"WHO ARE WE, IF WE ARE NOT OUR BODY?"

SURVEILLANCE AND PRIVACY IN THE POST-9/11 ERA

by Zselyke Csaky

M.A. LONG THESIS

SUPERVISOR: Prof. Judit Sandor, Ph.D.

Central European University

1051, Budapest, Nador utca 9.

Hungary

TABLE OF CONTENTS

Abstract

It is often argued that the events of 9/11 have transformed our lives to a considerable extent. This argument implies fundamental changes in the field of privacy and suggests that the state encroaches upon our personal life to a much greater extent that before. The thesis therefore examines how privacy protection has changed since the attacks through the analysis of laws and policies of the United States, the European Union and the United Kingdom, where applicable. The analysis is conducted by narrowing down the focus from the general level of counter-terror laws to surveillance and the use of body scanners.

The general overview of counter-terror legislation shows that practices employed across the jurisdictions are remarkably similar and result in sweeping laws that significantly curb civil liberties. Preventive and soft security measures are prevalent in the inventory of the European Union as well, which therefore cannot serve as a model to the US. In addition, the analysis of surveillance laws in the United States and in Europe demonstrates the intensification of surveillance by the state, whilst the use of body scanners contributes to the aggravation of the situation. Yet, however privacy-invasive these measures should be, they still do not corroborate the emergence of a new conception of our body.

Introduction

Since the end of the cold war, human rights has become the dominant vocabulary in foreign affairs. The question after September 11 is whether the era of human rights has come and gone.[1]

Ten years have passed since the devastating events of 9/11. These ten years have been busy with forming policy-level and legislative answers to the threat of terrorism in the United States and in the European Union as well. This emerging, new type of threat, sometimes referred to as "superterrorism"[2] can be interpreted as creating a constantly sustained "state of exception"[3] that often serves as an explanation for the curbing of civil liberties by the state and also for the extraordinary measures applied against terrorist suspects. But how long can they be called exceptional? To what extent can they be justified in the normal course of life? Some argue that what we are heading towards is a new era where the constant and continuing "state of exception" becomes the "new normalcy".[4] Surveillance measures, economic sanctions against individuals, and other counter-terror preventive policies are on the borderline of the sphere of "exceptionalism". This sphere covers the "*array of illiberal policies and practices that are legitimated through claims about necessary exceptions to the norm*".[5] In the meantime, the terrorist is often constructed as the monstrous "other", someone who is inherently different from us.[6]

[1] M IGNATIEFF, *Is the Human Rights Era Ending?*, NEW YORK TIMES (February 05, 2002), http://www.nytimes.com/2002/02/05/opinion/is-the-human-rights-era-ending.html?src=pm [2011-10-01].
[2] Freeman, M. (2005). Order, rights, and threats : terrorism and global justice. In: R Ashby Wilson, *Human Rights in the `War on Terror'*, 1, 37 (2005).
[3] On the state of exception see the works of Carl Schmitt and G AGAMBEN, THE STATE OF EXCEPTION (University of Chicago Press ed. 2005).
[4] L. LAZARUS & B J GOOLD, SECURITY AND HUMAN RIGHTS 3 (Hart Publishing ed. 2007).
[5] Neil In: C. Aradau & R Van Munster, *Exceptionalism and the "War on Terror": Criminology Meets International Relations*, 49 BRITISH JOURNAL OF CRIMINOLOGY 686, 688 (2009).
[6] On the concept of the friend-enemy distinction see the works of Carl Schmitt, inter alia C SCHMITT, THE CONCEPT OF THE POLITICAL (University of Chicago Press ed. 2007).

During the past decade the notion of privacy as well as privacy protection itself has changed to a considerable extent. Although the concept of privacy has always been difficult to capture and it is only getting more and more complicated,[7] the post-9/11 world significantly contributed to the shaping of it. Moreover, in the United States likewise in Europe due to the technological advances and their massive use by criminals as well as law enforcement authorities the "right to be let alone"[8] was severely affected. These changes were so fundamental that some newspapers not only claimed that privacy is "eroding"[9] or "under attack"[10] but that it is dead altogether. However, this might have been only a false perception: "*Privacy, it seems, is not simply dead. It is dying over and over again"*.[11] Yet, the changes that took place after the 9/11 attacks deserve closer investigation. Not only because the growing importance of national security has resulted in a new, stricter regime which often caused significant harm to civil liberties, but also because there is another danger in these so-called "temporary" measures: that they might be here to stay.

Therefore the aim of the thesis is to analyze the changed circumstances in the post-9/11 world with a special focus on privacy. The thesis intends to explore two separate, yet intertwining issues: 1) the legislative and policy-level reactions to the new circumstances in the era of global terrorism and 2) the effects and influence of this "new normalcy" on us, individuals, i.e. on our private sphere and on the human body itself. The literature of privacy and the war on terror is vast and multifaceted therefore I attempted to focus the topic as much as possible. When analyzing privacy harms I chose to focus mostly on informational privacy,

[7] For an interesting and comprehensive account on the conceptualization of privacy and a new take see: D J SOLOVE, UNDERSTANDING PRIVACY (Harvard University Press ed. 2008).
[8] As formulated by Warren and Brandeis in their seminal article: S Warren & L D Brandeis, *The Right to Privacy*, HARVARD LAW REVIEW (1890).
[9] R O'Harrow, *Privacy Eroding, Bit by Byte*, WASHINGTON POST (2004) [07-10-2011].
[10] B Sullivan, *Privacy Under Attack, but Does Anybody Care?*, MSNBC (2006) [07-10-2011].
[11] Solove quoting Deborah Nelson in SOLOVE, *supra* note 7, at 5.

which concerns the "*collection, use, and disclosure of personal information*".[12] In addition, bodily privacy was included in the last chapter in connection with airport searches but strictly in an interpretation in which "bodily" refers to measures affecting our physical body and not in its original, more extended meaning that concerns decisions about one's body (e.g. abortion). As a methodological tool I have chosen the comparative approach to demonstrate the "globalized" and overreaching nature of the topic: there will be a comparison of American and European legislation, adding country-specific examples from the United Kingdom where applicable. To simplify things by "European" laws and regulations we refer to the acts and practices of the European Union and the decisions of the European Court of Justice (ECJ) or to the decisions of the European Court of Human Rights (ECtHR). Altogether, they create a uniform sphere, which includes most of geographical Europe, and therefore in the thesis they are handled as a separate jurisdiction.

The choice of these jurisdictions is deliberate and has factual as well as symbolic underlying reasons. What is common and symbolic in all three is that there have been three "first-hand" experiences of global terrorism in the Western hemisphere: 2001 New York (US), 2004 Madrid and 2005 London (EU and UK). In addition, the US and EU are the two most relevant Western actors on the international sphere therefore it is important to analyze their approach; whilst although having some overlapping regulations with the EU the United Kingdom can be placed somewhere between these two. It has a common law system with rather deferential courts unlike other European countries and a long history of domestic terrorism unlike the United States. Nevertheless, by citing and analyzing American and European laws, regulations and cases the aim of the thesis is not to show how different they are or how divergent the sphere of privacy protection is. On the contrary, the assumption is

[12] D J SOLOVE, M ROTENBERG & P M SCHWARTZ, PRIVACY, INFORMATION AND TECHNOLOGY 1 (Aspen Publishers ed. 2006).

that however different these jurisdictions might be the newly implemented privacy-invasive measures and techniques in the war on terror are surprisingly similar in all of them.

The (1) first part of the thesis introduces the basic characteristics of the post-9/11 era. By describing the consequences of certain hastily implemented laws and regulations in the aftermath of the attacks this chapter intends to establish a common ground for discussion. The (2) second part goes on to survey in detail the changes in the field of informational privacy through a special focus on surveillance laws. With omnipresent surveillance techniques in the new millennium we cannot avoid analyzing our new "Orwellian" or "Kafkaesque" environment, as scholars and critics constantly refer to it.[13] The (3) third part of the thesis focuses and narrows down the topic even more and aims to dissect a relatively new topic that has stirred enormous debate recently, namely, biometric identification and the use of body scanners. By aiming to answer the rhetorical question[14] in the title the final chapter tries to analyze indirect effects of counter-terror measures that might be permanent and reach beyond the sphere of law. Altogether, this narrowing structure of the thesis permits us to gain a general overview of the field of privacy protection after 9/11.

[13] See inter alia: L Donohue, *Anglo-American Privacy and Surveillance*, 96 THE JOURNAL OF CRIMINAL LAW AND CRIMINOLOGY 1059 (2006); M Kirby, *Terrorism: The International Response of the Courts*, 12 INDIANA JOURNAL OF GLOBAL LEGAL STUDIES (2005); LIBE, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, EUROPEAN COMMISSION JOINT RESEARCH CENTRE 1 (2003).

[14] Apart from being rhetorical this question constitutes our body as our visible representation to others. It by no means intends to assume that the self is equal to the physical body.

I. The Post-9/11 Era

Preventive police and preventive state?

So what impact has all this had on our response from a law enforcement perspective? The simple answer is that it has changed everything.[15]

In the contemporary "risk society",[16] a term coined by Ulrich Beck, institutional methods of control are easily disempowered by the perceived magnitude of risk and this has consequences in everyday politics: we are more prone to "*think security instead full employment, public education and the good society*".[17] In the meantime the value of life is also becoming more and more precious to the state in the sense that the protection of its citizens from newly emerging threats is vital, as it has become part of the core identity of the all-encompassing welfare state. Terrorism attacks this very core by showing that the state is not capable of protecting everyone and providing security and control over its territory to its own citizens.[18] It also has consequences when planning counter-terror measures as it means that police and security agencies have had to align their policies and practices to the exigencies of the situation.

Therefore new strategies have emerged and a culture of "risk management" rather than ordinary law enforcement is unfolding in front of our eyes. This new method tries to reconcile the interest of the state in enacting strict security measures with its human rights obligations, however, often without success. The most prevalent example of a failure is the

[15] P Clarke, *Learning From Experience – Counter Terrorism in the UK Since 9/11* (The Colin Cramphorn Memorial Lecture, April 2007).
[16] U BECK, RISK SOCIETY: TOWARDS A NEW MODERNITY (Sage Publications ed. 1986).
[17] G Mythen & S Walklate, *Criminology and Terrorism: Which Thesis? Risk Society or Governmentality?*, 46 BRITISH JOURNAL OF CRIMINOLOGY 379, 387 (2006).
[18] D Garland, *The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society*, 36 BRITISH JOURNAL OF CRIMINOLOGY 445 (1996).

slow but relentless development of the phenomenon of "*all-risks policing*".[19] The term, coined by Clive Walker, suggests that since risks can come from any direction, i.e. from citizens and non-citizens alike the police is willing to take action on less evidence-based information and try to prepare and react to every possible scenario. This also means that "*traditional markers as nationality and citizenship are not good indicators anymore",*[20] which can result in "suspicionless searches" and anti-terror acts tend to be formulated in a sweeping way.

The situation in the United Kingdom is a good example to demonstrate the magnitude of change. Although the UK has had a long history of extremists and terrorist attacks, mostly from the side of the IRA (Irish Republican Army), according to Peter Clarke Deputy Assistant Commissioner of the New Scotland Yard the role of the police has considerably changed in the past decade.[21] Police and security services have started a much closer cooperation that entailed police getting hold of information in a much earlier phase of the investigation. In addition, regional counter-terror units were set up to cover the whole area of the United Kingdom. However, this type of "risk management" means that the police tend to try and fulfill a "preventive" role, which can often result in the violation of certain rights, especially procedural rights. As Peter Clarke said:

> "*You could call this a "Risk Management" model of counter terrorism. If that sounds like 'consultant speak', I apologise. Let me immediately revert to English. What I am saying is that public safety will take precedence over evidence gathering, at all stages of an investigation."*[22]

[19] C. Walker, *Neighbor Terrorism and the All-Risks Policing of Terrorism*, 3 JOURNAL OF NATIONAL SECURITY LAW & POLICY 121 (2009).
[20] J. Ip, *Suspicionless Searches and the Prevention of Terrorism*, COUNTER-TERRORISM AND BEYOND 1, 2 (2010).
[21] Clarke, *supra* note 14.
[22] *Id.* at 7.

However, public safety can easily become a "catch-all" term and justify restrictive measures and abuse of rights.

These developments, nevertheless, can be viewed in a wider framework than simple changes in law enforcement practices. Some scholars in comparative constitutional literature argue that a change in constitutional models might be underway. This point of view is comprehensively demonstrated in an article by Andras Sajo, who claims that since the 9/11 attacks there has been a considerable shift towards the executive, which can pave the way for the emergence of a new type of constitutional model, the "counter-terror state".[23] This model consists of a "cluster" of constitutional responses to threats and perceived risk and it is based on two other models: militant democracy and the preventive state. The militant democracy paradigm was developed by Karl Loewenstein in his 1937 essay[24] as a possible answer of democracies to fascist movements. He claimed that extremist movements pursued emotionally manipulative policies against which democracies were defenseless and which might have resulted in the destruction of these democracies by their very own means. To avoid this certain measures needed to be implemented such as the outlawing of parties or the prohibition of symbols, etc. Sajo claims that only few constitutions contain reference to emergency situations or prevent abuse of democracy. However, Art. 17 of the European Convention on Human Rights is one rare example since it provides for protection against the abuse of convention rights.[25]

As for the other constituent element of the "counter-terror state" Sajo describes Carol Steiker's preventive state model. Steiker argues in her article published some years before the

[23] A Sajo, *From Militant Democracy to the Preventive State?*, 27 CARDOZO LAW REVIEW 2255 (2006).
[24] K Loewenstein, *Militant Democracy and Fundamental Rights*, MILITANT DEMOCRACY 231 (A Sajo, Eleven International Publishing ed. 2004).
[25] The article provides that *"Nothing in this Convention may be interpreted as implying for any state, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention"*.

9/11 attacks[26] that preventive measures were becoming so popular in law enforcement that they might have become routine and have spilled over from ordinary criminal law to other, general administrative areas of the welfare state. This vision gained increasing credibility after the attacks as described above.

From the two models Sajo forms the model of the "counter-terror state", which is tailored to the exigencies of the present situation, i. e. states operating under the constant threat of global terrorism. The question from now on is to what extent this possibly emerging new model turns against itself and starts undermining liberal democracy. There are many aspects of our lives that can be affected by these measures, from liberty restrictions to privacy violations. To be able to counter terrorist threat effectively, massive data collection is needed as a preventive method, which can result in the constant surveillance of citizens and in a more disastrous consequence that Sajo depicts clearly: the risk that "*all citizens are treated as being, at least to a small extent, potential terrorists*".[27] Moreover, there is another risk of singling out groups as theoretically more dangerous than others (eg. Muslims) and this way discrimination can become institutionalized in the process. Taking into account these possible abuses the author still claims that the existence of certain conditions can nevertheless justify a constitutional shift towards a "counter-terror state". The liberal constitutional state with its inherent risk-taking behavior might not be prepared in times of (constant) emergency to handle appropriately the magnitude of risk characteristic of a terrorist attack. Therefore Sajo argues that should global terrorism pose a constant threat to nation-states they have to be ready to implement a counter-terror order of which rights restrictions are part of and stronger judicial control plays an important role, but the limits of departure from "normalcy" are set in advance. Nevertheless, should we agree with Professor Sajo, we have to point out that in this

[26] C S Steiker, *Foreword: The Limits of the Preventive State*, 88 THE JOURNAL OF CRIMINAL LAW AND CRIMINOLOGY (1998).
[27] Sajo, *supra* note 22, at 2270.

case the question still remains: when do these "states of exceptions" begin, where do they end and how do we know that emergency is over? In other words: how long and in what circumstances can a fear from the unknown define our lives and justify the sometimes authoritarian moves of the executive?

