratic regimes “not always to measure up to their own stated ideals” specifically in terms of information transparency (ibid).

The application of surveillance for security purposes is rooted in the realization of the authoritative power of government as a rational form of authority that is based on the argument of efficiency (Weber 1978). What is also important to look at is the second characteristics of rational authority that is legality (Rogerson and Milton 2013). In this process of assuring efficiency, legal tensions caused by surveillance in a liberal democratic political system is intense, immense and growing (Richards 2013).

It is self-evident that collection and processing of personal data are critical in delivering efficient governance (2009 House of Lords Report on Surveillance). However, it is self-evident too, that there has to be limits defined and placed for balancing the good and the bad such conducts can produce. As 2009 report of House of Lords on surveillance states "trust in the state is an essential prerequisite for compliance with the law" (p27) and therefore erosion of that trust by covert activities of state without popular consent is potent to erode democracy. From certain perspectives, and specifically from the legal perspective, the shaping of the behavior of citizen is a function of governmentality. It is the identification of identity that enables "private interactions juridically possible" which is guaranteed by governmentality (Ripstein 2009:13). It is central to state apparatus for which it is imperative to know 'who is who and who is where' to support the environment where the laws are operational (Thorburn 2012).

Despite the fact, that government surveillance is subject to legal procedures and authorization, according to Bush administration and the DoJ, taking secret security surveillance programs through usual procedures would harm and even potentially dismantle the ends the programs are there to pursue by dramatically increasing the probability of leaks and exposure. This would lead to deficiency, destruction and ultimately failure of missions aiming to enable and empower the US security apparatus and the national security of the state. At the same time, the administration has been aware of the fact, that covert mass surveillance programs oppose and pose challenges for constitutional rightsensured by thedemocratic political system (Ball et. al 2009).Mass and covert surveillance programs are perceived as signals that the government has no trust for its citizens.The indiscriminate creation of individual profiles by the state for identifying potential threats puts owners in 'categories of suspicion' (Marx 1998). It goes beyond boundaries of the presumption of innocence (Brakel and Hert 2013). The presumption of innocence that is a vital legal principle for the citizen of a constitutional democracy is incompatible with nature of

surveillance and profiling (Thorburn 2012) because it also aims knowing and shaping the state of wrongdoings before they occur. It is not a coincidence that as Gilbert mentions surveillance is "frequently treated as inevitably infringing liberal conceptions of the rights of individuals and citizens" (Gilbert 2007: 11).

Surveillance and Social Control

By nature, surveillance “at its core is about control” (Monohan 2010: 91). Social control is defined as “mechanisms for ordering society through the regulation of individual and group behavior” (Monohan 2010: 96). The phenomenon of modern surveillance is overcoming one of the last barriers to total social control (Lyon 2007: 5). Classification and categorization of people by their proneness to risk such as violence can be seen also as "form of organization of power through surveillance strategies" (Lyon 2007: 4). Government surveillance practices in the US exposed by Snowden revealed that while citizens were subject to every day monitoring, the executive has been exempted from being watched and so contributing in further asymmetric changein relative balance created by the design of the political system (Muir 2015).

Thetargets of mass surveillance have not much knowledge of how surveillance systems work, and because systems are close by nature, they “resist opportunities for democratic participation in how they are designed, used, critiqued or regulated” (Monohan 2010: 91). Monohan defines surveillance systems as enablers of “control of the people through identification, tracking, monitoring and/or analyses of individuals, data or systems” (2010: 96). Information systems are specifically oriented towards “data creation, collection and analyses for the purposes of intervention and control” (ibid: 95).

The spread of technology has created a state where surveillance goes "beyond non-consensual" (Richards 2013) creating so-called ‘liquid surveillance' (Bauman & Lyon 2013). It is defined by unknowingly provided or manufactured consent and participation of targets willingly possessing respective devices and engaging in activities. Many times, people do not voluntarily provide information but they do so unconsciously. Moreover, they do not and practically cannot consent or oppose its use (De Zwart et al 2014). As Marx characterizes modern information society, it is transparent in its character enabling an increase in the possibility of documentation and analyses of our ‘history, current identity, location, psychological states, and behavior’, creating predictive profiles that possibly enable determining ‘individual futures’(Marx 1998). The categorization as the product of this process that is aiming to the influencing and managing individuals and groups is affecting "the choices and chances of data subjects" (Lyon 2003: 13).

The meaning of categorization by its very nature is discrimination. Classification of subjects and formations by their dangerousness automatically creates social sorting and treatment based on the class (ibid). In the core of the process, we have the individualization of securitization andchanges in perception of old and new threats some of which actual and others only perceived creating the sense of the necessity for more control (ibid).

As Marx assesses the potential of new surveillance technologies, he characterizes them as capable "to reveal the unseen, unknown, forgotten or withheld" (Marx 1998: 172). Therefore, surveillance enables persuasion of targets through increased persuasion power based on information not possible to obtain otherwise. The use of this product by government, security and intelligence agencies results increased capacity of watcher to monitor, control, direct and even create behavior (De Zwart et. al 2014, Richards 2013). One of threats government surveillance poses is the creation of such an asymmetry between 'watchers and the watched' when the firstcanapply to selective treatment, discrimination, even blackmail (Richards 2013) leading to erosion and ultimately destruction of liberal principles and democracy. There are two instances where anti-democratic nature of this kind of surveillance is specifically rooted. First is that surveillance technologies "act as forms of legislation without much if any democratic participation or representation" and the second is that because of the first "social inequalities are aggravated rather than ameliorated, which hinders the actualization of democratic modes of associated living" (Monohan 2010: 100). Certain types of surveillance challenge the democratic form of political system more than others. Particularly, those are systems of differential and automated control (ibid: 97). Combination of those two poses greater threat to democracy as the classification is done by artificial intelligence (ibid).

Thorburn identifies three types of use of data that government collects on citizens with purposes of consequential application (Thorburn 2012). First one is identification which he defines as "regulating and guaranteeing the identity of individual", the second one is surveillance which is the "capturing of specific information about our activities" and finally the profiling which is subscription of certain attributes to individual based on "what particular persons or classes of persons look like" (Thorburn ibid: 16). Due to the diversity of information as a representative aggregation of data from nearly all fields of life where we can differ in our character, the divide between those fields of activities is 'collapsing' (Boyd 2008: 14). Distinct from nature activities

and conversations immigrate to contexts through time that may possibly receive very different and unpredictable meanings (Bigo 2012). This process is taking place within an environment where "abstract data including video, biometric and genetic as well as compromised administrative files are manipulated to produce profiles and risk categories in a liquid networked system" (Lyon 2003: 13). The attributes of the system such as ‘liquid' and ‘networked' are of special importance in understanding the meaning and impacts of surveillance and the ways it functions. The term “liquid surveillance” means “circulating, connecting and reconnecting different spheres of the social, reframing their boundaries and creating new networks of information and power” (Bigo 2012: 281). Cross-examination and interactive communication between different sorts of data is the key to the more accurate production of prediction.

The Selection and Discussion of Methodology

The nature and the meaning of modern surveillance and particularly the US government mass security surveillance programs have been a source of countless debates and discussions in recent decades. Scholars, politicians, investigative journalists, and intellectuals, in general, recognize the relevance and the social importance of the issue, the necessity of understanding the socio-political and scientific meaning of phenomenon in terms of its influence on society and the state. The case of US mass surveillance programs has been very important empirically making resonance internally and worldwide and scientifically in terms of yet incomplete but unprecedented availability of produced evidence for studying this particular field of state activity that by nature demands secrecyanddenies access. The preliminary study of some of the materials hints evidence for a positive outcome in terms of the theoretical assumption that mass surveillance programs of US government not onlyhave tense relations with vital and defining principles of the design of the political system but in certain instances demonstrate incompatibility and as an outcome in the course of their implementation negatively influence and erode the structures placed by political system.

Because of the influential configuration of the independent variable (Seawright and Gering 2008), the case of US government surveillance qualifies as an influential case. The main mission of influential case analyze is the validation of general theory (Gerring 2007). Case-based research focuses on the causal relationship within an individual case as in this particular study in contrast to variance based research that is focusing on the population mean. The traditional observational case studies where tracing is oriented towards finding out the variance caused by treatment of dependent variable (y) by the independent variable (x), producing difference making evidence, can be contrasted to within case in depth tracing producing "mechanistic" evidence(Beach and Pedersen 2016)**.** The application of case selection guidelines for traditional causal mechanism based research is rather problematic compared to approach taking causal mechanisms as a system for in-depth within case analyses (ibid). As Beach and Pedersen put it "studying mechanism in particular cases focuses on in-depth empirical analyses of what actually happened in the case to shade light or how the cause (or set of causes) produces an outcome…" (Beach and Pedersen 2016: 4). Tracing a process to understand functioning mechanisms is beyond examining a single variable intervening and making the change. It is rather understood as

a system the parts of which interacting transmitting causal forces from causes to outcomes (Machamer 2004, Machamer, Darden and Craver 2004).

