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 the defining moment of how security functions in the modern 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 a technology-enabled environment that scholarship characterizes as ‘surveillance society’ (Gandy 1989, Lyon 2001, Lyon & Bauman 2012).

Within technology-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 possibly vast 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 to uncontrolled repetition (Lyon 2007) leading to certitude in expectations. It is the reason why in security in general and in the war 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).
Surveillance has 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-emptive security policies, surveillance processes and practices are aiming to create the profiles of actual and potential sources of threats with high accuracy to produce 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 (Ceyhan 2008).

Because surveillance in the fight against terrorism must be a covert action to achieve its goal (Kitrosser 2007), in this circle of knowledge production and its operational execution specifically in the US war 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 the state 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 group behavior” (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 the US 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 the modern 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 the US 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 a list of US constitutional rights (Ballet. al 2009) including the presumption of innocence of persons for example that is a vital legal entitlement for the citizen of constitutional democracy (Thorburn 2012).

There is a consensus in scholarship, governments, and public intellectuals in general that it is fundamentally imperative to examine the meaning and the influences of modern
surveillance technology on state and society. In 2013 President Obama ordered a detailed 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 current head 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 been several remarkable events that coming together form a chronological chain with available 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 the selected 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). 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 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 the influential configuration of the independent 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 the certain 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 cover the background of the topic by 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 the US, the relations in US government structure in terms of surveillance,
examination of the list 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.