Although it is beyond the means of the thesis to reconstruct the legal debate around the applicability of Carl Schmitt's "state of exception" to the post-9/11 era in its entirety, there is one strand I should mention before discussing in detail laws and regulations in force. Some scholars claim that the emergence of a "counter-terror state" is not a future possibility but rather reality we should accept:

> "*Finally, with the threat of terrorism likely to persist for the foreseeable future […] these [suspicionless stops and searches] should not be conceived of as being temporary security measures for exceptional times, but rather as harbingers of a new normality*".[28]

It is also often argued that this new normality is, however, not without precedent. The vocabulary and the measures for combating terrorism is claimed to have been ready before the attacks on the Twin Towers from biometrics to the fight against terrorist finances in the framework of fighting organized crime.[29] They were just waiting to be employed.

[28] Ip, *supra* note 19, at 21.
[29] A. Garapon, *The Oak and the Reed: Counter-Terrorism Mechanisms in France and the United States of America*, 27 CARDOZO LAW REVIEW 2041 (2006).

The United States after 9/11

"No group or nation should mistake America's intentions:

We will not rest until terrorist groups of global reach

have been found, have been stopped, and have been defeated."[30]

Since the United States is a global actor with global responsibilities and more extensive interests than other countries, its counter-terror responses can be set apart from other states' and even from the European Union, which also being a global actor, yet, a "soft power"[31] as generally defined. The American "War on Terror" had far-reaching consequences on international relations. However, it is beyond the scope of the thesis to analyze in detail the international and military aspects of US counter-terror policies such as those in Iraq and Afghanistan. Therefore this chapter focuses only on legislation that concerns domestic policies and influences the lives of US citizens at home; and we will get a mere impression of international effects by addressing executive acts in connection with detention abroad. It describes legislative changes after 9/11 starting with some provisions of the PATRIOT Act (however, privacy-related concerns will be examined in the next chapter) and a policy document, the National Strategy for Combating Terrorism. Then it will go on to address the use of presidential powers in two Supreme Court cases challenging detention in Guantanamo Bay.

Legislative Changes: The PATRIOT Act

The USA PATRIOT Act,[32] a fast and sweeping response to the 9/11 attacks was passed on October 24, 2001 and modified and re-enacted in March 2006. Although there is more and

[30] George W. Bush In: *National Strategy for Combating Terrorism*, CIA.GOV (2003), https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf [2011-11-01].

[31] On the notion of soft power see: J S NYE, SOFT POWER: THE MEANS TO SUCCESS IN WORLD POLITICS (PublicAffairs ed. 2004).

[32] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56, 115 Stat. 272 (2001))

more widespread campaigning for its revocation or revision from civil rights organizations such as the American Civil Liberties Union (ACLU), first the 16 sections containing sunset provisions were extended in 2005 and this year the remaining 3 got a four-year-extension yet again without much consideration from Congress.[33] Since then there have been almost one hundred new pieces of legislation passed in connection with the "war on terror".[34] The PATRIOT Act covered 341-pages in its first version and initiated changes in the field of security, surveillance, money laundering, immigration, criminal law and intelligence. Due to lack of space only some of the most problematic areas will be examined however, privacy-related features will be addressed in detail in the next chapter.

The definition of terrorism in section 802 is rather extensive: *"(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended-- (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping;"* and are domestic or international in nature. The broadness of the definition means that sanctioned acts might include acts of political protest and it can easily be abused by the government against opposition; therefore the Act can interfere with the course of normal political life.

The use of the so-called "sneak and peek" warrants constitutes another problematic issue. They permit law enforcement officials to conduct a search in the homes or offices without prior notification of the individual and seize certain objects or electronic communication, if necessary.[35] In 2010 there were 3970 "sneak and peeks" of which 76%

[33] *Post 9-11 Surveillance,* ACLU, http://www.aclu.org/timelines/post-911-surveillance [2011-11-01].
[34] For a comprehensive list see: http://www.counterterrorismtraining.gov/leg/index.html [2011-10-24].
[35] R Falk, *Encroaching on the Rule of Law,* NATIONAL INSECURITY AND HUMAN RIGHTS - DEMOCRACIES DEBATE COUNTERTERRORISM (University of California Press ed. 2007).

were drug-related, 24% were other and only less than 1% was connected to terrorism. [36] These numbers clearly demonstrate two things: (1) the doubts concerning the effectiveness of "sneak and peaks" in the "War on Terror" and (2) the way how counter-terror measures "spill over" from one area of law enforcement to others and become part of everyday practice.

The widespread use of National Security Letters (NSLs) is another example of overuse and possible abuse of extended counter-terror powers. With the issuance of NSLs FBI agents can have access to phone records, computer records, credit and banking history without the need for a court authorization. However, there were several sign of abuse found by the Department of Justice (DOJ) investigator, including NSLs used in non-emergency situations and also, there has been an emerging trend in issuing them: in 2010 alone there were 24 287 NSLs issued regarding 14 788 people, which is almost twice as much as in the previous year and more than ten times as much as in the year following 9/11.[37] Regarding their usefulness in countering terrorism the ACLU found that between 2003 and 2006 the FBI issued 192 499 NSLs, which led to one terror-related conviction that could have occurred without the PATRIOT Act as well.[38]

Policy Changes: A National Strategy for Combating Terrorism 2003

After the attacks a comprehensive US strategy for combating terrorism was drafted in 2003.[39] This Strategy, as it chose the above citation from George W. Bush as its motto, aimed for the total destruction of the "enemy" and this way the eradication of terrorism as such. This is a major difference with European examples explained in detail below, who often having had

[36] *Surveillance Under the PATRIOT Act* (American Civil Liberties Union, October 24, 2011), *available at* http://www.aclu.org/national-security/surveillance-under-patriot-act [2011-11-01].
[37] P YOST, *Rise in FBI Use of National Security Letters*, WASHINGTON POST (May 10, 2011), http://www.washingtonpost.com/politics/rise-in-fbi-use-of-national-security-letters/2011/05/09/AFN6xLdG_story.html [2011-11-01].
[38] Surveillance Under the PATRIOT Act, *supra* note 35.
[39] National Strategy for Combating Terrorism, *supra* note 30.

some experience with domestic terrorism looked at it in general as a phenomenon that does not necessarily need emergency legislation.[40]

The Strategy complemented the National Security Strategy by countering threat before it reaches the borders of the country - this way it demonstrated a preventive approach. Its goals were focused around the four "Ds" of (1) defeating terrorist organizations, (2) denying further sponsorship and support to them, (3) diminishing the underlying conditions that could nurture them and (4) defending the country. Although it aimed to destroy terrorism totally at the same time it recognized that victory is not self-explanatory in this area and therefore called for constant vigilance. This relentless vigilance was palpably demonstrated *inter alia* with the color-coded threat advisory-system that rarely changed from the orange "high" or the yellow "elevated" levels;[41] or the "If You See Something Say Something" public awareness raising campaign.[42]

Responses of the executive branch

On September 18, 2001 Congress passed the Authorization for the Use of Military Force (AUMF),[43] which permitted the use of "*all necessary and appropriate force*"[44] against nations, organizations and people involved in the attack. This means that legislative acts were not the only basis in the "War on Terror". The rather broad authorization in AUMF constituted as the source of power to detain terror suspects abroad, with which later George W. Bush issued the decree mandating the detention of suspects as enemy combatants.[45] This

[40] Although as seen below they also enacted their own counter-terror legislation, Garapon argues that European and US approaches are still different: Garapon, *supra* note 26.
[41] However, the color-coded system was replaced with a new version, the National Terrorism Advisory System (NTAS) which contains „more specific" information: http://www.dhs.gov/files/programs/ntas.shtm [27-10-2011]
[42] More information: http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm [27-10-2011]
[43] Public Law 107-40, 115 Stat. 224 (2001).
[44] AUMF s2(a).
[45] Military Order of November 13, 2001: Detention, Treatment and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed.Reg. 57831.

was an example of the use of executive powers, which also played a significant role in the "War on Terror". However, problematic historical examples such as the internment of US citizens of Japanese origins[46] still remind us that executive actions in wartime or in emergency situations can be dangerously sweeping and therefore we should be vigilant with their use.

Supreme Court challenges to counter-terror laws have so far included cases related to the detention of terror suspects at Guantamano Bay. In *Hamdi v Rusmfeld*[47] the Court held that US citizens retained their right to *habeas corpus* even if they were kept in prison as enemy combatants. Eight out of nine justices rejected the government's arguments that presidential powers based on Art. II of the Constitution or the AUMF justified detention of US citizens, stripped of their right to due process. Justice O'Connor writing in the name of the majority argued that they still had a limited right to due process, without some procedural protections such as the burden of proof falling on the government. However, two justices of the plurality opinion and Justice Scalia and Justice John Paul Stevens from the dissenters argued that the executive did not even have this broad war-making powers. Hence the powers of the executive were challenged indirectly in this case. In addition, in the 2006 case of *Hamdan v Rumsfeld*,[48] which concerned Salim Ahmed Hamdan, the chauffeur of Osama bin Laden, the Supreme Court ruled on the legality of military courts that tried the plaintiff. The Court found that these courts were against the Uniform Code of Military Justice and the Geneva Conventions as well and according to the majority opinion, George W. Bush did not have the power to set them up.

[46] *Korematsu v. United States*, 323 U.S. 214 (1944).
[47] *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004).
[48] *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006)

These two decisions challenged the extent of executive power and found it too broad, which can have long-lasting consequences in the legal and theoretical debate concerning separation of powers. In *Hamdan* Justice Breyer argued that

> "*Congress has denied the President the legislative authority to create military commissions of the kind at issue here. Nothing prevents the President from returning to Congress to seek the authority he believes necessary."*[49]

This means that the Justices drew the limits of presidential powers in the vague situation between peace and wartime and rejected the "overbroad" interpretation of the authorization given by AUMF.

Another abuse of power surfaced when the illegal wiretapping program of the National Security Agency (NSA) leaked through the press.[50] This program, which was authorized by President Bush to let federal agents spy on American citizens phone calls and e-mails without a warrant, resulted in immediate public outcry. The government argued that (1) the program is not illegal as it is based on AUMF, (2) it is narrowly focused, *"aimed only at international calls and targeted at al Qaeda and related groups"* and (3) it is consistent with constitutional and federal requirements.[51] Nevertheless, ACLU initiated a lawsuit against the agency. The organization was successful in the first round of litigation since the program was declared unconstitutional by a district court,[52] yet, the circuit court overturned the decision and the Supreme Court dismissed it based on the lack of standing, which is a

[49] *Id.* at 636.
[50] J RISEN & E LICHTBLAU, *Bush Lets U.S. Spy on Callers Without Courts*, NEW YORK TIMES (December 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all [2011-11-10].
[51] *The NSA Program to Detect and Prevent Terrorist Attacks - Myth V. Reality*, DEPARTMENT OF JUSTICE (January 27, 2006), http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf [2011-11-10].
[52] *ACLU v. NSA: The Challenge to Illegal Spying*, ACLU, http://www.aclu.org/national-security/aclu-v-nsa-challenge-illegal-spying [2011-11-12].

common problem in case of surveillance cases.[53] This entails that the Supreme Court is not always willing to review presidential powers in the "War on Terror".

Europe after 9/11

"Who, then, should check and complement American power? (…)

My answer is Europe."[54]

The European Union is likely to be perceived as a "normative power", which means that it has an ideological basis that includes the protection of values and human rights and which "*predisposes the Union to act in a normative way*".[55] This term, coined by Ian Manners refers to the peculiar nature of the EU as a supranational organization entails that the Union is expected to act in a more normative way than its global counterparts.

However, in the aftermath of the attacks normative behavior might not always "pay well". Therefore this chapter will critically assess whether the EU could fulfill the high expectations and act as a normative power in the face of the new era of terrorist threats during the past ten years. For this assessment first an overview will be given of the policies such as the Framework Decision on combating terrorism[56] or the Counter-terrorism Strategy[57] and then the measures applied will be analyzed including the European Arrest Warrant and economic sanctions against individuals. Subsequently the challenges to the legality of some

[53] *American Civil Liberties Union et al. v. National Security Agency et al.,* 493 F.3d 644 (6th Cir. 2007). Cf. ECHR cases on surveillance, which provide for standing in case of organizations and journalists prone to have their phones tapped.

[54] T G ASH, *The Peril of Too Much Power*, THE NEW YORK TIMES (April 09, 2002), http://www.nytimes.com/2002/04/09/opinion/the-peril-of-too-much-power.html?src=pm [2011-10-14].

[55] I. Manners, *Normative Power Europe: A Contradiction in Terms?*, 40 JOURNAL OF COMMON MARKET STUDIES 235–58, 252 (2002).

[56] 2002/475/JHA http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:164:0003:0007:EN:PDF [28-02-2011]

[57] http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf [28-02-2011]

of the measures taken by persons to the European Court of Justice will be summarized, especially the recent landmark decision by the ECJ in the *Kadi case*[58]. The overview of the area of the fight against terrorism should be indicative as how the protection of fundamental rights functions in the European Union and whether we can still call the EU a norm-centered power.

The Framework Decision on Combating Terrorism

The EU acted promptly after the fall of the Twin Towers and drew up Council decision 2002/475/JHA binding to all Member States. The decision defined the notion of a "terrorist offence" rather broadly with an objective and a subjective element. The objective element consists of the acts that can amount to a terrorist offence such as attacks on a person's life or the taking of hostages whilst the subjective element specifies it as "terrorist" in case it: (1) seriously intimidates population, (2) unduly compels the government or an international organization to perform or to abstain from performing an act or (3) seriously destabilizes or destroys the fundamental political, constitutional, economic or social structures of a country or an international organization.[59] The scope of terrorist activities is also broadened by the inclusion of inciting, abetting or aiding and other activities related to terrorist offences and it is an interesting feature of the decision that it specifically includes extradition as a possible penalty.

Although the introductory text of the decision starts with the enumeration of the universal values the Union is founded on, the consequences of the wording might encroach exactly upon those championed values and rights. By drawing the boundaries of the definition of terrorism so extensively and adding all possible related activities the Council

[58] Joined cases of C-402/05 P & C-415/05 P Kadi & Al Barakaat International Foundation v Council and Commission (2008).
[59] Art 1 of 2002/475/JHA

tried to set up an all-encompassing formula. However, this formula can become a dangerous tool in the hands of governments since it could be used outside its scope, such as in the case of non-government friendly protest groups.[60] The other problem with this approach of "*cast the net as widely as possible, identify suitable enemies, not worry about false positive identifications"* [61] is that it strengthens the legal sphere of exception by adding the "unexceptional"[62] and therefore legitimizes the surveillance and control of large and different groups of society.

The EU Counter-Terrorism Strategy

The Counter-Terrorism Strategy was issued after Europe gained "first-hand experience" of the nature of the threat, in the wake of the 2004 Madrid and the 2005 London bombings. The strategy set out to combat terrorism in cooperation with international actors such as the United Nations and "*promote good governance and democracy*".[63] These aims are built on the four pillars of Prevent, Protect, Pursue and Respond. The first pillar seeks preemptive[64] measures to combat the spread of radicalization and extremist ideas whilst the pillars of protection, pursuance and responding deal with hard security measures. The latter include border control and the use of other instruments such as the European Arrest Warrant, the freezing of terrorist funding or police and judicial cooperation in extended areas.