Because of its clandestine nature, studying government security and intelligence surveillance programs poses extraordinary problems in terms of uncovering and concluding the causation logic and operating mechanisms. The information produced in the field is largely classified, confidential and for a strictly limited audience. For this reason, the case of US is unique not only because of the huge empowered independent variable, but as mentioned above, has no good alternative in terms of materials for studying the phenomena. Materials include legislative acts on surveillance, leaked classified documents, interviews of former members of US intelligence community, articles of investigative journalism and declassified documents approved for public release (most of the time declassified partly only) etc. In addition to this, materials such as political statements of government officials and congressional testimonies showing the evolution of process also representing value for studying the process has been considered.

As I am studying a process based on qualitative data where the cause leads to an outcome the essence of the selected method must be the capacity to link the cause to the outcome. Causation is not "just X: Y patterns of constant conjunction or manipulation of X to produce the difference in values of Y" but it can be understood also as a system(Beach and Pedersen 2016: 5). Causal mechanism is described as an ordered sequence of events in combination with entities engaging within evolving process that transfer causal forces (Beach and Pedersen 2016, Machamer 2004). At the same time activities are exactly what transmit the forces of the cause into effect or X to Y (Macahmer et al. 2000). In outcome producing process as a system, the integral parts of it are not independent in their relations to the outcome but rather have transmittive power in combination (Beach and Pedersen 2016).

The causal mechanism should be traced empirically well enough to theorize it explicitly through the understanding of underlying causal logic. Tracing mechanisms have become an increasingly more used method for studying cases (Beach and Pedersen 2016). In contrast to large N studies that provide ‘width' case studies provide more depth or detail richness, completeness, wholeness described in the literature as ‘thickness' (Blatter and Blume 2008) providing the case study with superior internal validity (Gerring 2007). The presence of control group in within case study is not compulsory when the case is an example where "the causal effect of one factor can be

isolated from other potentially confounding" (Gerring and Seawright 2007: 122). Control group for this study is irrelevant so far as "process tracing offers us analytical tools that can enable us to control for other causes working at the empirical level" (Beach and Pedersen 2016:17).For within case study, the existence of more than one X leading to Y is not problematic even if it is unchecked**.** It can be assumed that X1 and another sufficient X2 are leading to Y outcome and it can theoretically be assumed they are linked via different mechanisms. Therefore, it is possible to distinguish them by evidence through the use of tools offered by process tracing making the presence of confounding variables not an issue (Beach and Predersen 2016). Consequently, the possible application of the rival methods and specifically counterfactual form of explanations were excluded because it does not represent "core explanatory tool in case study settings" (Goertz and Levy 2007: 18).

To understand the functioning system, we need to focus on entities that are "things engaging in activities" and composing activities which are "producers of change" (Machamer Lindley and Carl 2000, p. 3). The mechanism has a variety of definitions and one of them is "mechanisms are entities and activities organized such that they are productive of regular changes from start or set-up to finish or termination conditions" (Machamer Lindley and Carl 2000, p. 3). It is the organizational combination of those two that produce the Y.

Given its attributes as a scientific tool, causal process tracing qualifies as the best fitting method for this study. CPT specifically fits for studying the type of available in this case qualitative evidence that by its form and nature enable to observe the causal process (Collier 2011**).** It is a tool enabling to take diagnostic evidence and through intensive static description and analyses draw descriptive causal inference for which it is very important not specifically focus on change itself but on series of specific moments (ibid**).**As defined by Collier "Process tracing is a fundamental tool of qualitative analyses" (Collier 2011: 1). It is invoked to carry out "within case analysis based on qualitative data" (ibid). Process tracing as described by George and Bennett "attempts to identify the intervening causal process, the causal chain and the causal mechanism between an independent variable and the outcome of the dependent variable" (George and Bennett 2005: 206). The definition of process tracing by Bennett and Checkel is "process tracing is analyses of evidence on processes, sequences and conjectures of events within a case for the purposes of either developing or testing a hypothesis about causal mechanisms that might

causally explain the case" (Bennett and Checkel 2015: 7). Blatter and Haverland suggest, that there is only one "overarching methodological principle that should guide the selection of cases if the major technique of drawing causal and descriptive inferences is processed tracing: accessibility" (Blatter and Haverland 2012: 102). They also point two potential dangers for researchers to be avoided that are "getting lost in the myriad of details that real case exhibits and lose focus conceptually and theoretically relevant factors" and "getting affiliated with investigated actors" (ibid: 102).

When applying process tracing it is necessary to distinguish between diagnostic evidence that is a type of evidence indicating the process is taking place and the real evidence that shows transmitting power of causal mechanism within evolving process (Bennett and Checkel 2015). One of the methodological problems with mechanisms is their nature which some scholars believe to be probabilistic (Hedström and Ylikovsky 2010:51) while others consider it sufficient in specific circumstances (Mahoney 2001:51). The core of the problem according to Bennett and Checkel is that "even if the world is deterministic we observe it as probabilistic because of measurement error and specification error" (Bennett and Checkel 2015: 12). Given the fact that mechanisms are operationalized in a specific case, applying process tracing in within cases study can be problematic in terms of generalizability until it looks like from the beginning to confirm the hypothesis or it explains "though test case" (ibid 2015:13). In terms of validity, CPT as a method fits purposes of this study because it serves much better for narrow specifications for within case study. While the potential weakness of CPT for wider generalization is compatible with the design and the aim of this research, it is not correct to think that cases explored using CPT provide 'one-dimensional thinking'. By conceptualization of direction, CPT can draw conclusion towards wider generalization for similar instances in other cases that can be superior to ones done by using the other methods (Blume and Blatter 2008).

In process tracing it is very important to not overlook "normative or material structural context" but also focus on "exploring what individuals knew when and how they behaved" (Bennett and Checkel 2015: 23). At the same time, however, it is critically important to consider the interpretation of actions and motives of individuals in instances when the evidence is probabilistic.

As Blatter and Haverland put it all case studies that are done by applying CPT as a method "are grounded in configurational thinking and use the fact that causation plays out in time and space as a 'natural basis' for drawing causal inferences" (Blatter and Haverland 2012: 87). They differentiate two types of configurational thinking which are the causal conjunction and the causal chain. They define causal conjunction as "causal configuration in which multiple causal conditions work together (in additive or interactive way) at a specific point of time or over a short period of time to produce the outcome of interest" (ibid: 94). Causal chain is "a causal configuration in which specific causal conditions form the necessary and (usually together with other conditions) sufficient preconditions for triggering other necessary and sufficient causal conditions or configurations at later point in time, and this causal chain leads at the end of the process to the outcome of interest" (ibid). Due to the nature of materials available and the absence of the possibility to observe all entities and conditions when events took place and I will focus on causal chain prioritizing it over causal conjunctions. When tracing a process, the sequence of events can be distributed by single events following one another each of which is closely bound to next one by causal links (Bennett and Elman 2006). According to Mahoney "each event in the sequence is both a reaction to antecedent events and a cause of subsequent events" (Mahoney 2006: 526-527). The path that the events form from A to B as X leading to Y might possibly require two different conditions. First, the first event such as possession of sufficient surveillance capacity and application in this case as the first step is enough to cause the chain of events leading to Y. Second, to have the Y we need more than the first event and possibly n amount of them for Y to occur (Bennett and Elman 2006). X might not be the primary cause of Y but rather sufficient but not necessary part of the set of factors causing the Y which requires totality of those factors to appear (Goertz and Levy 2007).

In terms of sufficiency and necessity of events for Y to occur the events for every single case have a unique sequence as well. It is important to uncover attributes determining the status of events by their meaning of necessary, sufficient or necessary and sufficient to understand the process. Usually in process tracing of within case study the X causal variable of interest does not directly lead Y outcome of interest but rather mediates that can be illustrated with X_1->X_2-X_3->X_4->Y chain as an example (Gerring 2007). Blatter and Haverland define necessary condition as "A causal factor (X) is a necessary condition if the outcome (Y) occurs only if X exists" (Blatter and Haverland 2012: 92) Sufficient condition is defined as "A causal factor (X) is a

sufficient condition if the outcome (Y) always occurs when X exists" (ibid). Sufficient conditions in the beginning of the chain are more important than necessary ones the role of which in its case is dependent which part of the chain it occupies (Goertz and Levy 2007). Turning points in causal chain are the ones where it could easily "move to another path" (ibid). As Beach and Pedersen state however sometimes "mechanisms linking causes and outcomes do not logically have to be sufficient or necessary to produce Y" (Beach and Pedersen 2016).The occurrence of critically important events within the chain of events can be tied to important key individuals and their decision making or larger structural or historical forces (ibid).

According to Beach and Pedersen process tracing can receive three forms by its purpose of the application. The first form is theory testing process tracing aiming to explain whether the causal mechanism is present and functions as theorized and the second is theory building process tracing aiming to explain what is the causal mechanism between X and Y (Beach and Pedersen 2013: 12). Those two types are labeled as theory-centric process tracing. The third type is outcome explaining process tracing the purpose of which is to show what mechanismic explanation accounts for an outcome. This type is branded as case-centric process tracing (ibid). This study is a contribution to theory testing by studying the influence of US mass security surveillance programs on political order and governance to see whether the causal mechanisms led to the outcomes as theorized.

To understand the process well, I will also examine the statements of representatives of executive branch including to the very top to President of the United States, of intelligence officers and whistleblowers to compare them with documents uncovered before and after the statements allowing following evolving process. Within discourse and narratives, it is possible to read the underlines revealing unstated truths by comparing the dynamic of rhetoric and events causing them. For materials of this nature, I use CDA (critical discourse analyses). Discourse analyses are a tool aiming the meaning and using discourse analyses means being interested in forms as conveyers of meaning (Trappes-Lomax 2008). Different types of CDA can vary theoretically and analytically so far as there is no unitary theoretical framework and therefore different approaches can be applied when analyzing texts, speeches etc. (Van Dijk 2001). The definition of discourse analyses by Trappes-Lomax is "the study of language viewed communicatively and/or communication viewed linguistically" (Trappes-Lomax 2008: 134).

More detailed definitions as he notices himself “involve reference to concepts of language in use, the language above and beyond the sentence" language as meaning in interaction, and language in situational and cultural context” (ibid: 134). CDA is the best fitting type for addressing part of materials for this study allowing explaining the use of language in power and politics of discourse (ibid) because of its distinguishing pattern which is that CDA is aiming uncovering “hidden effect of power...concerns itself with issues of identity, dominance and resistance” (ibid: 139-140). CDA is “specifically interested in power abuse that is in branches of law, rules and principles of democracy, equality and justice by those who wield power” (Van Dijk 1993: 255).

Politics of Surveillance in the U.S.

After 9/11 the large-scale terrorist threat has stopped being hypothetical and became very concrete and visible. The measures to counter repetition of similar occurrences went far beyond from politics of normal as a reaction and outcome of unprecedented securitization in the face of as many argue potentially existential threat. The legal and technological tools with which Intelligence and law enforcement were equipped to engage in intelligence gathering conducts went beyond 'the normal' as they enabled such operations without judicial permission, based not only on probable cause but solely on relevance (USA PATRIOT ACT, Sect. 215). The entitlement to personal privacy is an important component in American political culture in terms of the social contract (Stevens 2003, Bloss 2007). The post 9/11 security environment, shaped by international terrorism and development of surveillance technology among other factors, has influenced the evolution of political thought and public opinion on this among other issues. The new post 9/11 doctrine of the executive of conducting and keeping its covert invasive mass surveillance programs in secrecy even from legislative, the observed disproportionate public reaction to the existence of secret mass surveillance programs and extended efforts of US security apparatus are some of symptoms and part of this process.

The tendency of misuse of powers by intelligence agencies has not been a new phenomenon in the US and in general. Yet in report of Senate Select Committee investigation on activities of intelligence agencies in US, published in 1976 leading also to FISA, it was concluded, that in all aspects of their operations intelligence agencies showed general tendency and institutional inclination of increasing their reach and power by expanding beyond their initial scope (Senate Select Committee on Intelligence 1976). Some of the conditions contributing and enabling this tendency listed in the report of 1976 were the absence of legislation on intelligence that would mandate the role of legislative in balances and checks in this area of state activity, the institutional inclination and efforts of intelligence agencies to bypass existing checks, the locking of the covert operations within intelligence community and in many cases leavingthem underreported or unreported even to executive branch itself (Senate Select Committee on Intelligence 1976 report). Within intelligence community secrecy from legislative and other institutions and especially from public are 'operative norm' (ibid). In post 9/11 period similar patterns can be identified in multiple cases when the national security oriented concept of

governance appears to be prioritized as the vital enabler of the functionality of other components of state and society. An important reason for this is that the resonance of 9/11 has been of such a magnitude that in the post 9/11 period security has unquestionably become the top priority of US government and the fear the primary motif of actions (Lyon 2003).

There is a well-expressed consensus in the US government and the public in general, that the US should be made more secure from terrorist attacks and therefore there is a necessity of greater intelligence capacity. As it was concluded that one of the reasons of failure to prevent 9/11 has been the failure toset the right priorities by executive andthe lack of information sharing among intelligence agencies (9/11 Commission Report), the US PATRIOT ACT enabled intensification of information sharing both in horizontal and vertical dimensions of intelligence and law enforcement structures (Kreimer 2004). It is necessary to highlight, that the responsibility of the US government's executive branch (which is the part of government interested in the secrecy of information and under which those institutions function) in failure to prevent 9/11must be viewed within totality of circumstances that includes other actors playing role in policymaking process (Rogerson and Milton 2013).

Many professionals of intelligence and security in the US and scholars believe, that international terrorism and organized crime that operate "in a technologically fluid global environment" (Bloss 2007: 209) consequently create a necessity driven tendency of continually developing, strengthening and deploying more efficient surveillance tools to ensure US national security. Surveillance technology has been described many times as vital security enabler both by scholars (Lyon 2003, Ceyhan 2006) and importantly also practitioners including former head of Federal Bureau of Investigation James Comey and head of National Security Agency Admiral Michael S. Rogers who very recently described those programs as "critical, indispensable, vital"[3] to U.S. national security.In an environment where the boundaries between internal and external threats are inseparable many times, such as in the case of terrorism, the new strategic approach of major US intelligence and security agencies such as National Security Agency (NSA), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Defense Intelligence Agency (DIA) etc. is better interlinking the efforts to detect and monitor potential sources of threat or

[3]20/03/2017 testimony of heads of FBI and NSA before Senate Intelligence Committee on alleged Russian interference in 2017 US presidential elections

subjects of interest to secure and prevent them from producing violence. One of the outcomes of strengthened cooperation among intelligence and security agencies is disclosure of information on persons of interest which compromise their personal data to a greater audience and is an object for examination for purposes not applicable before. In recent decades in general two parallel processes of ‘compromise' of rights of citizens to powers of government in the US has been happening. The first is the ‘transformation of the privacy framework' or the process of changes in legal norms in favor of more surveillance and decreased rights of citizens to privacy (Bloss 2007). The second is the technological advance that enabled intelligence agencies to implement their missions in ways that overcome operating legal entitlements. A very important component in this process is that the compromise of identity through technology is eliminating the knowledge, willingly participation and the consent of targets.

However political, the secret surveillance programs such as NSA programs revealed by Snowden are hard to bring to judgments of the court and moreover to give the public opportunity of insight. Access is denied, details remain secret based on the argument of putting the national security at stake which is in the interest of none except that of enemies and this retreats no counterargument (Richards 2013). As Richards correctly notices, the laws restricting surveillance legally mean nothing in case of secret programs of government as such laws pose challenge only when those programs are exposed (ibid). In several legal cases where private entities went to court against secret surveillance programs, the legal conclusions have been that except if reasonable evidence is presented from accuser, such as that their privacy has been targeted or that there has been any “legally cognizable injury” caused by government actions, the decision has been in favor of government (Richards 2013: 1943).

The role and the Relations of U.S. Government Executive and Legislative Branches from Perspective of Government Surveillance

In his September 20th 2001 speech addressing joint session of Congress President Bush promised, that his administration "will direct every resource at our command, every means of diplomacy, every tool of intelligence, every tool of law enforcement, every tool of financial influence and every tool of war to the destruction and the defeat of the global terrorist network"[4]. By replacing probable cause with reasonable suspicion and relevance in the USA PATRIOT Act, the administration has set lower legal standards for authorization of conducting surveillance for intelligence gathering purposes (Bloss 2007). In addition, to make the procedure of dealing with terror and terrorists, under post 9/11 'New Paradigm', George W. Bush authorized a system of detention and interrogation that arguably"operated outside the international standard for the treatment of the prisoners of war established by 1949 Geneva Conventions" (Mayer 2006).