Whilst the fundamental rights concerns associated with hard security such as privacy and data protection rights were addressed by scholars to some extent [65] soft security

[60] Amnesty International In: M De Goede, *The Politics of Preemption and the War on Terror in Europe*, 14 EUROPEAN JOURNAL OF INTERNATIONAL RELATIONS 161 (2008).
[61] Ericson In: *id.* at 170.
[62] After the London bombings of 2005 the Home Office claimed in a report that the men did not have any distinguishing characteristics, they were all "unexceptional." In: Aradau & Munster, *supra* note 5.
[63] Para 5 of the Strategy
[64] Preemptive is used in the sense that measures are taken before the threat materializes.
[65] See inter alia In: Michael Levi & David Wall, *Technologies, Security, and Privacy in the Post-9/11 European Information Society*, 31 JOURNAL OF LAW AND SOCIETY 194 (2004); and LAZARUS & GOOLD, *supra* note 4.

instruments were mentioned less often. The measures under the heading of Prevention target especially the spheres of the practice of religion, prisons and the Internet. The decision to "single out" these places can be justified but there is still a danger that the consequences will be disproportionate.[66] Also, the call for enhanced civilian and bureaucratic involvement[67] in policing and preventing terrorism might lead to establishing what Judith Butler calls "*petty sovereigns*",[68] who decide on whether to issue travel visas to certain persons or to put them on lists. This results in large proportions of power being further distributed to uncontrolled areas, which means that it becomes more and more difficult to address human rights violations since their source or the one who is responsible for potential abuse cannot be easily pinpointed.

Other instruments

Stemming from these legal and policy documents several other instruments were also introduced in the fight against terrorism such as the European Arrest Warrant (EAW), the Data Retention Directive or the "war on terrorist finances". These instruments, however, have since then been assessed not only from the aspect of their effectiveness but also regarding their human rights implications.

The European Arrest Warrant was put into practice in 2002[69] to help fight cross-border crime. Nevertheless, since its establishment there were some doubts concerning the fairness of the procedure and the proportionality of issuing a warrant. Warrants have been issued for petty crimes such as stealing chicken; moreover, sometimes they were issued years

[66] As a Swedish journalist claims, the strategy suggests that in the face of terrorism that "»we«□(the white part of the European Union population), must prevent□»them«□(the Muslims) from being radicalized". In: Goede, *supra* note 58, at 170.
[67] Para 9 of the Strategy: "We need to spot such behaviour for example through community policing and monitoring travel to conflict zones".
[68] Butler In: Goede, *supra* note 58, at 170.
[69] 2002/584/JHA http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:190:0001:0018:EN:PDF [28-02-2011]

after committing the alleged crime and misused to send people back to their home countries.[70]

The Data Retention Directive 2006[71] obliged the providers of communication services all around Europe to keep communication data from a period of 6 months up to 2 years. This directive resulted in numerous attacks by civil society groups and by the Data Protection Commissioners of the Member States themselves. Peter Hustinx, the European Data Protection Supervisor called it "*the most privacy invasive instrument ever adopted by the EU*"[72] and argued that since there were problems in the implementation on the national level, at the moment citizens are faced with legal uncertainties. It is also problematic that the directive has a sweeping effect in a sense that everyone is subject to the surveillance of his or her personal communication, not only terrorist suspects.

The "war on terrorist finances" began with the United Nations Security Council Resolutions that were transposed to EU law.[73] They served as a basis for setting up a list of the freezing of assets of those associated with terrorist activities or those alleged to have links to terror suspects. There are several problems stemming from the nature of these measures and the authority issuing them. The "blacklists" have been criticized for serving as kind of bills of attainder since it allows for declaring outlaw persons or groups of persons and also for mistakes in adding people to the lists.[74] Concerning the issuing authority, it is problematic

[70] For an overview of problematic cases see: Fair Trials International - http://www.fairtrials.net/images/uploads/EAW%20-%20Cases%20of%20Injustice_1.pdf [28-02-2011]

[71] 2006/24/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [28-09-2011]

[72] P Hustinx, *The Moment of Truth for the Data Retention Directive* (Conference "Taking on the Data Retention Directive," December 03, 2010), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf [2011-10-01].

[73] The main Security Council Resolutions being SCR 1333, 1373 and 1390.

[74] K Roach, *Sources and Trends in Post-9/11 Anti-Terrorism Laws*, SECURITY AND HUMAN RIGHTS (Hart Publishing ed. 2007).

that the lists are compiled by a newly set up executive, the Sanctions Committee, without judicial oversight therefore alleged suspects cannot challenge the grounds on which they are charged, only in front of the European Court of Justice (ECJ).

ECJ Case Law: Challenges to the Legality of the Measures

Therefore, since regulations have direct effect, there were several challenges brought to the ECJ regarding the legality of counter-terror measures. Most of the cases were in connection with blacklisting and economic sanctions against individuals. One of the first cases was the *case of Jose Maria Sison,*[75] founder of the Communist Party of Philippines. Mr. Sison, who sought asylum in the Netherlands, had been placed on the list of suspected terrorists which he contested. He applied for an interim relief arguing that the measures deprived him of the basic necessities. However, the application was rejected by the Court of First Instance (CFI) in 2005 and the ECJ also dismissed his appeal in 2007 on the basis of lack of urgency.

Another unsuccessful but well-known case was the case of the Basque youth organization, *SEGI*.[76] The organization was included in the list because of alleged connections to the Basque separatist movement, ETA, as a result of which they claimed to have had suffered serious damages. The Court of First Instance denied their application for compensation on the grounds of lack of jurisdiction. The organization pursued the claim further before the ECJ arguing that the decision of CFI stripped them of effective judicial protection. Nevertheless, the ECJ upheld the decision and ruled that since the option of preliminary ruling procedure was still open to the applicants there was no breach of the right to an effective remedy.

[75] Case T-47/03 R, Jose Maria Sison v Council and Commission (2003).
[76] Case C-355/04 P Segi and Others v Council of the European Union (2007).

However, after the first few unsuccessful cases two judgments were handed down in 2008 that signaled a change in the direction taken by the ECJ. The first was the landmark case of *Kadi*,[77] in which the applicants argued that by being included on the list they were victims of a serious miscarriage of justice and that their right to property, fair hearing and judicial redress were violated. The CFI handed down a judgment in which it assessed the relationship between international law and EU law and took a dualist approach. It argued that since the measures were simply an implementation of a UNSC Resolution as a result of Article 103 of the UN Charter it does not have the jurisdiction to rule on the legality of such measures. However, in line with the Opinion of Advocate General Maduro, who argued that the fight against terrorism is not a "*political question*" i.e. the executive does not have unlimited discretion, [78] the ECJ overturned the judgment of the CFI. The Court argued that fundamental rights are part of the general principles of Community law and cannot be overridden by international agreements therefore the freezing of assets violated due process standards. The importance of the judgment lies in the turn the ECJ took in relation to international law and the resulting sovereigntist approach.[79] It underlined the autonomy of EU law and the importance of fundamental rights, however; on the other hand it somehow called into question the commitment of the Union to effective multilateralism as it overruled the decision of another international organization.[80]

The *OMPI I & II cases*[81] were also regarded as successful challenges to the legality of economic sanctions. This time, however, the freezing of assets was initiated by CFSP

[77] Joined Cases C-402/05 P and C-415/05 P Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission (2008).
[78] Opinion of AG Maduro, Para 34 http://blogeuropa.eu/wp-content/2008/02/cnc_c_402_05_kadi_def.pdf [28-09-2011]
[79] P T Tridimas, *Terrorism and the ECJ: Empowerment and Democracy in the EC Legal Order*, QUEEN MARY UNIVERSITY OF LONDON, SCHOOL OF LAW 1 (2009).
[80] G de Burca, *The European Court of Justice and the International Legal Order After Kadi*, 1 HARVARD INTERNATIONAL LAW JOURNAL (2009).
[81] Cases T-228/02 and T-256/07 Organisation des Modjahedines du peuple d'Iran v Council (2008)

Common Position 2001/931 which was to give effect to the UN sanctions, therefore the legality of the measures was analyzed under Community law. The CFI ruled in *OMPI I* that due process rights were violated as the applicants were not notified about the grounds and they could not counteract evidence on which the decision was made. Nevertheless, in a new Council decision the organization was again included on the list of terrorist suspects. In *OMPI II,* however, the CFI held that this time due process requirements were satisfied and did not annul the new decision, but at the same time argued that it was "*vitiated by illegality*".[82]

Another European Example: Counter-terror Legislation in the UK

To make comparison easier and demonstrate the effects of 9/11 on national legislation as well, the responses of the United Kingdom will be analyzed below. Although, the UK had significant previous experience with domestic terrorism (the case of Northern Ireland and the IRA as mentioned above) and several counter-terror laws had been in effect, 9/11 considerably extended and deepened the reach of existing legislation.

The United Kingdom Terrorism Act 2000

The United Kingdom Terrorism Act (2000 c. 11) was born before the attacks of 9/11 to counter domestic terrorism, yet, it serves a good example of the extension of the powers of the executive and it also supports the initial assumption that the vocabulary of the "War on Terror" was ready before the attacks. The Act was the first piece of counter-terror legislation that became permanent, while it defined terrorism in a much broader way than other, previous counter-terror legislation. According to Kent Roach it contained several features of militant democracies: including a harsher punishment for those who commit acts of violence

[82] Para 58 of OMPI II (2008).

with a religious, political, racial or ideological motivation and the opportunity for outlawing specific groups by making membership and association with them illegal. The inclusion of motivation was especially problematic since it could influence police when investigating a crime to look for the religious, political and other backgrounds of suspects and this way endanger members of certain ideological, religious etc. groups.[83]

The extension of stop and search powers of the police demonstrated well the effect the Act had on the everyday lives of citizens. According to sections 44-47 a three-stage procedure is to be followed by law enforcement authorities: the authorization, the confirmation and the exercise itself (sections 44-47). Reasonable suspicion is not necessary as grounds providing for the carrying out of the procedure and the confirmation is made by the executive, however, police officers should address the provisions of Code A of the Codes of Practice to the Police and Criminal Evidence Act (1984). Nevertheless, the use of these extended powers came under judicial scrutiny soon. In the UK case of *Gillan*[84] two applicants, who participated in a protest against an arms fare in London where they were stopped and searched, challenged the actions of the police in front of the House of Lords. They claimed that the authorization of stop and search powers was too extensive since it included the whole Metropolitan area and that it had been constantly renewed. However, the House of Lords found that the renewal was not a *"routine bureaucratic exercise"*[85] and the geographical scope of the authorization was also justified the whole London being under serious threat. The applicants also brought up the compatibility of the legislation with Articles 5,8,10 and 11 of the ECHR but the House of Lords stated that the measures were proportionate.

[83] K Roach, *Anti-Terrorism and Militant Democracy: Some Eastern and Western Responses*, MILITANT DEMOCRACY 171 (A Sajo, Eleven International Publishing ed. 2004).
[84] R. (Gillan) v. Commissioner of Police of Metropolis (2006) UKHL 12.
[85] Gillan (2006) para 18.

The applicants were not satisfied with the outcome and took their case to the ECHR. In *Gillan and Quinton*[86] they invoked the violation of the same articles as in domestic proceedings. The Court found a violation of Article 8, the right to respect for private life on the grounds that the law did not provide sufficient safeguards against abuse, i.e. its quality was not in accordance with the requirements. It emphasized that the wording of the Act was too lax and gave too wide discretion to police officers since they are "*not required even subjectively to suspect anything about the person stopped and searched"*.[87] In the application statistical data was cited about the effectiveness and application of the law and the Court observed that there were 117 278 searches conducted in 2007/08, which is a 215% increase compared to the previous year and this amount was very disproportionately distributed. Blacks and Asians accounted for the largest growth (322% and 277% respectively), while Whites lagged behind (185%).[88] Relying on these data the Court came to the conclusion that there was considerable risk of discrimination and abuse of power on the side of the police.

The Anti-Terrorism Crime and Security Act 2001

Since the Human Rights Act of 1998 came into force in 2000 the courts have dealt with 21 cases in the UK that involved a conflict between liberties and security and required them to engage in an act of balancing.[89] The legislative responses to the new threats were very fast; Parliament swiftly adopted the Anti-Terrorism Crime and Security Act in 2001 (ATCSA), which covered a wide range of activities from aviation security to police powers.[90]

[86] Gillan and Quinton v the United Kingdom (4158/05) (2010).
[87] Gillan and Quinton (2010) para 84.
[88] Gillan and Quinton (2010) para 46.
[89] B J Goold, *Public Protection, Proportionality, and the Search for Balance*, MINISTRY OF JUSTICE RESEARCH SERIES, ii (2007).
[90] M Elliott, *United Kingdom: Detention Without Trial and the War on Terror*, 4 INTERNATIONAL JOURNAL OF CONSTITUTIONAL LAW (2010).

However, Part IV of ATCSA came under close scrutiny in a case involving the detention of terrorist suspects without trial. The decision in the *Belmarsh prison*[91] case was applauded as the "*finest assertion of civil liberties*"[92] since resulted in the quashing of the relevant part of ATCSA. It also became a much-cited example of the effect of the Human Rights Act, under which judicial authorities were able to issue a declaration of incompatibility. Although the question whether the detention of suspects was considered necessary was answered in the affirmative since the House of Lords were confirmed that a threat existed to the "life of the nation"; the Law Lords argued that s23 of the Act was not only discriminatory but also disproportionate to foreign nationals. The case then went on to the Strasbourg court, which affirmed the decision of the House of Lords and ruled that although the UK had previously secured a derogation from Art. 5 of the ECHR (right to liberty and security of person) it was invalid as it was not "*strictly required by the exigencies of the situation*".[93] After this decision the Parliament drew up a new scheme, which introduced control orders as a method of pre-emption of terrorism[94].

The Prevention of Terrorism Act 2005

The Prevention of Terrorism Act 2005 (PTA) was again the result of a very fast procedure in the Houses of Parliament. It took 17 days to pass the bill since the government would have had to release unconditionally those detained if the legislation was not in force by March 2005.[95] Although so far about 50 people have been subject to control orders and at the

[91] A v Secretary of State for the Home Department, UKHL 56 2 AC 68 (2004).
[92] Gearty In: C. Walker, *The Threat of Terrorism and the Fate of Control Orders*, 4 PUBLIC LAW, 5 (2010).
[93] A and others v United Kingdom, 29 EHRR 29 (2009) para 182.
[94] Pre-emption covers measures taken before the threat materializes.
[95] E Bates, *Anti-terrorism Control Orders: Liberty and Security Still in the Balance*, 29 LEGAL STUDIES (2009).

moment there are 8 in force[96] the need for control orders and the consequences of its application have been heavily debated.