Because international terrorism has no borders and operatives of radical terrorist organizations and their allies operate also within the US, exempting US persons from surveillance practically would have been an unjustified risk potent to destabilize the state structures if similar events were plotted and executed within the US again. At the same time, the powers of the executive for this kind of decision making are disputed fiercely by lawmakers and public. While the President can be granted "tremendous discretion" by the legislative branch, it is clear, that practically checking abuses of power in the domain of intelligence remains unbalanced and non-efficient mechanism (Kitrosser 2007: 6-7). Despite legal tensions and large opposition of public opinion, the Bush administration believed, that the issues of privacy and transparency are subject of being "outweighed by critical public interest" (white paper on sec. 215: 19) such as national security. This view has been highlighted again in 2006 DoJ paper on Presidents authorization of NSA to intercept communications where the legitimacy is build first of all by rooting the lawfulness of such actions within "defense of the nation" as total priority (DoJ 2006: 1). Only after, the document makes reference to the President's statutory powers rooted in the constitution to "conduct warrantless surveillance for intelligence purposes to detect and disrupt armed attacks

[4] http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html

on the United States" (DoJ 2006: 1). As would characterize the US Republican Congressman Bruce Fein[5] referring actions of Bush administration within new legal doctrine “he (George W. Bush) claims that there are no restraints on his ability, as he sees it, to collect intelligence, to open mail, to commit torture, and to use electronic surveillance" (Mayer 2006). The necessity driven ‘special policies for special times' doctrine employed by the government in post 9/11 period has been attempted to be accommodated within ‘executions with good faith' (white paper on section 215) narrative excluding the notion of misuse of power against US citizens. The public consented to grant the government special powers to protect them against the foreign enemies but found itself under surveillance which as Tom Daschle[6] put it after it was revealed that the government is conducting secret mass surveillance also within the US, has been "the power we did not grant" (Daschle 2005).

DoJ claims that when it comes to Presidents statutory authority of authorizing NSA mass surveillance program, the reference should not be made to FISA, because there may be "ambiguity" issue, but rather it should be read "in harmony" with Presidents Authority of Use of Military Force Against Terrorism (DoJ 2006: 3). Otherwise, as DoJ claims, the constitutionality of FISA itself is subject to being questioned (ibid).

The concept of special powers derived from necessity in special times, which has been the “defense of the nation” in this case, has been argued many times to be interpreted in certain ways in post 9/11 period to legitimize abuse of power by conduct of secretive mass surveillance that does not fit within "micro secrecy" within "macro-transparency" model mandated by the US constitution (Kitrosser 2007: 3). It has created an imbalance between branches of government. The general meaning of balance in the constitution is the creation of symmetry between "liberty enhancing features" of the legislative branch and "energy and efficiency-enhancing" power of executive (ibid: 5). Certain patterns of organizational structure of legislative and powers embodied in this institution aim the prevention of the erosion of enablers of liberties by preventing ill-judged and/or secretive conducts of the executive (Vermuele 2005). The powers embodied in the institution of the US president are interpreted as enablers of protection of country through efficiency and capacity of timely action in times of necessity (Kitrosser 2007:

[5] Bruce Fein is a US Constitutional Attorney, Deputy Attorney General from 1981-82 Under Reagan Administration
[6] Tom Daschle is former US Senator, Senate Majority Leader from Democratic Party in 2001-02

6). The structural relations of legislative and executive as described by Kitrosser comes down to balancing "the need of wisdom and liberty against the needs of energy and efficiency", and while transparency is a main feature in the first, it is the secrecy that is in the design of the second (2007:11-12). The nature of executive branch, that is the only one "structurally equipped to respond to immediate unanticipated threats" (, US Constitution Article II, §§ 1-3, Kitrosser 2007) leads to its entitlement to possess the capacity for special circumstances where administration selects and employs specific tools and means. In emergencies, the executive branch is ‘abled' to surpass legislative and judicial procedures to act timely in the name of national security because of limited time to operate (Kitrosser 2007). As mandated by FISA however, it is the legal obligation of DNA, heads of US intelligence agencies and the President to keep congressional intelligence committees informed on intelligence activities currently, except the times when the president can use his statutory power to restrict or limit prior communication of information (Cumming 2006).

The advantage of ‘single-handed' presidential system has been proven by history to be "the President's ability to operate in secret" (Kitrosser 2007: 13). It is the checks and balances embodied in the legislative branch that is there to balance the power, to prevent the use of that power against the people of the country (ibid). Presidential powers were described as to be in three different zones by Justice Jackson in Youngstown Sheet & Tube Co. v. Sawyer case (343 U.S.: 579). In the first zone, the legitimacy of presidential power is the most powerful because "the President acts pursuant to an express or implied authorization of Congress" (Ibid: 635). I second zone the President can go beyond statutory authority broadening the reach of presidential power still having that statutory authority as a basis for judgment behind actions (Ibid). In third zone actions of the president might be "inherent and trump contrary statutory authority" (ibid). The actions of US president when authorizing secret mass surveillance programs were implemented through powers described as the third zone (Kitrosser 2007). One of the most important conclusions in 1976 Senate Intelligence Committee report has been that its secrecy that provides with conditions and leads to abuse.

Surveillance in Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

After 9/11 terrorist attacks, the determination of Bush Administration has been that deployed tools fail to provide with efficiency in securing the nation and therefore new superior legal and technological tools are necessary to combat threats of Terror. The USA PATRIOT ACT has been one of the first legal tools that executive was equipped with, enabling the designing and deployment of new strategic and technological tools and means for securing the nation. It has also become the most important for this period normative legal document for intelligence community defining their mandate within the new legal framework. The USA PATRIOT ACT was signed by President George W. Bush becoming effective on 26th of October 2001. In the Act, under title II from page seven Congress addresses "Enhanced Surveillance Procedures" directed at the interception of "wire, oral and electronic communications relating to terrorism" (USA PATRIOT ACT: 7).

International terrorism by nature and strategy differs dramatically from traditional for state threats. Terrorist operatives deploy different tactical approach, motif, and objective. Consequently, the strategy of institutions fighting terror has becomeadaptive to enable efficiency. In short period after 9/11 those institutions begun prioritizing and shifting to pre-emptive and preventive strategies through surveillance and technology (Bloss 2007, White 2006). This process has been rooted in mentioned above altered legal doctrine in part of surveillance authority and seizure aiming to deter terrorist activities (Bloss 2007). The US government ruled out, that in the war on terror the strategic component of targeting and intercepting terrorist communications as a vulnerability is an absolute necessity and priority (administrative white paper on section 215 of USA PATRIOT ACT). The US Electronic Communication and Privacy Act of 1986 has also been passed through Congress taking new shapes under environment created by USA PATRIOT ACT providing law enforcement with right to "intercept electronic communications without a warrant or court order if they obtain the consent of one of the communication participants or an exigency[7] exists" (Bloss 2007: 218). The process, however, took place in secrecy as the Bush administration claimed that national security

[7]Exigency is a legal term that describes an emergency circumstance that may compel to abandon standard search and seizure practices. Examples are imminent threats to personal safety, risk of destruction of evidence, or pursuit of an escaping suspect

demands top secrecy of surveillance programs which otherwise would be threatened of being stripped from its core attributes providing efficiency in their pursuit of security (Kitrosser 2007).

In defense of its the post 9/11 intelligence activities, the administration did not make the claim that all its actions were in accordance with FISA (ibid) but still claimedto have the legitimacy of its actions of intelligence gathering in the use of presidential power derived from necessity in crisis and emergency and for preventing them to defend the nation. Most importantly the discourse of administration attempted to represent the conducts as foreign intelligence gathering. The PATRIOT ACT refers ‘foreign intelligence information' gathering aiming to protect the nation as one of the core functions of state security apparatus by definition. Foreign intelligence information in the ACT is defined as "information, whether or not concerning a United States person, that relates to the ability of the United States to protect against-..." threats that "...relates to national defense or the security of the United States" or its "conduct of the foreign affairs" (USA PATRIOT ACT: 10). From the legal perspective, these formulations are elastic and relatively open to interpretations within contexts and provided intelligence agencies with a large area for employing operational tools with ease, having restrictions and checks rather as symbolic attributes underprioritized by necessities of national security. In the USA PATRIOT ACT and in post 9/11 legal documents that relate to surveillance activities of Intelligence agencies the legitimacy of conducts and practices, in general and primarily, can be found to be built first of all over protection from international terrorism (USA PATRIOT ACT of 2001, Administrative White Paper on Section 2015 of PATRIOT ACT, FASC Memorandum of Law 2015 etc.).