The PTA defines a control order as "*an order against an individual that imposes obligations on him for purposes connected with protecting members of the public from a risk of terrorism*"[97]. Therefore the orders serve to protect the public in cases where prosecution is not possible for several reasons such as lack or insufficiency of evidence, impossibility of extradition to home country because of the likelihood of torture, etc. As these "suspects" continue to serve as a threat to national security in the United Kingdom, the state has designed ways to render them harmless. Such obligations imposed on them are enumerated in s4 of the Act and include the prohibition or restriction of specified activities, communications with specified persons or by specified means, movements within and out of the United Kingdom, the requirement of electronic monitoring, etc. There are two types of control orders, non-derogating, i.e. those that do not curb the right to liberty "significantly" and therefore are issued by the Secretary of State and derogating ones, that require the supervision of a court to be issued.[98] Nevertheless, the use of control orders raised numerous problematic issues that can be grouped into three categories: (1) problems emanating from the wording of the Act, (2) problems in connection with the right to liberty (Art. 5 of the ECHR) and (3) problems in connection with fair trial rights (Art. 6 of the ECHR).

The latter two are too specific therefore out of the scope of this thesis, yet, the wording of the Act deserves some analysis. It raises concerns, as sometimes the language used is too vague and can give way to different interpretations depending on the aims of the executing body. For example, "terrorism-related activity" is defined very broadly in s1ss9

[96] Annual Renewal of Control Orders Legislation 2010. UK Parliament Publications. [28-10-2011].
[97] Prevention of Terrorism Act 2005 s1ss1.
[98] The term "derogation" refers to Art 5 of the ECHR.

since it includes the "*commission, preparation or instigation of acts*" as well as the facilitation, encouragement and support of such activities, therefore it is unclear whether members of anarchist or antiglobalist organizations can come under the scope of the act. Also, the list of possible interferences by the executive is not exhaustive, which may make the orders in the hands of the Secretary of State an arbitrary instrument.[99] Another problem that can be related to the language of the Act, although it concerns substantive requirements, is the applied standards. The standard for issuing an order is quite low since it only requires that there are

> "*reasonable grounds for suspecting that the individual is or has been involved in terrorism-related activity; and [the Secretary of State] considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, to make a control order*".[100]

This "reasonable grounds" standard is coupled with another low standard in the case of derogating control orders: the court can only interfere if the Secretary of State's decision is "obviously flawed".

A review process of the PTA was launched by the beginning of 2011 and the key questions in the consultation process included the indefiniteness of detention periods, the use of secret material and intercepted evidence and the effectiveness of the system as a whole.[101] This resulted in the repeal of control orders; however, the coalition government seems to cling to the use of them just with a different name. They were replaced with a "*more focused*

[99] J C Tham & K D Ewing, *The Continuing Futility of the Human Rights Act*, PUBLIC LAW (2008).
[100] PTA 2005 s2ss1.
[101] Review of Counter-Terrorism and Security Powers. (2011) http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/sum-responses-to-cons?view=Binary [28-09-2011]

and targeted regime"[102] called Terrorism Prevention and Investigation Measures (T-PIMs) in May 2011. However, media and commentators were skeptical about the new regime and in the news they called them only "control orders mark II",[103] which signifies that control orders are here to stay with us longer.

Conclusions

The thesis intended to demonstrate the characteristics of the post-9/11 world by describing legislative and policy-level responses in the United States, in the European Union and in the United Kingdom. By including two global actors and a member state of one of them the thesis intended to provide a very wide-ranging overview of the changes. The three examples above have several differences, not only in outcomes but also in initial settings such as legal systems and historical background. Historical differences include that the UK, like some other European countries (e.g. France, Spain), has already known terrorism since they had to cope with its domestic variant. Although it is true that global terrorism is an inimitable phenomenon some difference between US and EU approaches can be attributed to a shared history of terrorist violence of the latter. The fact that these countries do not face the "unknown" with all its terrifying effect contributes to a somewhat more moderate attitude in policy making.

However, in general it can be stated that all the examples characterize global, post-9/11 terrorism as a threat of such magnitude that justifies emergency legislation and disproportionate reactions. The disproportionate nature of the reactions is palpably described

[102] Review of CT powers and legislation published. Home Office. http://www.homeoffice.gov.uk/media-centre/press-releases/ct-powers [28-09-2011]
[103] See A Travis, *Control Orders: Home Secretary Tables Watered-down Regime*, THE GUARDIAN (2011); *Review of Terror Laws: New Name for an Old Problem*, THE GUARDIAN (2011).

in either final court judgments such as the *Kadi* decision by the ECJ claiming that fundamental rights were violated or the *Belmarsh prison* case, when the House of Lords and the ECHR both declared that the detention regime of ATCSA was disproportionate; or it can be seen from challenges brought by civil rights organizations, such as when the ACLU challenged several parts of the PATRIOT Act.

In addition, Alison Brysk claims that the different policies towards terrorism can be accounted to a difference "*in prior legal regimes, which are reinforced or reconstructed in response to terror*".[104] She argues that European countries such as Germany have unitary legal regimes and apply uniform standards to everyone, the UK authorizes some departure from this in a rule-bound way, while the US applies a differential regime where standards apply to only part of the population and there is a "grey zone" of illegal state action that leaves place for abuse. Also, the United States uses the executive model for promulgating counter-terror measures compared to the legislative models used by European countries. In the former, the executive branch plays a much bigger role leaving less place for legislation as it could be seen above. According to Barak-Erez,[105] there are several differences between the two models. These include a difference in secrecy and transparency, with legislative acts available to the public as opposed to executive acts that often come to the attention of the public only by being leaked through the press.[106] Counter-terror laws also tend to have judicial limitations and the mechanism of review included in their texts, while

[104] NATIONAL INSECURITY AND HUMAN RIGHTS - DEMOCRACIES DEBATE COUNTERTERRORISM 7 (A Brysk & G Shafir, University of California Press ed. 2007).
[105] D Barak-Erez, *Terrorism Law Between the Executive and Legislative Models*, 57 THE AMERICAN JOURNAL OF COMPARATIVE LAW 877 (2009).
[106] For example the scandal around the spying by the National Security Agency: C SAVAGE & J RISEN, *Federal Judge Finds N.S.A. Wiretaps Were Illegal*, NEW YORK TIMES (March 31, 2010), http://www.nytimes.com/2010/04/01/us/01nsa.html [2011-11-01].

there is no such possibility in case of executive actions.[107] However, the negative side of legislative actions is that they are prone to be incorporated into the legal system and remain with us much further than executive orders in general. Although they often have sunset clauses, these tend to be extended from time to time. Yet, Erez-Barak argues that executive orders can also become more long-lasting than intended to be by providing "precedent" such as the World War II presidential orders cited by George W. Bush. In addition, there can be a difference in timing with executive orders being much faster and effective in times of crisis but lacking the public debate behind them. However, as seen above most counter-terror legislation were passed in a hurry, which also left no place for public deliberation.

Concerning the EU, after the above mentioned legislative changes and challenges before the ECJ the question is whether the European Union can be regarded as an "*alternative normative space within current global security practice*".[108] The policy-level and legislative overview showed that the European Union like its American counterpart cannot escape the "appeal" of exceptionalism either. Although the EU identifies itself on the face as the protector of human rights and fundamental values, its counter-terror policies have significant indirect implications that curb civil liberties and provide a possibility for abuse by the state. The analysis of some of the practical instruments such as the European Arrest Warrant, the Data Retention Act or economic sanctions on individuals also demonstrated that counter-terrorism policies might result in a sweeping implementation that can often lead to severe human rights violations.

[107] However, it is remarkable in the US context that regarding detention orders both branches were unwilling to "expose" themselves to judicial review: the presidential order included only trials by military courts while Military Commissions Act of 2006 also limited access to courts by enemy combatants.
[108] Beck In: Goede, *supra* note 58, at 168.

However, the analysis of the case law revealed a new approach on the side of the ECJ that seems to bring back the "human rights element" into the picture. The annulment of certain counter-terror measures on the grounds that they violate fundamental rights show that the Court is still willing to push the Union in the direction of a more norm-centered power. Yet, we still have to wait to be able to decide whether it is because of the importance of the rights themselves or there is an underlying struggle for the autonomy of EU law. It is even more so as the analysis of UK legislation supports critical voices. First, the evaluation of Terrorism Act 2000 proves that the vocabulary of the "War on Terror" was ready before the attacks and second, the struggle of the government with control orders and their continuation in subsequent legislation shows that there is considerable danger of "exceptional", "temporary" legislation becoming permanent.

Altogether, it seems that *prima facie* legislative and executive counter-terror actions in the US and in Europe despite the many differences in legal systems and historical background were strikingly similar from the definition of terrorism to emergency actions and their spillover to other areas of law enforcement. This similarity can be accounted to the analogous threat of global terrorism, yet, in the next chapter it will be analyze whether there is a difference in the impact of the threat on a lower level, the level of individual privacy and surveillance legislation.

II. Privacy and the Spread of Surveillance

As it was mentioned in the introduction, it is extremely difficult to define privacy and therefore the scope of the right. Although according to some scholars it is difficult to even evaluate its importance to individuals.[109] The thesis is based on the underlying assumption that privacy is a fundamental right, which is essential to individual self-fulfillment. It also contributes to a flourishing democratic society by protecting autonomous individuals, as privacy-expert Anita Allen argued: "*Opportunities for individual forms of personal privacy make persons more fit for social participation*".[110] However, the concept has been harshly criticized for example by feminist authors claiming that separating the private and public domain left women in the private domain unprotected, exposed to domestic violence masked under the heading of "privacy".[111]

Despite these problems, Daniel J. Solove tried to develop a new understanding of privacy based on a bottom-up approach and conceptualize it in a more general way.[112] This concept includes all aspects of life that people might perceive as private but frames privacy as contingent on the circumstances, i.e. society and culture. Therefore he acknowledges that what we perceive as private can and have changed over time, yet, there are some aspects that have usually been considered to be part of it such as family, sex, home, or communications. Our body, the topic of the third chapter, was also often perceived as the core of privacy and something to protect and shield from others. This approach is prevalent in the opinions of the Supreme Court of the United States and characterized well in a 1998 decision of the Court:

[109] „The panic about privacy has all the fingerpointing and paranoia of a good old American scare, but ir's missing one element: a genuinely alarmed public. Americans care about privacy mainly in the abstract." Franzen In: SOLOVE, *supra* note 7, at 5.
[110] A L ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 51 (Rowman & Littlefield Publishers ed. 1988).
[111] J DECEW, *The Feminist Critique of Privacy*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (FALL 2008 EDITION) (2008), http://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=privacy [2011-11-10].
[112] SOLOVE, *supra* note 7.

"One's naked body is a very private part of one's person and generally known to others only by choice."[113] However, it has not always been like this. As Solove explains, people used to have very different ideas about nudity and privacy of the body throughout the history of humankind, yet, by today the "ownership" over one's body has become universally accepted.

This chapter aims to describe the characteristics and legal background of surveillance in the United States and in Europe. However, as surveillance interferes with the right to privacy, first it is essential to sketch a short outline of the meaning of the right. The concept of privacy protection is significantly different in Europe from its sister concept on the other side of the ocean in name and in content as well. Although general privacy rights are protected under Art. 8 (right to private and family life, protection of home and correspondence) of the ECHR, there is a separate regime for informational privacy rights. The data protection regime, which is a "*catch-all term for a series of ideas with regard to the processing of personal data"* [114] is claimed to be much stricter and in many aspects incomparable with the United States, where data protection is primarily regulated by statutory and not constitutional law.[115] To understand the relationship between privacy and data protection scholars often make a distinction to view privacy as an "opacity tool" and data protection as a "transparency tool".[116] Nevertheless, in the first section the thesis will focus specifically on data protection in the case of Europe as it is a peculiarity and deal with general privacy rights under the ECHR only in the second section on surveillance. In the introductory part the development of privacy protection in the United States will also be described. This way this chapter is going to present a very rough outline of this extensive

[113] *Elli Lake v. Wal-Mart Stores, Inc.* 582 N.W.2d 231 (Minnesota 1998) 235.
[114] S. Gutwirth et al., *Reinventing Data Protection*, 1, 3 (2009).
[115] S SOTTIAUX, TERRORISM AND THE LIMITATION OF RIGHTS: THE ECHR AND THE US CONSTITUTION (Hart ed. 2008).
[116] To read more on this see inter alia: P De Hert & S. Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, PRIVACY AND THE CRIMINAL LAW 61 (2006).

field, which makes comparison incomplete. Yet, by juxtaposing the different regimes it can still shed some light on the similarities and differences between them.

Privacy Protection in the United States and in Europe

Although with the Warren and Brandeis article[117] the beginning of the "history" of privacy in the United States dates back to as early as the 19th century, the different fields of privacy protection developed only later. According to Mills, the development of privacy protection can be broken down into three subgroups which construe the "family tree" of contemporary US privacy jurisprudence: (1) privacy torts, (2) 4th Amendment jurisprudence and (3) constitutional protection.[118]

As for privacy torts they were categorized into four types in Prosser's landmark article in 1960: intrusion, public disclosure of private facts, false light in the public eye and appropriation.[119] Concerning 4th Amendment jurisprudence, it started with a case that has "direct connection" with Warren and Brandeis's seminal article: *Olmstead v United States.*[120] In this Justice Brandeis voiced a dissenting opinion, which became law only later in *Katz,*[121] yet, it extended privacy protection in the field of search and seizure and stated that "*the Constitution protects people, not places*".[122] However, the details of these cases will be described in more detail in the next part on surveillance. The last branch of the "family", i.e. constitutional jurisprudence developed after *Griswold,*[123] which defined a right to privacy from the "penumbra" of other rights: the 1st (right of association), 3rd (prohibition of

[117] Warren & Brandeis, *supra* note 8.
[118] MILLS, *supra* note 108.
[119] W L Prosser, *Privacy,* 48 CALIFORNIA LAW REVIEW 383 (1960).
[120] *Olmstead v. United States* 277 U.S. 438 (1928).
[121] *Katz v. United States* 389 U.S. 347 (1967).
[122] *Katz* at 351.
[123] *Griswold v. Connecticut* 381 U.S. 479. (1965).

quartering soldiers without consent), 4th (protection from unreasonable search and seizure), 5th (protection against self-incrimination) and 9th (rights not specifically enumerated in the Constitution) Amendments. In addition, *Whalen*[124] extended the scope of substantive due process protection to information privacy. Nevertheless, privacy can sometimes even be in contradiction with these very penumbral rights it emanated from, for example with freedom of speech.

The other source of privacy protection is statutory law, which emerged only from the mid-1960s and mid-1970s after the above mentioned seminal Supreme Court cases. The Privacy Act of 1974[125] provided the basis for certain rights such as the right to access to public records. Another piece of important legislation, which will be discussed in the next chapter, the Foreign Intelligence Surveillance Act (FISA)[126] regulates foreign intelligence information gathering; however, important parts of it were significantly amended by the PATRIOT Act. Electronic communications is regulated by the Electronic Communications Privacy Act (ECPA)[127] and most recently by the Video Voyeurism Prevention Act.[128] This criminalizes the capturing of nude images of people with a reasonable expectation of privacy and will be relevant in the last chapter on body scanners.