DARPA's Total Information Awareness Program

9/11 attacks exposed the US government and intelligence community "inadequacies of its information gathering techniques, its information technology, and its information holding" (Stevens 2003: 1). Alongside with adopting legal tools, to acquire adequacy also in terms of technological capacity, the US government authorized Total Information Awareness program as a prototypical system of surveillance among other components pursuing data search and pattern recognition through data mining techniques. Total Information Awareness program intended to conduct "mass surveillance without warrants for the purposes of identifying potential terrorists through data mining for pattern matches" (Monohan in Lyon Ball and Haggerty 2012: 287).

The program was developed by Defense Advanced Research Project Agency (DARPA) of Department of Defense to "analyze, detect, classify and identify foreign terrorist" (Stevens 2003: 2). The TIA as described by DARPA focused on data mining from new data sources including "transactional data from communications, financial, education, travel, medical veterinary, country entry, place/event entry, transportation, housing, critical resources and government" (TAPAC 2004: 15). TIA was aiming to create virtually all possible planning types of terrorist threat, actions, and transactions that would possibly follow such kind of planning and set a framework for pattern recognition that would track matching patterns in databases also in real time (TAPAC 2004). The program however created controversies as it was clear that its core function and the mission was indiscriminate surveillance and profiling.

In different occasions, the US Congress has addressed the gathering and the use of personal information as government practice. The Privacy Act of 1974 was meant to limit the power of the government from disclosure and misuse of personally identifiable data (TAPAC 2004). Leaked information and interviews with whistleblower intelligence insiders show that the executive did challenge the boundaries of the legal framework (The Washington Post 2005, Risen 2006). While even approved legal norms and practices were subject to debates and controversies themselves, it came out that the real conducts went far beyond thecontroversial framework set by normative legal documents. Many of intelligence gathering practices of state in this process were contested as unconstitutional and criticized as an abuse of power.

One of the reasons why these activities and their legal backing has been contested as unconstitutional has been the fact, that indiscriminate and/or unauthorized gathering, storing, disseminating of aggregate data on persons through technology and its use poses a great risk of social control in a free society (TAPAC 2004) and creates dilemmas. From one hand in the face of threats, people demand the state to build capable security apparatus to secure the nation. At the same time, people are concerned with their privacy and do not want to compromise everything to be included in an aggregate profile regardless whether if it would label them positive or negative. On the other hand, there is the counterargument of TAPAC called ‘false positive'. This is the danger of being subject to negative discrimination because of incomplete data when aggregate profiles failed to include the data that would have a positive impact on owner's profile preventing negative outcomes. Because of largely negative public opinion on the program, the government renamed the program from Total Information Awareness to Terrorist Information Awareness. However, this rather symbolic step did not change the nature of project given the fact that the objective of the program that was invention and development of technology that can "automatically extract evidence about the relationship among people, organizations, places, and things..." has not changed (DARPA 2003: 7). DARPA assessed that there is significant potential for efficiency through the cooperation of agencies included in the experiment (DARPA 2003). Those nine agencies were U.S. Army Intelligence and Security Command (INSCOM), National Security Agency (NSA), Defence Intelligence Agency (DIA JITF-CT), Central Intelligence Agency (CIA), DoD's Counterintelligence Field Activity (CIFA), U.S. Strategic Command (STRATCOM), Special Operations Command (SOCOM), Joint Forces Command (JFCOM) and Joint Warfare Analyses Center (JWAC).

In 2003 amid to clash of needs of Intelligence Community and the concerns on civil liberties from Congress and the public, Secretary of Defense at that time Donald Rumsfeld Initiated investigation on the impact of the use of advanced information and surveillance technologies for intelligence and security purposes in the war on terror. The mission was assigned to already mentioned Technology and Privacy Advisory Committee (TAPAC). The central component targeted by this investigation has beenfirst of all exactly the Total Information Awareness program of DARPA (Defense Advanced Research Projects Agency) and also the data mining practices by security and intelligence agencies (TAPAC 2004). The committee identified data mining and profiling as a vital tool in the fight against terror. TAPAC also concluded that there

are many programs with the same logic and aim as TIA conducted by different agencies and that TIA has been asmall part of the realization of the concept it was part of (2004). Another conclusion has been that it is essential to establish a new legal framework by creating comprehensive "system of laws and technological measures to facilitate data mining and information sharing" given the "urgent need to enhance information sharing among agencies concerned intelligence gathering, national security and law enforcement" (TAPAC 2004: 6). This conclusion can be interpreted as an admission, that the present practices of security and intelligence agencies in the technology-enabled environment and within ‘surveillance industrial complex' is no longer possible to facilitate within existing legal normative framework that served as abase for directives in process of conduct and in the processing of the outcomes of conducts.

One aspect that was vital in conclusion was that the use of technology for security purposes can be done without compromising US citizen's identifiable data. This contradicts the view of scholars insisting that when there is an exclusive aggregate profile of a person, the name or identity plays no meaningful role in the determination of treatment (Lyon 2003). According to TAPAC however the answer as they put "lies in clear rules and policy guidance, adopted through open and credible political process, supplemented with education and technological tools, developed as an integral part of the technologies that threaten privacy, and enforced through appropriate managerial, political and judicial oversight" (TAPAC 2004: 8). This hypothetical possibility, however, does not necessarily go sound with basic operative norms of intelligence agencies that following such long chain of events and persons would create great vulnerability of compromising and exposing themselves losing their most valuable attribute, the secrecy, and so becoming rather a law enforcement agency alike institution.

The persistence of Intelligence Community of not addressing domestic terrorist threats differently from that international in areas they do not differ is clear and reasonable. It would simply lead organizations involved in international terrorism to shift their strategic thinking and to operate where they are less vulnerable and detectable and can exploit vulnerabilities better. Consequently, the narrative that the legal framework on domestic surveillance should be guiding priorities of intelligence agencies has a strong political component in it opposed to the strategic logic of intelligence agencies. From the security perspective, it is not something empowering Intelligence Community in the war on terror.

Given TIA-s controversial nature, tensions with the law and civil opposition, the funding of the program have been stopped by Congress in 2003. As concluded in the report, the eliminating TIA and TIO (The office developing the program), but granting permission for continuation of four other projects of TIO for developing "processing, analyses and collaboration tools for counterterrorism foreign intelligence" as specified in classified annex of decision, was a green light for continuing further development of TIA under different labels (TAPAC 2004: 1-2). The pursuit of centralized databases is central to data mining efficiency. Throughout this process the executive learned that political transparency in the war on terror is not an ally, secrecy is. Exposure of its strategic planning and development of tools and techniques considered necessary for national security were blocked by public opinion and legislative branch. Thishas been one of the most influential points in a time when the administration and the Intelligence Community decided that secrecy of secrets as a necessary organizational operative norm has to be strengthened further rather than to be compromised.

2005 Leaks on US Governments Secret Mass Surveillance Programs

In 2005 the first information on NSA secret surveillance program has become public making huge resonance in the US. The central controversial component of mass surveillance program has been the data collection on the US citizens and warrantless wiretapping of communications made from or to US (Risen 2006: 43-44, Mayer 2006). The authorization of secret surveillance program by the administration has been made yet in 2002 (Basen and Elsea 2006). The authorization has been criticized as a violation of FISA (Kitrosser 2007). Bush administration, however, argued, that the creation of the program and its secrecy are justified by national security necessity. According to Bush administration the conducts in this particular case could not and should not be accommodated in originalist interpretation of constitution[8] and rather the laws should be interpreted as living and evolving within contexts of time providing legal framework not only for authorization of program but also for secrecy of its existence (Kitrosser 2007: 2, Schoenfeld 2006). Despite being widely challenged by different organizations, law-makers and a large part of the public, there has not been cases of convictions related to the secret programs.The case demonstrated, that despite controversial activities, in terms of national security-related conducts the executive remains largely immune to accountability.