Concerning the legislative background of the European Union, there are primary and secondary sources of data protection. Primary sources include Art. 16 of TFEU,[129] which provides everyone with a right to protection of personal data; and Art. 39 of TEU,[130] giving authorization to the Council to set rules of data protection. The most recent but at the same

[124] *Whalen v. Roe* 429 U.S. 589 (1977).
[125] Privacy Act of 1974, Public Law No. 93-579, 5. U.S.C. s552(a).
[126] Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511, 50 U.S.C. s1566.
[127] Electronic Communications Privacy Act of 1986, Public Law No. 99-508, 18 U.S.C. s2510.
[128] Video Voyeurism Prevention Act of 2004, Public Law No. 108-495, 18 U.S.C. s1801.
[129] Treaty on the Functioning of the European Union (OJ 2010 C 83) – previously known as „Treaty of Rome".
[130] Treaty on the European Union (OJ 2008 C 115) – previously known as the „Maastrich Treaty".

time very important change in the field was the inclusion of a specific right to the protection of personal data in the Charter of Fundamental Rights of the European Union. Here data protection is provided as an independent fundamental right and not as part of the right to privacy. As for secondary sources, one of the most important informational privacy-related regulation is the Data Protection Directive.[131] It provides for transparency about the processing of personal data generally and sets forth the rights of data subjects such as a right to erasure, correction or rectification of personal data. In Art. 2(a) it defines personal data as

> "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

Because of the novel nature of the field the case law of the European Court of Justice is rather scarce on data protection. Apart from infringement proceedings[132] initiated against member states the few cases include a preliminary ruling requested by the Austrian Supreme Court and another one dealing with the clash between data protection and freedom of information in Germany. The former, the *Österreichischer Rundfunk (ÖRF)*[133] case was the first decision handed down on the Data Protection Directive. It challenged the obligation of public bodies to communicate salaries and pensions above a certain level with the name of the recipient and relied on Art. 8 of ECHR, this way protecting data protection rights under general privacy rights. On the contrary, in the *Bavarian Lager*[134] case the Court found no

[131] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281).
[132] An action taken by the European Commission in case it finds a member state is not in compliance with EU-law, e.g. it fails to implement the Data Protection Directive in its national legislation.
[133] Joined cases of C-465/00 and C-138/01, Rechnungshof v. Österreichischer Rundfunk (2003).
[134] T-194/04, Bavarian Lager v. Commission (2007).

violation of the data subjects' right, who participated in a meeting of which the minutes were asked to be made public by another company. The Court distinguished this case from the *ÖRF* case on the ground that no personal opinions could be identified as all participants were present in their official capacities and therefore gave way to the freedom of information request.

In the United Kingdom there is a statutory basis for the right to privacy in the incorporation of Art. 8 of ECHR with the Human Rights Act and in the Data Protection Act of 1998. The latter was enacted to bring UK legislation in line with the EU Data Protection Directive and regulates the use, collection, storage and disclosure of personal data in a rather complex way. In addition, in common law jurisprudence the tort of the "breach of confidence" is applied in privacy-related cases. This tort provides an actionable right if information is disclosed that can possibly interfere with one's right to privacy: such as the unauthorized publication of Michael Douglas's wedding photos[135] or Naomi Campbell's treatment at Narcotics Anonymous.[136] These cases are good examples of the clash between the right to privacy and freedom of speech.

A case that can serve as a lithmus test to demonstrate the nature of the relationship between the US and Europe can be the series of discussions on the exchange of Passenger Name Records. After the attacks of 9/11 the US Department of Homeland Security requested access to and transfer of PNR data of all air passengers, which resulted in the signing of the PNR Agreement in May 2004.[137] The Council decision declared that the level of data protection provided by the US Customs and Border Protection is adequate according to EU

[135] *Douglas v. Hello! Ltd.* [2005] HRLR 27.
[136] *Campbell v. MGN Ltd.* [2004] UKHL 22.
[137] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183).

regulations. However, the European Parliament was not satisfied with this and applied to the ECJ for annulment arguing that the decision was taken *ultra vires* and resulted in the infringement of fundamental rights. The ECJ accepted the reasoning of the Parliament and ruled in the *PNR* case[138] that the decision was not made under Community competences since it concerned the area of public security and the actions of states in the field of criminal law, which was excluded from the scope of the Data Protection Directive.[139] After this decision a new agreement was signed between the EU and the US,[140] which has been provisionally used since 2007 awaiting the adoption of a final version. Yet, neither this provisional nor the final version that is currently awaiting the European Parliament's first reading[141] can be said to protect privacy satisfactorily.[142]

However, there is still a meager chance of dismissal by the EP. This shows that the Parliament attributes more importance to the protection of personal data than authorities in the United State. This fact together with the extent of the debate shows the differences in approach of the EU and the US concerning the role of data protection.

[138] Judgment of the Court of Justice in *Joined Cases C-317/04 and C-318/04* European Parliament v Council of the European Union and European Parliament v Commission of the European Communities (2006).

[139] Art. 3 (2): „*This Directive shall not apply to the processing of personal data:- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.*"

[140] 2007 PNR Agreement (OJ 2007 L 204).

[141] Legislative Observatory: http://www.europarl.europa.eu/oeil/file.jsp?id=5836052 [2011-11-18]

[142] For details see the database compiled by Statewatch: http://www.statewatch.org/pnrobservatory.htm [2011-11-18]

The Spread of Surveillance

> *It is not expected that such mind-controlling devices will become reality before the 2020 horizon. Nevertheless this futuristic though probable example begs the question "who watches the watchers?"*[143]

The spread of surveillance has been probably the most "palpable" example of the consequences of the "war on terror". Two authors, George Orwell and Franz Kafka are often cited to describe the fears about changed circumstances, which are characterized by the omnipresence of government and control of the population in almost all areas of life. This chapter aims to focus on the analysis of privacy implications of the "war on terror" and demonstrate how surveillance laws have functioned in the second half of the 20th century and how they have changed after 9/11 in Europe and in the United States.

The surveillance literature uses two different terms to explain the expansion of surveillance measures and technologies: "surveillance creep"[144] and "surveillance surge".[145] While the former refers to the gradual and somewhat concealed build-up of new surveillance techniques and their incorporation in society under the name of technical progress or altered circumstances, the latter illustrate a prompt reaction to an unexpected event. The aftermath of the events of 9/11 and the subsequent London and Madrid bombings in Europe belong to the domain of "surveillance surge". There is a common name for all these measures taken in the name of security: the "surveillant assemblage".[146] This concept reveals that there is a certain "*relationship between heterogeneous surveillance technologies that »work« together as a*

[143] LIBE, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, EUROPEAN COMMISSION JOINT RESEARCH CENTRE 1, 26 (2003).
[144] G. Marx in D. Wood et al., *The Constant State of Emergency? Surveillance After 9/11*, THE INTENSIFICATION OF SURVEILLANCE - CRIME, TERRORISM AND WARFARE IN THE INFORMATION AGE 137, 141 (2003).
[145] C. Norris & G. Armstrong in *id.*
[146] Haggerty K. and Ericson R. in Levi & Wall, *supra* note 63, at 199.

functional entity without any other unity".[147] This way they do not only interfere with "informational self-determination"[148] but at the same time construct a very efficient structure for controlling societies.

Nevertheless, it has to be noted that these restrictive measures were not entirely new. The terrible events only served as a trigger that legitimized already existing trends and allowed for their expansion.[149] Together with technological advances this lead to the blurring of lines between different types of punishable activities since "*the transforming capabilities of ICTs make it increasingly difficult to distinguish between warfare, terrorism and criminal activities*".[150] Soft security measures such as surveillance have become part of our everyday lives; moreover they are proactively promoted and applied by the government. By now their abundant use entails a risk that from ordinary citizens a new group of "suspects" is being formed in the workings of the assemblage.[151]

In the subsequent part I am going to narrow the scope of the thesis and analyze how surveillance works in the United States and in Europe. First, 4th Amendment jurisprudence and the statutory background will be covered in the United States and then the chapter will focus on the case law of the European Court of Human Rights (ECtHR). Through this, surveillance laws of the different European countries can also be evaluated.

[147] *Id.*

[148] *"[T]he right of the individual to decide within what limits data concerning his private life might be divulged and to protect himself against an increasing tendency to make him »public property«"*Concurring opinion of J. Pettiti in *Malone v the United Kingdom* (1984) (8691/79).

[149] K. Ball & F. Webster, *The Intensification of Surveillance*, THE INTENSIFICATION OF SURVEILLANCE - CRIME, TERRORISM AND WARFARE IN THE INFORMATION AGE 1, 3 (2003).

[150] CYBERCRIME: LAW ENFORCEMENT, SECURITY AND SURVEILLANCE IN THE INFORMATION AGE 3 (D. Thomas, & B. Loader, 2000). ICTs refer to "information communications technologies".

[151] David Lyon, *Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies1*, 4 INTERNATIONAL POLITICAL SOCIOLOGY 325 (2010).

Surveillance in the United States

The 4th Amendment and Reasonable Expectations

From the above mentioned "family" of privacy it is 4th Amendment jurisprudence that is mostly applicable in connection with surveillance cases in the United States. The 4th Amendment provides that it is a right to be secure in one's "*houses, papers, and effects, against unreasonable searches and seizures*" and it also sets forth the conditions of lawful warrants, which should be issued

> "*upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

The first case that concerned surveillance in front of the Supreme Court was *Olmstead v. United States.* Olmstead was convicted for selling and importing intoxicating liquors in violation of the National Prohibition Act and had been wiretapped for several months of which he argued had been contrary to the 4th and 5th Amendments of the Constitution (protection against unreasonable searches and seizures and due process). Although the majority relying on the doctrine of physical trespass ruled that 4th Amendment protections did not apply to wiretaps, Brandeis's dissent became famous later. He claimed that there is a right to privacy inherent in the Constitution and that "*[s]ubtler and more far-reaching means of invading privacy have become available to the Government"*[152] which necessitate this protection. However, the doctrine of trespass was referred to in later surveillance cases as well.[153]

Olmstead's holding, however, was no good law after the 1960s and Brandeis's dissent received support in a case, which defined the "reasonable expectation" standard. This threshold defines the scope of protection against searches and seizures and it was specified in Justice Harlan's concurring opinion in *Katz.* The case, which overturned *Olmstead,*

[152] *Olmstead* at 473.
[153] See inter alia *Goldman v. United States* 316 U.S. 129 (1942).

concerned a decision to sentence an individual based on information caught through the wiretapping of a public telephone booth. Mr. Katz challenged the decision claiming that his 4th Amendment rights were violated by the conduct of FBI agents. Therefore the question formulated before the Supreme Court was whether (1) a telephone booth in public is a constitutionally protected private area and whether (2) physical intrusion is a necessary condition of a search and seizure to constitute "*violative of the Fourth Amendment*".[154] The Court, however, refused to answer the question this way and stated that "*the Fourth Amendment cannot be translated into a general constitutional »right to privacy«";*[155] *it* only protects against certain types of government intrusions into one's private sphere. They found that physical intrusion is not necessary for an interference to constitute as search and Mr. Katz had a "*reasonable expectation of privacy*"[156] therefore his 4th Amendment rights were violated. Justice Harlan defined a twofold requirement for the "reasonable expectation" standard: (1) a subjective expectation from the individual and (2) an additional element from society that it is willing to recognize this expectation. However, the decision resulted in a narrow conception of privacy in the Court's jurisprudence and defined it mostly in terms of secrecy, what an individual wants to preserve as private. This means that the "reasonable expectation" standard cannot be used in case the object is visible to everyone (the plain view rule), and if information is stored by third parties to whom the individual voluntarily gave his/her information (e.g. financial records).[157]

The Warrant Clause

In addition to the "reasonableness" standard of the search and seizure clause, the 4th Amendment has a second clause saying that "*no Warrants shall issue, but upon probable*

[154] *Katz* at 349-350.
[155] *Id.* at 350.
[156] *Id.* at 360.
[157] SOTTIAUX, *supra* note 114.

cause". However, there are two different interpretations about the reading of this clause. The "conventional" interpretation suggests that the two clauses should be read in conjunction, i.e. for a search or seizure to be reasonable there is need for a probable cause and a valid warrant. The second, more balancing interpretation requires the existence of a general standard of "reasonableness" of which these are only two factors to be considered.[158] This balancing approach can be very important in cases concerning terrorism where individual privacy interests are weighed against public security. However, the "probable cause" standard is higher than "reasonable suspicion" and it needs *"more than a bare suspicion but less than evidence that would justify a conviction"*.[159]

Also, there are certain exceptions that can justify a warrantless search such as the existence of "exigent circumstances" which would make the issuance of a warrant "impractical" for example because of the lack of time; and in case of the "special needs" doctrine. This latter is often applicable in case of administrative searches, when a warrant would constitute too much a burden.[160] There is an interesting exception concerning the means of surveillance: the use of pen registers is exempt from 4th Amendment protection. A pen register is a device that can record all phone numbers dialed from a telephone.[161] In *Smith v. Maryland*[162] the Court found that the defendant, who wanted to have evidence excluded on the basis that it was obtained contrary to 4th Amendment protections, had no reasonable expectation of privacy. They argued that when a person was dialing a number he/she should have been aware of the fact that the number is conveyed to the phone company and in addition, the content of the communication is still protected under the 4th Amendment. Nevertheless, in a few years time ECPA started regulating the use of pen registers under Title

[158] N Strossen, *The Fourth Amendment in the Balance*, 63 NEW YORK UNIVERSITY LAW REVIEW (1988).
[159] BLACK'S LAW DICTIONARY (B A Garner, Ninth Edition ed. 2009).
[160] SOTTIAUX, *supra* note 114.
[161] For a more concise definition see 18 U.S.C., Chapter 206 s3127.
[162] *Smith v. Maryland* 442 U.S. 375 (1979).

III and stated that law enforcement agencies should apply for a court order to use the device. However, the only requirement for the court order is certification that "*the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."*[163] This low standard was combined with an extension of the definition of pen registers to include "other facilities" in the framework of the PATRIOT Act,[164] which provided for the possibility of tracking the path of electronic and Internet communications along the same logic.

Procedural Safeguards

There are also some procedural safeguards present in 4th Amendment jurisprudence on surveillance. These were set out in *Berger v. New York*[165] which invalidated a New York state statute *prima facie.* Section 813 of the New York Code of Criminal Proceedings, which regulated the use of surveillance orders was found to be too broad in its language and therefore in violation of 4th Amendment requirements. The Court found that the statute did not satisfy at least three characteristics: (1) the need for a description of the place to be searched or object to be seized, (2) time limits on surveillance and (3) the notification requirement. Since there was no need for any precision regarding the search or seizure a "*roving commission*"[166] was given to the official conducting it. Concerning the time limit for surveillance, first the statute permitted it for an initial 2-month period, which was a "*series of searches and seizures*" and second, there was a possibility for extension only based on a mere showing of "*public interest*".[167] In case of the third criteria, the requirement of a notice the Court recognized that the success of the statute depends on secrecy, yet, they found it

[163] 18 U.S.C. s31223(a)(1).
[164] PATRIOT Act s216.
[165] *Berger v. New York* 388 U.S. 41 (1967).
[166] *Id.*
[167] *Id.* at 42.

unsatisfactory that it did not even require "*some showing of special facts*"[168] that would justify the lack of notice.

Statutory background

As mentioned above there are several federal laws regulating surveillance in the United States. These have to be employed together with 4th Amendment requirements, meaning that for example a warrant can be issued in accordance with laws but still unconstitutional under the 4th Amendment. After *Katz* Congress enacted Title III of the Omnibus Crime Control and Safety Streets Act[169] also known as the Wiretap Act. This act regulated domestic surveillance and included provisions like an extended time limit for continuous wiretapping (30 days). The number of authorized wiretaps has grown from 174 in 1968 to 3194 in 2010.[170] However, the act was silent about foreign activities and national security-related intelligence. Its "extension" to electronic communications, ECPA, was passed a few years later, covered surveillance for law enforcement purposes and domestic intelligence activities.

As there was a need to regulate foreign intelligence in 1978 the above mentioned FISA was passed by Congress to regulate electronic surveillance of acts of foreign origin. It was also a reaction to the widespread surveillance practices revealed in the Watergate scandal by the so-called Church Committee.[171] The act established a special court to issue orders composed of 11 judges, the Foreign Intelligence Surveillance Court (FISC) and a review court in case the government wants to appeal a denied order. However, the standard for the issuance of an order is essentially different from ordinary criminal investigations' "probable cause" standard. Although the act requires "probable cause" but not that there is criminal

[168] *Id.* at 60.
[169] The Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351, 42 U.S.C. s3711.
[170] Title III Electronic Surveillance 1968-2010 compiled by EPIC: http://epic.org/privacy/wiretap/stats/wiretap_stats.html [2011-11-10].
[171] An 11-member investigating Committee lead by Sen. Frank Church: http://www.pbs.org/moyers/journal/10262007/profile2.html [2011-11-22].

activity involved but that the object of surveillance is a *"foreign power"* or *"an agent of a foreign power"*.[172] Therefore federal officers have to ascertain the identity of the object or person, which can be *inter alia "a foreign-based political organization", "a group engaged in international terrorism or activities in preparation therefor",* or can mean *"acts in the United States as an officer or employee of a foreign power"*.[173] It can be clearly seen that this provision is easy to abuse by the government for domestic crime prevention purposes without the general strict standards. Also, under FISA surveillance activity can be continued up to 120 days or one year depending on the target and there is no notification requirement. The constitutionality of FISA came under review in the lower court case of *Duggan.*[174] The Court of Appeals found that FISA adequately balances *"the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information"*.[175] However, it is still not clear why foreign and domestic surveillance should be handled differently, especially in the presence of global terrorism.

The PATRIOT Act made substantial changes to several statutes, including ECPA and FISA that concern surveillance. In addition to changes mentioned in the previous chapter and above, these included the (1) expansion of FISA, (2) making access easier to stored wiretap communications and (3) "roving" surveillance. First, the scope of FISA was expanded by s218 of the PATRIOT Act, which simply replaced the previously existing primary purpose rule (the purpose of investigation was gathering of foreign intelligence) with *"a significant purpose*". This change entails that the lower standards of FISA for obtaining an order can be used by law enforcement if they prove that information they want to obtain is connected somehow with foreign agents or powers. Secondly, the regulation of stored wiretap

[172] FISA, s1801(a) and (b).
[173] *Id.*
[174] *United States v. Duggan* 743 F.2d 59 (2nd Cir. 1984).
[175] *Id.* at 73.

communications, which had previously fallen under the Wiretap Act were shifted to the Stored Communications Act[176] with s209 of the PATRIOT Act. This means that law enforcement officers can simply access them since it is no longer considered to be an interception. Thirdly, s206 of the Act allowed for the interception of communications beyond "*specified persons*" by inserting "*in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons*".

Surveillance in the case law of the European Court of Human Rights

Basic safeguards

As surveillance is an invasive conduct it interferes with the fundamental right to private life, which together with respect for family life, home and correspondence is protected by Article 8 of the European Convention on Human Rights. The right to privacy is not formulated as an absolute right; the possible limitations are enlisted in the second paragraph:

> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

These limitations are examined by the Court in a cumulative way, i.e. first it is verified whether (1) there was an interference with the right in question, then (2) if it was in accordance with the law and if (3) it was necessary in a democratic society for the above mentioned reasons. This cumulative approach means that if there is no legal basis for the

[176] *Stored Communications Act* 18 U.S.C. s1701.

conduct of surveillance or if the quality of that law is not appropriate according to the standards of the Court,[177] the "necessity" requirement will not be examined.[178] However, some critics argue that this overemphasizing of the "legality" aspect leads to the "*formalisation and depoliticisation of human rights questions*"[179] which might bring the erosion of those rights.

Nevertheless, it is important that the second criteria, i.e. "in accordance with the law", "*does not only refer back to domestic law but also relates to the quality of the law*".[180] Therefore the Court has devised its own criteria for assessing the quality of legislation on surveillance. As laid down in one of the first cases, *Klass and others v. Germany,*[181]

> "*domestic legislature enjoys certain discretion* [however] *this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance*".[182]

Therefore there must be adequate and sufficient safeguards against abuse, which entails that the law must be foreseeable. The safeguards that should be set out in law are:

1) The nature of the offences which may give rise to an interception order;
2) a definition of the categories of people liable to have their telephones tapped;

[177] See the standards in detail below.
[178] "*The interference with the Article 8 rights of the applicants was therefore not »in accordance with the law« within the meaning of paragraph 2 of that provision. This conclusion obviates the need for the Court to determine whether the interference was »necessary in a democratic society« for one of the aims enumerated therein (see Malone, p. 37 para 82, Kruslin, p. 25 para 37, Huvig, p. 57 para 36, and Khan para 28, all cited above)*". Association for European Integration and Human Rights and *Ekimdzhiev v. Bulgaria* (2008) (62540/00) para 93.
[179] Hert & Gutwirth, *supra* note 115.
[180] *Malone v. the United Kingdom* (1984) (8691/79) para 67.
[181] *Klass and others v. Germany* (1978) (5029/71) – it is interesting to notice that although the case was decided in 1978, the Court invokes the very two reasons that are invoked today as justifying more extensive surveillance, i.e. technological progress and terrorism: "*The first consist of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years.*" (para 48).
[182] *Id*, at para 49 [by author].

3) a limit on the duration of telephone tapping;

4) the procedure to be followed for examining, using and storing the data obtained;

5) the precautions to be taken when communicating the data to other parties; and

6) the circumstances in which recordings may or must be erased or the tapes destroyed.[183]

The section will examine these safeguards through several ECHR cases, including the most recent ones on surveillance. *Ekimdzhiev (2008)*[184] concerned Bulgarian while *Iordachi (2009)*[185] covered Moldavian legislation on surveillance; from the two German cases *Weber and Saravia (2000)* dealt with an admissibility decision while *Uzun (2010)*[186] concerned the use of GPS for surveillance by law enforcement authorities. In addition, the UK case of *Liberty (2008)*[187] covered allegations by civil rights organizations of government surveillance whilst *Kennedy (2010)*[188] was a decision upholding the lawfulness of the Regulation of Investigatory Powers Act (RIPA) 2000.

Foreseeability

The first standard the Court generally examines is the foreseeability of the law in question. Foreseeability requires that the law is formulated with sufficient clarity so that it can be indicative as to which are the circumstances under one is exposed to the possibility of surveillance. Although the law has to be accessible to everyone, the Court assured that foreseeability "*cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*".[189] On the other hand, it does serve the purpose of protecting an individual against arbitrary

[183] *Weber and Saravia v. Germany* (2000) (54934/00) para 95.
[184] Association for European Integration and Human Rights and *Ekimdzhiev v. Bulgaria* (2008) (62540/00).
[185] *Iordachi and Others v Moldova* (2009) (25198/02).
[186] *Uzun v. Germany* (2010) (35623/05).
[187] *Liberty and others v the United Kingdom* (2008) (58243/00).
[188] *Kennedy v. the United Kingdom* (2010) (26839/05).
[189] *Id*, at para 93.

interference by the separation of powers, i.e. by circumscribing the authority and defining the role of both the executive and the judge in deciding on surveillance measures. The insistence on the law being particularly precise is easier to understand in light of the availability of new and constantly changing technologies: it always has to be determinable whether a new technology is governed by the statute or not. Yet, we cannot fully dispose of the judicial interpretation of laws as it constitutes an important part of the criminal law system.[190]

However, the Court refined the foreseeability requirement in face of the threat of terrorism in the case of *Kennedy*. This meant the relaxation of requirements for the purpose of reasonableness. The Court argued that "*the condition of foreseeability does not require States to set out exhaustively by name the specific offences*".[191] Therefore invoking "national security" as a reason for interference or the targeting of "serious crimes" were considered sufficiently clear notions to justify surveillance as they are "*both frequently employed in national and international legislation*".[192] This indicates that the Court has drawn a line in surveillance cases up until which it is willing to interfere with the domestic security practices of states and beyond that states have a "margin of appreciation"-like[193] freedom. It is not surprising, however, that this line was drawn when faced with national security interests and means that the Strasbourg Court does not want to interfere with the sovereignty of states to a greater extent.

[190] *Uzun* at para 62.
[191] *Kennedy* at para 159.
[192] I*d.*
[193] *"The term »margin of appreciation« refers to the space for manoeuvre that the Strasbourg organs are willing to grant national authorities, in fulfilling their obligations under the European Convention on Human Rights"*. In: S Greer, *The Margin of Appreciation: Interpretation and Discretion Under the European Convention on Human Rights*, 5 (2000).

Grounds

The first two criteria, i.e. "*the nature of offences that may give rise to interception*" and the "*definition of categories of people*" liable to have their communications intercepted can be merged together as the grounds of interference. In Europe there are two different types of laws regulating these grounds: either (1) the offences are enumerated or (2) the types of criminal sanctions are enlisted ("serious offences", "very serious offences" etc.). The German law on the Restrictions on the Secrecy of Mail, Post and Telecommunications (hereinafter the "G10 Act"), which in light of the case law on surveillance can be considered one of the most detailed and precise laws in Europe providing safeguards against the interception of communications, enumerates each and every offence and this list is occasionally reviewed by the German Constitutional Court. In Austria the differentiation is made according to the length of possible sentences, whilst in the United Kingdom and in Hungary there is a "mixed solution": certain types of offences are listed but at the same time a category of crimes resulting in more severe sentences is also set out.[194]

Limiting the duration of permissible surveillance also serves the purpose of protection since it ties the hands of the executive by fixing the boundaries of interference into private life. Usually there is a fixed time limit within which the warrant is valid that can be renewed only once. The G10 Act sets 3 months as the limit which can be renewed for an additional three months by a new application if the statutory conditions are still met.[195] In the United Kingdom, the validity of a basic warrant is 3 months also, however, if the case at question threatens national security or the economic well-being of the country, it is doubled to 6

[194] 2/2007 (I.24) AB határozat (Decision of the Hungarian Constitutional Court, 2007).
[195] Gesetz zur Beschränkung des Brief-, Post- under Fernmeldegeheimnis (Restrictions on the Secrecy of Mail, Post and Telecommunications Act or "G10 Act", 2001) section 4.

months.[196] After the previously set conditions have ceased to exist, or if the desired aim have been reached or the warrant have proven fruitless, the interception has to end.

These seem to be rather clear and fixed limits on interference. However, in surveillance cases the Court does not only follow the "legality" requirement as described above but takes into account whether the law is effective or it can be circumvented. This is what happened in *Ekimdhziev* when the Court looked at the number of warrants issued to see if there is reasonable suspicion that surveillance is overused. Also, in the case of *Iordachi* the Court found that although the warrant was valid for 6 months nothing prevented the authorities to apply for a new warrant after the end of the 6 month-period. This resulted in unclear circumstances and the possibility of continuous surveillance. Since the grounds were not clearly set out either the Court ruled that Moldovan law did not provide adequate protection against interference.

Procession of data

The last three criteria, i.e. the use of data and its destruction, can also be merged under the title of processing the obtained data. The Court requires states to set out a scheme of clear rules on what happens with the data and who has access to it in each and every phase. These rules have to be accessible to the public therefore it is not enough that they exist in the internal codes of conduct of the authorities. The Court emphasized by referring to the G 10 Act as an example in *Liberty*, that the fact that these rules are publicly accessible does not damage "*the efficacy of the intelligence-gathering system or given rise to a security risk*".[197]

[196] Regulation of Investigatory Powers Act 2000 (RIPA 2000), section 9(6). Originally it was two months but the Labour Government extended it. Aradau & Munster, *supra* note 5.
[197] *Liberty* at para 68.

A special aspect of the use of obtained data is purpose limitation or the limitation on its transmission to other authorities. The Court recalled the decision of the German Constitutional Court in *Weber,* which quashed certain parts of the G 10 Act by arguing that

> *"[t]he transmission of data constituted a further serious interference with the secrecy of telecommunications, because criminal investigations could be instituted against persons concerned by the interception of telecommunications which had been carried out without any prior suspicion of an offence."*[198]

This means that the information obtained cannot be used for criminal investigation against a third person even if it gives rise to considerable suspicion, without a new warrant. The separation of powers is a relevant issue here as well since the executive should not have an exclusive role in deciding over the material but judicial or other independent oversight is required. Therefore in the case of *Ekimdzhiev* the Court found that the Bulgarian law on surveillance violated Article 8 since the Minister of Internal Affairs had exclusive control over the processing and use of intercepted material. However, there is not always need for judicial oversight, an independent body can be deemed sufficient as well. This is why in the case of *Kennedy* for example, the Court found that the existence and operation of the Interception of Communications Commissioner provided enough safeguard against any violation of the purpose limitations.

Additional safeguards

Although not set out explicitly in the list of safeguards there are some additional elements that the Court is examining before, during and after the completion of an interception. Such are exceptional situations when there is an "urgent need" for the carrying out of interception and there is no time for judicial authorization. To avoid abusing this time frame, usually it is

[198] *Weber* at para 40.

set rather short in the relevant law, e.g. 24 hours.[199] However, there are some countries where it can be longer, such as in the United Kingdom, where the executive has 5 days to ask for an authorization.[200] It is obvious that the longer the period is the more prone it is to any kind of abuse on the side of law enforcement authorities.

In the course of interception the possibility of external control is also important. This oversight can be done either by an independent body with the required powers or each and every individual might be given the possibility to check whether he or she was under surveillance. However, the latter is a rare option, which is usually not provided for in the law of most European countries. In Germany recourse might be had to the G10 Commission, but for example in Bulgaria the collected material constitutes state secret and therefore it would constitute a crime to inform the persons under surveillance even after the completion of the interception.[201] Although there is no notification requirement in the United Kingdom, there is a possibility of having recourse to an impartial body called the Investigatory Powers Tribunal (IPT). Persons believing to have been intercepted can complain to the IPT and it has the powers to quash the interception orders or order the deletion of already collected materials.[202] Therefore the Court ruled in *Kennedy* that the notification requirement has been "substituted" to a great extent in the United Kingdom by the IPT. The German law provides the possibility for external control during and after interception as well, since the G10 Commission and a parliamentary board made up of MPs have oversight over the monitoring measures: the minister has to report every month to the Commission and every six months to the parliamentary board.[203]

[199] See inter alia *Ekimdzhiev* or *Iordachi*.
[200] RIPA 2000 9(6).
[201] *Ekimdzhiev* at para 90.
[202] *Kennedy* at para 89.
[203] G10 Act 2001, section 5.

The availability of effective remedies is also crucial in surveillance cases. Notification after completion is important to be able to seek redress, yet,

> *"[a]ccording to the Court's case-law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy".*[204]

Therefore the Court recognized that secrecy is an inherent part of the process. Nevertheless, they also argued in this case that as soon as the interception is over and persons concerned can be notified without jeopardizing the results or risking uncovering the methods used it should be done in a reasonable time.