[8] The form of interpretation of constitution where the laws are applied in a fashion believed to be what founding fathers had in mind

Bulk Collection of Data and 2007 Secret FISC Orders

The administrative white paper on bulk collection of telephony metadata first authorized in 2006 under section 215 of USA PATRIOT ACT indicated that the main purpose of the collection of bulk data is the prevention of terrorist threat (2013). The Program has been constantly prolonged under orders of Foreign Intelligence Surveillance Court judges the existence of which has been unknown to the public at that time. According to Bush administration, only phone numbers which were connected, the duration and the time of connections were recorded excluding the content and the scripts (Ibid). This has been challenged by Edward Snowden multiple times on different occasions. The view of the executive in this document is that reasonable belief in connection of companies and entities to international terrorism based on relevant information is a legitimate legal basis for a court order authorizing bulk data collection. Section 215 of USA PATRIOT ACT is formulated with belief, that the government will not know about the existence of materials relevant for deterring terrorism and other threats to national security (white paper on sec. 215: 12). Under section 215 Congress did not limit FBI to obtain a warrant only for data collection in "relevant to an authorized investigation" but they recognized that it is a necessity to collect records for data mining purposes to identify threats that were unknown before the collection (white paper on sec. 215: 12). During investigations, the scope and the width of it can go far beyond single authorized action. Operations are potent and prone to include much larger environment and entities within. One authorization of surveillance of single phone number can lead to surveillance of several others as "contacts of interest" believed to provide with potential intelligence (white paper on sec. 215: 4).

The information on secret FISC orders on interception of US domestic communications by NSA has become public only in 2013 when Edward Snowden leaked classified documents on secret surveillance programs of US government. After secret FISA courts authorized NSA surveillance program "overwhelmingly directed at non-U.S. persons" it also gave government "reasonable amount of time" (FISC 3 April 2007 order: 1) for filing revised version that would meet requirements of 1976 FISA act. This is one more fact revealing how the necessity enabled the government to bypass legal requirements for usual times. Formulations such as ‘reasonable amount of time' and ‘overwhelmingly directed at non-U.S. persons' are open to interpretations within contexts. Moreover, the executive initiated ‘new legal theory' under which connections

discovered during authorized surveillance conduct would be surveilled and only then reported to the court (Vinson's FISA court order of May 2007). The May 2007 order signed by Judge Vinson detailing the evidence for probable cause legitimizing the authorization of conduct remains classified. The circumstances that would let surveillance of related electronic communication numbers and addresses also remain classified for public access. The order itself is declassified partly only. The word ‘foreign powers' mentioned many times in order supports the narrative that the government is fighting outside threats. The US citizens appearing under the radar by circumstances are ‘masked' in reports remaining anonymous under thelabel ‘US person' and the number attached to that to distinguish if there are more than one (Senate Intelligence Committee testimony of heads of NSA and FBI on Russian Interference in 2017 US elections).

The longlisted definitions in 1978 FISA of what characterizes an entity as a foreign power (and representative of a foreign power), leaves no doubt that its mandate is capable reaching nearly everyone within the US would any reasonable suspicions arise. As it was exposed by Edward Snowden, the transfer of files through not US-based servers would qualify them as foreign communication and therefore a legitimate target for interception. FISA Amendment Act of 2008 equipped the government with authority to initiate and conduct investigation and surveillance activities without presenting probable cause when the target is falling under category of foreign intelligence source while the 2007 FISC order also enables government not to report employment of electronic surveillance that has been conducted during effective period of order even if the operation has not been authorized. Still, theorder specifies that procedures of conduct on US persons should "meet the requirements of these procedures and the Foreign Intelligence Surveillance Act" (NSA FISA court order of May 2007: 25).

Snowden and After

In 2013 a private contractor working for NSA at that time Edward Snowden has leaked unprecedented number of classified documents on secretive mass surveillance programs and projects of the US government. Those documents that were handed to journalists and published mainly through WikiLeaks, exposed number of secret surveillance program code names such as Prism, Tempora, Xkeyscore, Verizon Court Order, Boundless Informant, Bullrun and Edgehill etc. including the specific mission of each program. Those programs were aiming to provide the government with actionable intelligence through a variety of procedures including recording and storing phone calls, mining data from servers of communication and tech companies, intercepting electronic communications, braking encryptions etc. (Hayes 2014). Those programs were authorized to access and mine data from servers of companies such Google, Facebook, Microsoft, Yahoo, Apple, Youtube, Skype etc. which daily process data and communications of billions of people. For data mining naturally complex and large input of data is a necessary component of analytical success.

Before Congress would reauthorize section 215 in February 2010, the members were provided with a written briefing on surveillance programs. The fact, that the re-authorization of section 215 has not been seriously challenged in 2011 and latest in 2015 extending its power till 2019 is evidence, that it is producing positive outcomes in process of securing the US against the terrorist threat. In 2015, for example, it has been revealed that FISC has denied none of 1457 surveillance requests from FBI and NSA (FISC Memorandum of Law 2015).

Constant controversies caused by secret mass surveillance programs after they were relieved led US President Barack Obama to ordered detailed investigation to review the meaning and the impact of intelligence and communication technologies. The task has been assigned to the Presidents Review Group on Intelligence and Communication Technologies (the review group afterward). In Report and Recommendations of the Presidents Review Group on Intelligence and Communication Technologies: Liberty and Security in Changing World, the US government recognizes the necessity of protecting two forms of security in its pursuit of security through surveillance, national security and personal privacy (2013). In their report the review group states that the narrative of balance between security and liberty "contains elements of truth" but it

is "also inadequate and misleading" because there are "safeguards of liberty that cannot be and should not be subject to balancing" (The Presidents Review Group report 2013: 16).

Among other recommendations the review group suggests transferring bulk-metadata to private party who would store it and government could access only for national security purposes preventing possible misuse, to restrict the ability of FISA to compel private companies to disclose any information qualifying such cases as "creating potential risks to public trust, personal privacy and civil liberty" (The Presidents Review Group report 2013: 17). Under careful formulations the report points that the conducts and the rules of conduct are very problematic and should not be allowed to function further without setting new standards if a possibility of doing so emerges.

One of the vital components casing controversies in the evolving process has been thatthe section 215 of US PATRIOT ACT demolished the limitations on what kind of entities are compelled to produce records by government request authorized by FISC and it also changed the procedure of producing such an order by FISC (The Presidents Review Group report 2013). If before the government was obliged to show reasonable suspicion based on facts to request such orders, after section 215 became effective, the FISC could authorize it simply based on governments belief, that the conduct aims (The Presidents Review Group report 2013) the "investigation to protect against international terrorism or clandestine intelligence activities" (USA PATRIOT ACT 2001, Sec. 215, 216). The US government defined the list of principles in USA FREEDOM Act of 2015 that aims to improve the situation. Those included principles such as minimization procedures determining the character of the case and follow up procedures including decision that the call records that are determined not to fall under category of foreign intelligence should be destroyed (p. 3), that even in emergencies there is clearly defined path of steps of conduct to keep the insight etc. These principles aim to minimize the pressures and the negative effects of security surveillance programs on US political structures. The Act tried to roll back the effects of 9/11 to create more transparency in decision-making processes.

After many efforts and attempts of creating regulations and guidelines to accommodate security surveillance within the design of the US political system and minimize its negative impact on some of the core principlesenabling the functioning of in the system, the government suffered yet another blowback in 2017. Just weeks after Trump administration entered the White House

WikiLeaks leaked 8761[9] new documents with thecodename ‘Vault7' on surveillance projects run under Obama administration. Those documents prove, that surveillance technology, strategy, tactics, application, and capacity of US Intelligence community has been developed further becoming more advanced and sophisticated. The new strategies and tools clearly aim not more transparency but enhanced secrecy. They pursue minimization of footprints to demolish possibility of tracking their application, self-destruction in time to stay undetected, and most importantly try to operate in a parallel secretive layer of governmental conducts aiming not compliance but avoidance from confrontation with legal norms rootedin definingand core principles of the design and the foundation of the U.S. political system.

[9] https://www.wsj.com/articles/fbi-is-probing-how-wikileaks-obtained-cia-spy-tools-1489008546

Conclusions

Different types of surveillance can produce different outcomes in similar environments. Conclusions based on this research address specifically the impacts of US government's security surveillance and profiling practices in the United States in post 9/11 period. Security surveillance and profiling in the war on terror possesses different from other types of surveillance attributes that are deterministic for outcomes it produces in terms of its influence on liberal political order.

A complex assessment of the meaning and the influence of US government security surveillance and profiling practices on US governance in post 9/11 period could only be made with full access to relevant materials. While the case of the US is unique in terms of materials enabling researching this field of state activity, only a very small portion of information is available for making a definitive evaluation.