Conclusions

Surveillance in modern societies has become a widespread practice. The chapter juxtaposed European and United States legislation and practice in this field, which interferes with the individual's private sphere to a great extent. First, to be able to position modern day surveillance regulation an overview was given of the field of privacy and the emergence of surveillance laws. The notion of privacy and privacy protection is different on the two sides of the continent. The ambit of 4th Amendment jurisprudence is much narrower than that of the ECHR's right to privacy and formulates privacy rather as isolation and secrecy. Another difference is that the limitations of the right are clear in the jurisprudence of the Strasbourg court since they are listed in Art. 8(2) while US courts are not provided with similar "help".

[204] E*kimdzhiev* at para 90.

However, as we have seen above similar balancing has to be done by the court between individual privacy and public security in terrorism-related cases.

The handling of law enforcement surveillance evolved to be similar in both cases. Although in this case it is 4th Amendment requirements that have clearly solidified in jurisprudence, i.e. the need for probable cause, a warrant and the definition of the object of search or surveillance (particularity); ECHR legislation is also evolving towards similar standards. As it could be seen from the cases above, the Strasbourg Court thoroughly examines the domestic law on surveillance and looks for certain recurrent characteristics. These include the foreseeability and clarity of the law, safeguards concerning warrants, notification, etc.[205] Statutory regulation in the US and in European countries, such as the UK spelled out requirements that were not always satisfactory from a human rights point of view and did not restrain surveillance to a sufficient extent. At the same time, courts have been often unwilling to interfere, claiming this to be the area of national security, for example in the case of NSA's warrantless surveillance program or in the *Kennedy* case above.

The emergence of global terrorism has influenced the sphere of surveillance in both sides of the continent. In the case of the United States this influence has been clearly attributable to the 9/11 attacks as the PATRIOT Act has relaxed several safeguards in existing legislation. Concerning Europe the proportion in the influence of the terrorist attacks cannot be measured based on the cases discussed above. In the UK the lawfulness of RIPA 2000, which still governs the field of surveillance and symbolizes some kind of continuity between the pre- and the post-9/11 era, was upheld by the Strasbourg court. What is noticeable from the approach of the ECtHR is that they are cautious when faced with questions of national security and willing to show a deferential attitude. Although it is true

[205] For an overview of the different requirements in the above mentioned cases see Annex 1.

that this is a general approach to matters of state sovereignty and cannot be attributed to the rise of terrorism, it still does not change the fact that this way the government is given a broader discretionary power and therefore an uncontrolled hand in the sphere of surveillance.

III. A Reconstruction of the Body through Security Practices?

"Over himself, over his own body and mind, the individual is sovereign"[206]

We more or less have come to accept that we have to pass through large "magnetic doors" to get to our flights, leave all liquids and sharp objects outside or endure thorough pat-down searches from airport officials. However, airport security techniques are becoming more and more sophisticated and their privacy implications are changing as well. This chapter will address the introduction of biometric identifiers or more specifically body scanners, since it raises questions not only about their impact on civil liberties but also about possible influences on underlying concepts and perceptions of our body. According to the National Science and Technology Council biometrics as a process constitutes of *"[a]utomated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics"*.[207] Biometric technology makes possible identification by the distinguishing characteristics or traits of a person such as fingerprints, iris, facial features as well as behavioral characteristics (gait, micro gestures).

The tragic events of 9/11 have transformed airports into extraordinary places where exceptional measures are employed to ensure the security of ordinary citizens. Airports are exceptional from two aspects: they are at the same time "non-places" of transition[208] and the premises of the attacks. This "double exceptionality" is entwined with the preemptive logic of security practices: in the age of surveillance the goal of security checks is to "*prevent particular futures from coming true*".[209] The aim of the present chapter is to analyze privacy

[206] J S MILL, ON LIBERTY 6 (Penguin Books ed. 1982).
[207] *Biometrics Glossary*, NATIONAL SCIENCE AND TECHNOLOGY COUNCIL - SUBCOMMITTEE ON BIOMETRICS (2006), http://biometrics.gov/documents/Glossary.pdf [2011-11-01].
[208] M B Salter, *Governmentalities of an Airport: Heterotopia and Confession*, INTERNATIONAL POLITICAL SOCIOLOGY 1 (2007).
[209] P Adey, *Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body*, 27 ENVIRON. PLANN. D 274, 275 (2009).

challenges and problems stemming from the use of a special biometric technology, body scanners and address to what extent the conception of our body is being changed as a result of biometric security measures. To demonstrate the current state of play, the legislative background of biometric identification and security practices of the United States and the European Union will be described. Afterwards some of the problems associated with biometrics and their interference with privacy will be addressed. The question is whether body scanners are only simple methods that enhance our security and effectiveness at the same time or they point towards a new perception of the body currently under construction that might entail other unintended and fundamental consequences.

Body Scanners in the United States

Congress reacted promptly to the terrorist attacks of 9/11 and enacted the Aviation and Transportation Security Act (ATSA) on November 19, 2001. This resulted in tighter security regulations on airports including the "*the use of voice stress analysis, **biometric**, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft*".[210] It also established the Transportation Security Administration (TSA) responsible for overseeing the installation of airport security technologies.

In the framework of ATSA there are different programs connected to biometric technologies. The use of Advanced Imaging Technology (AIT), i.e. body scanners, creates a photo of the full body and highlights objects on it.[211] These images "*are not equivalent to photography and do not present sufficient details that the image could be used for personal*

[210] Aviation and Transportation Security Act of 2001 Public Law 107-71, s109(a)(7) (emphasis by author).
[211] There are two different technologies currently employed: millimeter wave, which uses radio frequency energy and backscatter X-ray using low energy X-ray beams. For a comparison and possible health consequences see: http://www.tsa.gov/assets/pdf/ait_fact_sheet.pdf [2011-11-24].

identification".[212] That also means that parts of the body such as the face or genitalia are blurred and "*[a]nonymity is preserved by physically separating the image operator from the individual undergoing screening*".[213] Although the technology is often compared to a "virtual strip-search",[214] claimed to make discrimination possible on the basis of sex or by revealing medical conditions (e.g. breast implants might be visible) and it brings in the "human element" (unlike the magnetometer that is a machine), it is at the same time a preferred method to pat down searches, four out of five Americans support their use.[215]

Another special program that employs biometrics is the so called SPOT (Screening of Passengers by Observation Techniques (SPOT). This program takes passenger surveillance to a new level by employing specially trained officials called BDOs (behavior detection officials) to focus on the behavioral patterns and peculiarities of those travelling. They conduct further interviews with those who display suspicious micro gestures such as "*involuntary physical and physiological reactions that may indicate stress, fear or deception regardless of race, gender, age, or religion*".[216] Electronic records of detected behavioral patterns are retained for 15 years anonymously in a SPOT database and this way create an imprint of how people behave at a given time in a given place. However, the impact assessment assured that the data stored in the database could not be linked to other personal characteristics (such as age, color, etc.).

[212] *Privacy Impact Assessment Update for TSA Advanced Imaging Technology* (Department of Homeland Security, January 2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf [2011-11-10].
[213] *Id.* at 6.
[214] ACLU In: T W Mock, *The TSA's New X-Ray Vision: The Fourth Amendment Implications of "Body-Scan" Searches at Domestic Airport Security Checkpoints*, SANTA CLARA LAW REVIEW 213, 12 (2009).
[215] *Poll: 4 In 5 Support Full-Body Airport Scanners*, CBS News , http://www.cbsnews.com/8301-503544_162-20022876-503544.html [2011-11-01].
[216] *Privacy Impact Assessment for the Screening of Passengers by Observation Techniques (SPOT) Program* (Department of Homeland Security, August 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_spot.pdf [2011-11-01].

The use of body scanners has implications under the 4th Amendment, and as stated in the previous chapter has a three-prong requirement: (1) probable cause, (2) a warrant and (3) particularity of search or seizure. Yet, there are some cases when search without a warrant is not unconstitutional *per se* including administrative searches, the Terry rule and consent to search. As mentioned above, administrative searches are "*conducted as part of a general regulatory scheme in furtherance of an administrative purpose*",[217] whilst Terry stops are applied when police has a "reasonable suspicion" that the person is involved in criminal activity.[218]

Since *Katz* we also know that to be able to claim a violation of Fourth Amendment rights there (1) has to be a subjective expectation of privacy and that (2) it has to be considered reasonable by society. Although regarding administrative searches for example, the expectation of privacy is generally considered to be reduced, the reasonableness prong still has to be satisfied, i.e. there has to be a compelling governmental interest that outweighs privacy implications.[219] In the case of terrorist threats, however, this is easy to find: "*It is »obvious and unarguable« that no governmental interest is more compelling than the security of the Nation*".[220] Nevertheless, the search still has to be narrowly tailored and consent is implied generally by a passenger boarding the plane. At the same time, it is disputed by some scholars whether those who do not want to go through a privacy intrusive search have sufficient choice since not flying is their only other option.[221] Although TSA offers pat-down searches as an alternative to those who object to body scanners, a privacy rights organization, the Electronic Privacy Information Center (EPIC) argued in their petition

[217] *United States v Davies*, 482 F.2d 893, 9th Circuit (1973).
[218] *Terry v. Ohio*, 392 U.S. 1 (1968).
[219] E P Haas, *Back to the Future? The Use of Biometrics, Its Impact on Airport Security, and How This Technology Should Be Governed*, Spring JOURNAL OF AIR LAW AND COMMERCE 459 (2004).
[220] *Haig v Agee*, 453 U.S. 280, 307 (1981).
[221] Mock, *supra* note 213.

filed against the Department of Homeland Security that many people are not informed or this option or it is used as a "retaliatory" method.[222]

Body Scanners in the European Union

The framework of aviation security methods to be adopted by all 27 member states of the Union can be found in Regulation 300/2008 on common rules.[223] This document lays down that member states should have an airport and an air carrier security program but does not define their scope more precisely, moreover it ensures that if countries are willing to they can employ more stringent measures. The case is different with passports since from 2004 with Regulation 2252/2004[224] all EU members have to introduce biometric passports, the reasons being inter alia to "*align themselves with relevant US legislation*".[225] However, it has to be noted that the use of fingerprints in these documents can be problematic. The long history of criminal investigations entail that there is a stigma of criminality attached to fingerprints and in addition, there is research indicating that they might reveal male homosexuality.[226]

Biometric technology is applied on EU-wide level in the case of border control and immigration. Eurodac, the central database that collects the fingerprints of asylum seekers; VIS and SIS II, the common Visa and Schengen Information Systems collect and retain

[222] *EPIC V. DHS, No. 10-1157,* EPIC.ORG (July 02, 2011), http://epic.org/EPIC_Body_Scanner_OB.pdf [2011-11-15].
[223] Council Regulation (EC) No 300/2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L 97/72 (2008).
[224] Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385 (2004).
[225] *Integration of biometric features in passports and travel documents,* Europa.eu. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14154_en.htm [11-05-2011]
[226] G. Star, *Airport Security Technology: Is the Use of Biometric Identification Technology Valid Under the Fourth Amendment?,* 20 TEMPLE ENVIRONMENTAL LAW AND TECHNOLOGY JOURNAL 251 (2002).

biometric data and at the moment there are calls for interoperability between the systems.[227] The main problem with the use of biometric identifiers on EU-level can be summarized around three topics: (1) technical issues, that the current infrastructure is unreliable and therefore it is exposed to errors and failures, (2) political problems, i.e. a lack of inter- and intra-agency cooperation and (3) a communication deficit about who "*drives the agenda*" governments or private corporations, EU interests or those of the US.[228]

Although the EU had wanted to create common rules on the use of full-body scanners too this attempt met considerable resistance from the beginning.[229] Member states were free to implement laws on domestic airport security as long as they were in compliance with general EU human rights norms. These norms are collected in the Charter of Fundamental Rights from which the use of body scanners challenges the right to dignity (Art 1), the right to integrity of person (Art 3) and the protection of personal data (Art 8 and the Data Protection Directive. According to the latter the subject of a processing of personal data has a right of "informational self-determination",[230] i.e. to be notified of the act or to have the data rectified or corrected. As mentioned above, there are also rules on the use, storage and destruction of collected materials, nevertheless, in the framework of the Stockholm Programme[231] it was declared that the "*Internal Security Strategy affirms participation and prevention through cross-agency cooperation*".[232] Therefore information collected on

[227] A. Sprokkereef & P De Hert, *Ethical Practice in the Use of Biometric Identifiers Within the EU*, 3 LAW, SCIENCE AND POLICY 177 (2007).
[228] D Lyon, *Biometrics, Identification and Surveillance*, 22 BIOETHICS 499, 503 (2008).
[229] E. Lombard, *Bombing Out: Using Full-Body Imaging to Conduct Airport Searches in the United States and Europe Amidst Privacy Concerns*, 19 TULANE JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 1 (2010).
[230] J. Lodge, *Quantum Surveillance and `Shared Secrets' A Biometric Step Too Far?*, CENTRE FOR EUROPEAN POLICY STUDIES 1 (2010).
[231] The program governing the field of justice and home affairs in the European Union between 2010-2015.
[232] Lodge, *supra* note 229, at 4.

European and non-European citizens is to be shared between different police and security agencies, which might go contrary to purpose limitations.[233]

However, after a long debate an implementing regulation was adopted on the use of body scanners very recently. Regulation 1147/2011[234] that comes into force December 2011 aims to lay down the specific conditions of the use of body scanners and "*by providing passengers with the possibility to undergo alternative screening methods* [it] *respects fundamental rights*".[235] It adds security scanners that do not use ionizing radiation to the list of screening devices, next to strip-search and metal detectors and specifies that the machines shall not "*store, retain, copy, print or retrieve images*",[236] the human reviewer of the images shall be in a separate location, the image shall be blurred to preserve anonymity and passengers should be notified of the screening process beforehand.

Countries that currently employ body scanners in the European Union include the Netherlands and the United Kingdom. In the UK machines were deployed at Heathrow, Gatwick and Manchester airports after a failed attempt by a Nigerian man to blow up an aircraft leaving from Amsterdam.[237] Although there is an Interim Code of Practice for the use of body scanners,[238] which lays down the same rules as the EU regulation on body scanners and the government has started consultations on a permanent one, there is a major difference

[233] The principle that information can be used only for the legitimate purpose collected, and this purpose cannot be specified later than the time of the data collection. In: LIBE, *supra* note 13.
[234] Commission Implementing Regulation (EU) No 1147/2011 amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports.
[235] *Id.* preamble [added by author].
[236] *Id.* at Annex (3).
[237] Profile: Umar Farouk Abdulmutallab, *BBC News*, 12 October 2011. http://www.bbc.co.uk/news/world-us-canada-11545509 [2011-11-24].
[238] *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment*, DEPARTMENT FOR TRANSPORT (January 2010), http://assets.dft.gov.uk/publications/interim-code-of-practice-for-the-acceptable-use-of-advanced-imaging-technology-body-scanners-in-an-aviation-security-environment/cop.pdf.

with EU and US regulations: the transport minister told media that UK passengers will not be given the possibility to choose an alternative pat-down search.[239]

Privacy Implications of Body Scanners

Who are we, if we are not our body? And what is our body without us?[240]

As the analysis of the legislative background of the United States and that of the European Union has shown, the introduction of biometrics has the slippery rationale of prevention. This is problematic since, as analyzed above in connection with counter-terror and surveillance legislation, it can often result in vague and overbroad laws with the risk of their becoming permanent. The introduction of body scanners was part of this rationale, nevertheless, the main question at the moment is whether they are prone to abuse and constitute a risk to privacy rights. The main concerns are collected in this chapter below.