Overall, throughout post 9/11 period surveillance and profiling practices remained covert practices and formally ended after being revealed to the public. Throughout this period such practices produced an abuse of power by the executive branch of the government as well as intelligence and security agencies. It further created tensions and conflicts with the law due to the incompatibility of constitutional rights of citizens with implemented surveillance programs.

Every US government mass surveillance program has been conducted covertly not only because it is a necessary attribute for efficiency in the War on Terror, but also because of due legal incompatibilities. The government of the US has not been able to accommodate such practices in the operating legal framework defining the political system despite a wider effort to legitimize such practices.

In observed instances, separately and altogether the Influence of these programs has led to the compromise of legal norms and a certain degree of erosion of political norms.

Repetition of mass surveillance and profiling programs one after another even after harming to public trust in government and legal system are a testimony to the fact that surveillance and profiling practices are "vital, necessary and indispensable"[10] for US National Security. Data

[10] 20.03.2017 congressional testimony of head of FBI J. Comey and head of NSA M. S. Rogers

mining and profiling is a vital tool in the fight against terror (TAPAC 2004) and therefore will continue to exist as a necessity.

In the observed instances, the strategy of balance has never worked because of certain attributes in the design of US political system, as Presidents Review Group on Intelligence and Communication Technologies concluded, are not subject to balancing. Certain attributes of security surveillance and profiling practices fighting international and domestic terrorism in the US are equally impossible to balance as inalienable components of the practices of this type. This means that to keep its security surveillance programs both alive and functional, the US government, security and intelligence agencies will have to continue treating those programs with alternative standards other than that established by operating legal norms.

Bibliography

1. Administration White Paper., Bulk Collection of Telephony Metadata Under Section 215 of USA PATRIOT ACT., 9 August 2013
2. Andrew Bennett, Colin Elman, Complex Causal Relations and Case Study Methods: The Example of Path Dependence., Political Analyses (2006) 14:250-267
3. Ball, K. Webster, F. (eds. 2004), The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age, London, Pluto Press
4. Bauman, Z. (2000), 'Social Issues of Law and Order', British Journal of Criminology, 40: 205-221
5. Bazen B. E. And Elsea K. J., Legislative Attorneys, American Law Division., Memorandum on Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information., Congressional Research Service, 5 January 2006
6. Beach Derek and Rasmus Brun Pedersen., Process tracing Methods: Foundation and Guidelines., University of Michigan 2013
7. Beach Derek, Rasmus Brun Pedersen., "Selecting Appropriate Cases When Tracing Causal Mechanisms." *Sociological Methods & Research* 2016, 45: 1-35.
8. Bennett Andrew and Checkel J. Jeffrey (Ed.)., Process Tracing: From Metaphor to Analytical Tool., Cambridge University Press 2015, pp. 3-38
9. Blatter Joachim, Blume Till., In Search of Co-variance, Causal Mechanisms or Congruence? Towards a Plural Understanding of Case Studies., Swiss Political Science Review (2008) 14(2): 315-56
10. Blatter Joachim, Haverland Markus., Designing Case Studies: Explanatory Approaches in Small-N Research., Palgrave Macmillan UK 2012
11. Bloss W., Escalating U.S. Police surveillance After 9/11: an Examination of Causes and Effects, Surveillance & Society 2007, Special Issue on 'Surveillance and Criminal Justice' Part 1, 4(3) 208-228
12. Bigo, D. and Tsoukala, A. (eds. 2008), Terror, Insecurity and Liberty, Illiberal practices of liberal regimes after 9/11. New York, Routledge
13. Bowker G. and Star S (1999), Sorting Things Out: Classification and Its Consequences, Cambridge MA, MIT Press

14. Ceyhan A. (2008), 'Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics', Surveillance and Society 5(2): 102-123
15. Cumming A., Statutory Procedures Under Which Congress Is To be Informed Of US Intelligence Activities, Including Covert Actions., Congress Research Service 2006
16. Colier D., Understanding Process Tracing., Political Science & Politics 2011, Vol. 44, Issue 4, pp. 823-830
17. Trappes-Lomax in Davies Alan and Elder Catherine (eds.)., The Handbook of Applied Linguistics., Chapter 5, Discourse Analyses., Blackwell 2004
18. DARPA Report to Congress regarding The Terrorism Information Awareness Program, 2003
19. Daschle T., Power We Did Not Grant, 23 December 2005, The Washington Post Electronic Publication (http://www.washingtonpost.com/wp-dyn/content/article/2005/12/22/AR2005122201101.html)
20. De Goede M., Beyond Risk: Premediation and the Post 9/11 Security Imagination, Security Dialogue 2008; 39; 155, Sage Publications
21. Deluze, G. (1992), 'Postscript on the Societies of Control', October, 59, MIT Press, Cambridge MA, pp 3-7
22. De Zwart M., Humphreys S. and Van Dissel B., Surveillance, Big Data and Democracy: Lessons for Australia from the UK and the US, UNSW Law Journal Vol. 37 (2), pp.713-747, 2014
23. Ericson, R. and Haggerty, K. (1997), Policing the Risk Society, Toronto., University of Toronto Press
24. Flaherty, D. (1989), Protecting Privacy in Surveillance Societies, Chapel Hill: University of North Carolina Press
25. Foucault, M. (1979), Discipline and Punish, New York: Vintage.
26. Gandy, O. (1989), 'The Surveillance Society: Information Technology and Bureaucratic Social Control', Journal of Communications, 39(3), pp. 61-76
27. Gerring John., Case study Research: Principles and Practices., Cambridge University Press 2007
28. George L. A. and Bennett A., Case Studies and Theory Development in Social Sciences., MIT Press 2005

29. Goertz Gary, Levy S. Jack. (Ed.)., Explaining War and Peace: Causal explanations, necessary conditions and case studies, Routledge 2007
30. Hayes B., State of Surveillance: The NSA Files and the Global Fightback., State of Power, TNI 2014
31. Kitrosser H., „Macro-Transparency“ as Structural Directive: A Look at the NSA Surveillance Controversy., Minnesota Law Review 2007
32. Lyon, D. (2001), Surveillance Society: Monitoring Everyday Life, Oxford: Open University Press
33. Lyon, D. (2003), Surveillance After 9/11, Cambridge: Polity Press
34. Lyon, D. (ed. 2003), Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, London and New York, Routledge
35. Lyon, D. (2004) 'Surveillance Technology and Surveillance Society', in T. Misa, P. Brey and A. Feenberg (eds) Modernity and Technology, Cambridge, MA: MIT Press, pp. 161-184
36. Lyon, D (ed. 2006), Theorizing Surveillance: The Panopticon and Beyond, Cullompton UK: Willan Publishing
37. Lyon D., Kristie B., Haggerty K. (eds) Routledge Handbook of Surveillance Studies, Routledge (2012)
38. Lyon, D. (2012), Introducing Surveillance Studies, Cambridge, Polity Press
39. Machamer Peter, Darden Lindley, Craver F. Carl., Thinking About Mechanisms., Philosophy of Science, Vol. 67 No. 1. (Mar. 2000) pp. 1-25
40. Mahoney J., Path Dependence in Historical Sociology., Theory and Society 29(4) August 2000., 507-5048
41. Mansell, R., Avgerou, C., Quah, D., Sylverstone, R. (eds. 2007), Oxford Handbook of Information and Communication Technologies., Oxford.
42. Marx, G. T. (1998), 'Ethics for the New Surveillance', The Information Society 14: 171-185
43. Marx, G. T. (1988), Undercover: Police Surveillance in America, Berkley CA: University of California Press
44. Monohan, T. (ed. 2008), Surveillance and Security: Technological Politics and Power in Everyday Life. New York and London: Routledge

45. Rose, N. (1996), Powers of Freedom, Cambridge UK: Cambridge University Press
46. Seawright Jason, Gerring John, Case selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options., Political Research Quarterly (2008) 61:2 294-308
47. Stalder, F. (2002), 'Privacy is not Antidote to Surveillance', Surveillance and Society, 1(1), pp. 120-124
48. Van Dijk A. Teun., The Handbook of Discourse Analyses, Chapter 18 `Critical Discourse analyses., 14 Jan. 2008 (the year and publisher)
49. Van Dijk A. Teun., Principles of Critical discourse analyses., Discourse & Society 1993., Sage vol. 4(2):249-283
50. Westin, A. (1967), Privacy and Freedom, New York: Athenaeum
51. Anderson P., Fighting 'Terrorism', Repressing Democracy: Surveillance and the Resistance in the UK., Legal Studies Research Paper No. 2016/1, University of Warwick
52. Bigo D. In Ball K., Haggerty K. And Lyon D. (eds)., Surveillance, Security and Intelligence., Routledge Handbook of Surveillance Studies., Routledge 2012
53. Bauman Z. & Lyon D., Liquid Surveillance, Polity Press 2013
54. Ball K. and Webster F. (ed.) (2003). Intesnification of surveillance. Crime, terrorism and warfare in the Information Age, London, Pluto Press
55. Ball K. Et. al (2009) "Memorandum by the Surveillance Studies Network" in HOUSE OF LORDS selected committee on the Constitution: Surveillance, Citizen and the State, HL paper 18-II, 2nd Report of Session 2008-2009, Volume II: Evidence, p. 22-25
56. Boyd D., Facebooks Privacy Trainwreck: Exposure, Invasion and Social Convergence (2008) Convergence: The International Journal into New Media Technologies 13, 18
57. Bloss W., Escalating US Polic Surveillance After 9/11: an Examination of Causes and effects., Surveillance & Society 2007, Special Issues on 'Surveillance and Criminal Justice' Part 1, 4(3): 208-223
58. Boghosian H., Spying on Democracy., City Lights., San Francisco 2013
59. Brakel V. R., Hert D. P., Policing, Surveillance and Law in a Pre-crime Society: Understanding the Consequences of Technology Based Practices., Cahires-Politestudies 2013., N20 p.163-192

60. Ceyhan Ayse., Technologization of Security., Management of Uncertainty and Risk in the Age of Biometrics., Surveillance & Society 2008 5(2): 102-123
61. Clarke R. (1993), Profiling: A Hidden Challenge to the Regulation of Data Surveillance. Published in the Journal of Law and Information Science 4(2) (December 1993)
62. De Zwart M., Humphreys S. and Van Dissel B., Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK., UNSW Law Journal Vol. 37(2), 2014
63. Fayyad U., Piatetsky-Shapiro G., Smyth P. (1996) From Data Mining to Knowledge. Discovery: an Overview, In Fayyad U, Piatetsky-Shapiro G, Smyth P, Uthurusamy R.(eds) Advances in Knowledge Discovery and Data Mining. AAAI Press / MIT Press, Cambridge
64. Ferraris V., Bosco. F, Caifero G., D'Angelo E., Suloyeva A., Defining Profiling ., Fundamental Rights and Citizenship Programme of the EU 2013
65. Fritsch L. (2008), Profiling and Location-Based Services (LBS), in Hildebrandt M., Gutwirth S. (Eds.), Profiling the European Citizens. Cross-Disciplinary Perspectives, Springer, pp. 147-168
66. Fuster G., Gutwirth S., Erika E. (June 2010), Profiling in the European Union: A high risk practice. INEX Policy Brief, no. 10
67. Gilbert N., Dilemmas of Privacy and Surveillance: Challenges of Technological Change., The Royal academy of Engineering 2007
68. Harris S., FBI is Probing How WikiLeaks obtained CIA Spy Tools, The Wall Street Journal, 8 March 2017 (https://www.wsj.com/articles/fbi-is-probing-how-wikileaks-obtained-cia-spy-tools-1489008546)
69. Heidi Kitrosser, *"Macro-Transparency" as Structural Directive: A Look at the NSA Surveillance Controversy*, 91 Minn. L. Rev. 1163 (2007)
70. House of Lords Select Committee on the Constitution., Second Report of Session 2008-09, Surveillance: Citizen and the State., February 2009
71. Kreimer S. F., Watching the Watchers: Surveillance, Transparency and Political Freedom in the War on Terror., Journal of Constitutional Law, 2004, Vol. 7:1, pp. 133-181
72. Lyon D. (ed)., Surveillance as Social Sorting: Privacy, risk and digital discrimination., Routledge 2003

73. Lyon D., Surveillance Studies: An Overview., Polity Press 2007
74. Lipschutz, R. (2000) *After Authority: War, Peace and Global Politics in the 21st Century,* Albany: State University of New York Press
75. Marx G., Reichman N. (1984), Routinizing the Discovery of Secrets: Computers as Informants, in American Behavioral Scientist, Vol. 27, no. 4, pp.423-452
76. Marx T. G., Undercover: Police Surveillance in America., University of California Press 1988
77. Marx G. T., Ethics of New Surveillance (1998)., The Information Society 2006, 14:3, 171-185
78. Mayer J., The Hidden Power: The Lgal Mind Behind the "White Hoses" War on Terror., New Yorker 3 July 2006
79. McDowell M. A., The Impact of Clapper vs. Amnesty International USA on the Doctrine of Fear Based Standing., Georgia Law Review 2014, Vol. 49:247
80. Monohan T., Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance. In Surveillance and Democracy., Edited by K. D. Haggerty and M. Samatas. New York: Routledge 2010, 91-110
81. Muir L., Transparent Fictions: Big Data, Information and Changing Mise-en-Scene of (Governemnt and) Surveillance., Surveillance & Society 13 (3/4): 354-369
82. Report and Recommendations of The Presidents Review Group on Intelligence and Communication Technologies, Security and Liberty in Changing World, 12 December 2013
83. Report of the Technology and Privacy Advisory Committee (Chairman of committee Newton N. M.), Safeguarding Privacy in the Fight Against Terrorism, March 2004
84. Ripstein A., Force and Freedom: Kants Legal and Political Philosophy., Harvard University Press 2009
85. Rogerson K. Milton D., A Policymaking Process "Tug of War": National Information Security Policies in Comparative Perspective., Journal of Information Technology & Politics. 10:462-476, 2013
86. Richards M. N., The Dangers of Surveillance., Harvard Law Review vol 126: 1934-65, 2013
87. Risen J. 2006, State of War: The Secret History of the CIA and the Bush Administration

88. Risen J. & Lichtblau E., Bush Lets US Spy on Callers Without Courts., N.Y. Times 16 Dec. 2005
89. Salter M. (2006a) The Border and the State of Exception in Bell C. &Managhan T. (eds) Exceptional Measures for Exceptional Times: The State of Security Post 9/11. Toronto, ON, Center for International and Strategic Studies., York University
90. Schoenfeld G., Has the "New York Times" Violated the Espionage Act., Commentary, March 2006
91. Select Committee to Study Governmental Operations With Respect to Intelligence Activities., US Senate., U.S. Government Printing Officr., Washington 26 April 1976
92. Stevens G. M. (Legislative Attorney, American Law Division), Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws, Report for Congress, Congressional Research Service 2003 (Updated version)
93. The 9/11 Commission, The Final Report Of The National Commission On Terrorist Attacks Upon The United States, 22 July
94. Thorburn M., Identification, Surveillance and Profiling: On the Use and Abuse of Citizen Data., University of Toronto 2012
95. The Text of President Bush's 20 September 2001 address to a joint session of Congress and the nation, The Washington Post http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html
96. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001., The Hundred and Seventh Congress of the United States of America., 3 January 2001
97. U.S. Congress, USA FREEDOM Act of 2015, Washington 6 January 2015
98. 104th U.S. Congress, Antiterrorism and Effective Death Penalty Act of 1996
99. U.S. Department of Justice, Legal Authorities Supporting The Activities of The National Security Agency Described By The President, 19 January 2006, Washington DC
100. United States Foreign Intelligence Surveillance Court., Memorandum of Law, In Reapplication of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things., Washington DC., 2 June 2015, Signed by Deputy Assistant Attorney General Evans. J. S., National Security Division, U.S. Department of Justice

101. Vault 7, CIA Hacking Tools Revealed, WikiLeaks https://wikileaks.org/ciav7p1/index.html

102. Vermuele A., The Constitutional Law of Congressional Procedure, 71 U. Chi. L. Rev. 361, 386 (2005)

103. Vinson R., FISA court order of 3 April 2007

104. Vinson R., FISA court order of may 2007

105. Weber, M. (1947) 'The Theory of Social and Economic Organization,' In T. Parsons (ed.) *The Theory of Social and Economic Organization,* Glencose: Free Press

106. Westin A., Privacy and Freedom., New York: Athenaeum 1967

107. Weber M., Economy and Society., Berkley, University of California Press 1978

108. White J., (2006) Terrorism and Homeland Security, 5th Edition, Thomnson/Wadsworth

109. Youngstown Sheet & Tube Co. v. Sawyer 343 U.S. 579 (1952), U. S. Supreme Court (https://supreme.justia.com/cases/federal/us/343/579/case.html)

110. Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." Yale Journal of Law & Technology 5, pp. 1-56