The most obvious concerns are related to the operation of the scanners. By revealing the outlines of the body, as mentioned above airport officers expose the individual to a "virtual strip-search". First, this can reveal sensitive medical information such as breast implants, catheter tubes, adult diapers etc. or simply expose atypical body shapes. It can also interfere with religious beliefs (e.g. Muslims covering their bodies). Second, the inclusion of the "human element", i.e. the reviewer can aggravate the situation. Although it is clearly stated both in the TSA's policy and in EU regulation that the reviewer has to be separated from the screened individual so as not to make identification possible, this rule itself opens the way for data protection concerns. As the officer is separated in a cubicle it cannot be

[239] T ESPINER, *UK Airport Body Scans Will Not Be Opt Out*, ZDNET (November 23, 2011), http://www.zdnet.co.uk/news/security-threats/2011/11/23/uk-airport-body-scans-will-not-be-opt-out-40094486/.
[240] E Mordini & S Massari, *Body, Biometrics and Identity*, 22 BIOETHICS 488, 494 (2008).

made sure that he/she does not make a copy of the image for personal use (by a cell phone for example).[241] Privacy rights organizations also warned that the "blurring" feature in the scanners is only a software fix and that originally the devices were developed to store, record and transmit images therefore there are no guarantees that governments would not use these features when needed.[242]

The privacy-invasive nature of screening is also problematic because according to a group of 30 civil rights organizations[243] it goes contrary to the presumption of innocence. As mentioned above, lack of a warrant or probable cause results in the violation of the 4th Amendment save in the few exceptions. While administrative searches in airports constitute an exception since *Davis,*[244] they still have to satisfy the general reasonableness prong. The organizations claim that as body scanners represent a very privacy-invasive search, "reasonable suspicion" is needed for a passenger to be scanned and they cannot be used routinely. Otherwise there is a chance that as in the case of fingerprints in biometric passports there is a stigma of criminality attached to the search.

The proportional relationship between the invasiveness of the screening and the result to be achieved i.e. the prevention of an attack, is also questionable. Both American and European organizations claim that the effectiveness of body scanners is debatable and probably they would have failed in filtering out the 2009 Amsterdam attempt.[245] Also there

[241] Mock, *supra* note 213.
[242] EPIC V. DHS, NO. 10-1157, *supra* note 221.
[243] W FISHER, *Privacy Groups Challenge U.S. Airport Body Scanners*, INTERPRESS SERVICE (April 22, 2011), http://ipsnorthamerica.net/news.php?idnews=3012 [2011-11-18].
[244] *Davies*, para 63: *"a screening of passengers and of the articles that will be accessible to them in flight does not exceed constitutional limitations provided that the screening process is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to fly".*
[245] See inter alia: *ACLU Backgrounder on Body Scanners and "Virtual Strip Searches,"* AMERICAN CIVIL LIBERTIES UNION (January 08, 2010), http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches; EPIC V. DHS, NO. 10-1157, *supra* note 215;

are doubts as to the feasibility of building an effective line of protection because of the cost of scanners and additional personnel involved.[246] Hence the balance between the individual harm and national security interests cannot be properly evaluated.

It is not surprising therefore that the proliferation and use of body scanners was challenged by civil rights organizations. In the UK Liberty voiced its concerns in a contribution to the Department of Transport's consultation process on body scanners.[247] Before going into details on privacy harms they noted that as the text of the Direction setting out the rules on the use of body scanners is not public for reasons of national security, the government is in breach of the Human Rights Act and ECHR jurisprudence since they did not fulfill the Art. 8 criterion of "in accordance with the law".[248] After this Liberty went on to address necessity and proportionality requirements in Strasbourg manner and found that the lack of an alternative method disproportionately affects an individual's right to privacy. They also added that consent could no longer be truly implied by buying a flight ticket, as people are not notified in an early stage about the nature of the search.

In the United States the challenge to the deployment of the machines went further and EPIC initiated a lawsuit against the TSA arguing that body scanners resulted in "*the most sweeping, the most invasive, and the most unaccountable suspicionless search of American travelers in history.*"[249] They brought claims under the Administrative Procedure Act,[250] the Privacy Act, the Video Voyeurism Prevention Act, the Religious Freedom Restoration Act

---

Liberty's Response to the Department of Transport's Consultation on the Code of Practice for the Acceptable Use of Advanced Imaging Technology (body Scanners) in an Aviation Security Environment, LIBERTY (July 2010), http://www.liberty-human-rights.org.uk/pdfs/policy10/liberty-s-response-to-the-body-scanners-consultation-july-2010.pdf.

[246] A machine costs approximately $200.000 In: ACLU BACKGROUNDER ON BODY SCANNERS AND "VIRTUAL STRIP SEARCHES," *supra* note 238.

[247] LIBERTY, *supra* note 239.

[248] For an identical breach addressed before the Strasbourg Court see *Gillan and Quinton* above.

[249] EPIC V. DHS, NO. 10-1157, *supra* note 215, at 20.

[250] Administrative Procedure Act of 1946, Public Law 79-404, 5 U.S.C. s500.

(commonly referred to as RFRA)[251] and the 4th Amendment. EPIC argued that (1) the TSA violated its duties under the Administrative Procedure Act when they failed to initiate a consultation phase before installing the scanners. They also (2) failed to comply with the requirements of the Privacy Act given that the program resulted in the keeping of a "*system of records*"[252] and (3) violated the Video Voyeurism Prevention Act by capturing images of people of a private nature where they have a reasonable expectation of privacy. As RFRA provides that compelling government interest is needed with the least restrictive means employed, the (4) government here failed to pass the compelling interest test and offended the sincerely held beliefs of modesty by Muslims. EPIC also claimed a (5) violation of the 4th Amendment on the grounds of the search being unnecessarily invasive. However, the United States Court of Appeals for the District of Columbia Circuit in July 2011 upheld the lawfulness of body scanners and ruled that the TSA violated only the "*notice-and-comment rulemaking*" of administrative procedures.[253] EPIC did not agree with the decision and filed a complaint for rehearing claiming that the Court "*overstated the ability of the body scanners to detect threats to aviation security and understated the privacy intrusion to air travelers*".[254]

A different strand of reasoning in privacy literature concerns the fate of information collected in the process. First, the danger of a technology being used for purposes other than it was developed, or the so-called "function creep", [255] is a relevant problem in our debate as well. We might not want body scanners in our workplace or in the shop. Second, apart from

[251] Religious Freedom Restoration Act of 1993, Public Law 103-191, 41 U.S.C. s2000bb.
[252] EPIC V. DHS, NO. 10-1157, *supra* note 221, at 4.
[253] *Electronic Information Privacy Center et al. v. United States Department of Homeland Security et al.*, 653 F.3d 1, 26 (2011).
[254] EPIC.org, *Top News*. http://epic.org/privacy/body_scanners/epic_v_dhs_suspension_of_body.html [2011-11-26].
[255] E Mordini & C Petrini, *Ethical and Social Implications of Biometric Identification Technology*, 43 ANN IST SUPER SANITA 5 (2007).

the use of technology, the use of its "fruits" pose a different problem. The use of body scanners, if not carefully circumscribed, can result in the creation of databases. These databases contain the imprint of our physical bodies and our behavioral patterns and some scholars fear that the existence of them might have further consequences. They argue that at some point information ceases to be information only, loses it body and starts living its own life by constructing our "data doubles".[256] At the same time they also claim that the collection of such data into databases dehumanizes and "disembodies" the data from its subjects and "*animalize[s] the body into its prereflective and unconscious bodily capacities to affect and to be affected*".[257] This way it threatens bodily integrity and dignity.

Along the same logic it can be said that these technologies not only depict but also at the same time reconstruct the body as perceived by us and by others. An unintended consequence of body scanners and biometrics in general is that they "write" the information on the body and this might affect our self-identification or at least how we are being perceived and redefined from outside, i.e. how "*the state »sees« its citizens*".[258] The body therefore is being used as a passport that has to be shown and presented when crossing borders and airports. This act, which takes place at airports and becomes necessary in the process of "confessing" who we are,[259] might be the first step in the process of a reconstruction of our identities through the "use" of our body.

Conclusions

As seen above, defenders of privacy have warned about numerous dangers surrounding the introduction of body scanners, ranging from direct, bodily privacy harms to more abstract

[256] Adey, *supra* note 208, at 277.
[257] *Id.* at 275.
[258] Lyon, *Biometrics, Identification and Surveillance*, *supra* note 227, at 507.
[259] The role of "confession" in disciplining and governing citizens as subjects is elaborated on to a greater extent in the works of Foucault. In: Salter, *supra* note 207.

problems and unintended consequences of the proliferation of the technology. However, when evaluating the unintended effects of the introduction of body scanners two arguments that are not obvious at first sight should not be left out. First, our conceptions of the body might not be that stable and unchangeable as we think therefore any argument building on it necessarily builds on a "snapshot". Second, there is nothing inherently new in this technology since the

> "*endless history of identification systems teaches us that identification has never been a trivial fact but has always involved a web of economic interests, political relations, symbolic networks, narratives and meanings*".[260]

This means that identification and the development of identification systems is a fluid process, not a stationary condition.[261]

Concerning the less abstract side of the deployment of the technology, there are also positive changes. Privacy concerns were remedied to some extent in the European Union by the above mentioned regulation laying down specific conditions for the use of body scanners at airports. It is a good direction that the regulation standardized relevant practices to be used by national authorities in a publicly accessibly form. Also, the banning of X-ray scanners by the EU because of potential health concerns was hailed as a positive step.[262] Authorities slowly seem to recognize privacy concerns in the UK and in the US as well and start developing new, less intrusive technology. The TSA announced in July that they would roll

[260] Mordini & Massari, *supra* note 239, at 497.
[261] Moreover, some scholars argue somewhat controversially that the creation of a separate public identity might lead in a sense to more freedom not less since we can "hide" behind it. They claim that with biometric identification a possibility is given to individuals to create their own identity that distinguishes them from the masses and exist above the boundaries, and this can result in the "liberation" of them form the control of the state. However, we should not forget at the same time that the boundaries of permissible definitions, i.e. what "new identities" can people choose, are still created by the state. In: Mordini & Massari, *supra* note 239.
[262] *Europe Bans X-ray Scanners*, THE ECONOMIST (November 16, 2011), http://www.economist.com/blogs/gulliver/2011/11/body-scanners-0 [2011-11-20].

out new software that shows a stick-figure body instead of the outlines of passengers,[263] while UK airport Heathrow proclaimed the installation of "privacy-friendly" scanners along the same lines.[264] This entails that initial concerns will be cured to some extent and the work of privacy "watch dogs" have had its fruits. Concerning the rhetorical question in the title of the thesis it can be concluded that although our concept of identity and body could be shaped in the future to some extent by these technologies, this process is by no means a new phenomenon. However, the construction of a "data-double" substituting us seems to be pushed to the future for the time being.

[263] *TSA Scanners Start Moving From Naked Bodies to Stick-Figure Outlines,* ACLU BLOG (July 20, 2011), http://www.aclu.org/blog/national-security-technology-and-liberty/tsa-scanners-start-moving-naked-bodies-stick-figure [2011-11-20].

[264] *Heathrow trials privacy-friendly bodyscanners,* THE GUARDIAN (September 5, 2011), http://www.guardian.co.uk/uk/2011/sep/05/heathrow-privacy-bodyscanners?INTCMP=SRCH [2011-11-20].

Summary

The thesis intended to give an overview of privacy in the post-9/11 era by describing and analyzing legislative and policy-level responses in the United States, the European Union and the United Kingdom. The initial assumption was that it is global terrorism, which shapes the field after the attacks and there are significant changes in the laws and policies of states. In addition, it was assumed that the introduced changes may have unintended consequences and influence our conceptions about the body.

In the first chapter the measures initiated after the attacks were described in light of Professor Sajo's contention that altogether they might point toward a new constitutional order.[265] The clusters of practices building up the "counter-terror state" were very similar in all three jurisdictions. They included emergency legislation and disproportionate reactions on the side of states, ranging from unnecessarily broad and vague definitions of terrorism to limits on the right to liberty materializing in detention regimes and control orders. Although the European Union is often hailed as a champion of fundamental rights, the analysis showed that while there are positive tendencies, these are not enough yet to "*check and complement*"[266] American power. Examination of UK legislation also corroborated that the vocabulary of counter-terror measures had been ready before the attacks and that measures curbing civil liberties tend to survive legislative changes and become permanent part of laws. Altogether, it can be concluded that (1) the three jurisdictions employed remarkably similar measures to counter terrorist threat and that (2) "clusters" making up a possible counter-terror order can already be seen.

The strengthening of surveillance and the emergence of a "surveillant state" as a potential consequence of the "War on Terror" was analyzed in the second chapter. As

[265] Sajo, *supra* note 22.
[266] ASH, *supra* note 52.

surveillance interferes with the right to privacy the thesis first gave an overview of the concept of privacy protection in the US and in Europe. Although it seems that 4th Amendment protection is much more focused on secrecy whilst the ambit of Art. 8 is broader, a general balancing approach is used by courts when reconciling privacy and security in both cases. Concerning the situation after 9/11, however, the thesis could not demonstrate beyond doubt that the events constituted a bright line after which the whole field of surveillance changed. While the amendments of the PATRIOT Act on surveillance legislation are significant, no such changes could be seen in Europe. However, this might be attributed to the choice of jurisdictions and it needs further research of other national surveillance laws in Europe. What the thesis established therefore was rather an intensification of surveillance with the survival of pre-9/11 legislation.

The third chapter narrowed the focus of the thesis more and analyzed the emergence and privacy implications of a new technology, body scanners. The thesis intended to examine whether the introduction of these devices was just a simple, efficiency-enhancing step or they had a much deeper, unintended consequence: the reconstruction of our body and the materialization of our "data-double". In the course of this evaluation, direct privacy-related harms and other, more abstract consequences were also addressed. According to privacy advocates, apart from a disproportionately privacy-invasive search the introduction of body scanners has resulted in the refutation of the presumption of innocence and in the possibility of "function-creep". Also, because of doubts about the efficiency of the technology it is difficult to evaluate the balance between harms to individual privacy and security concerns. Yet, at the same time it seems that some of these harms are being addressed and authorities have started to realize problems concerning privacy implications.

Altogether, the current state of play shows that body scanners as a technology can be classified neither as a simple efficiency-enhancing step nor as a completely novel feature that

result in a significant change of our perceptions of the body. However, the areas the thesis covered have revealed some consequences of the "War on Terror" on the individual that we should not underestimate: surveillance might result in the forming of new groups of suspects on the basis of beliefs or religion, while body scanners and counter-terror laws can stigmatize in general each and every citizen as criminal suspects.

Annex I.

	Nature of offences that may give rise to interception	Limits on the duration of monitoring	Length of non-authorized operational control	Procedure to check whether someone is under surveillance	Notification after completion	Review Mechanism	Remedy
KLASS v Germany	factual indications of planning, committing or having committed - democratic order. External security, security of allied forces	3 months, non-renewable - after conditions ceased to exist or no longer necessary		Recourse to G10 Commission	Not required by the ECtHR but exists	Only after, non-judicial: G10 Commission every month, Board of MP every 6months	G10 Commission +Constitutional Court
MALONE v UK	serious crime, other methods unlikely to succeed, good reason to think that interception would lead to arrest						
WEBER and SARAVIA v Germany	necessary for timely identification of (1) armed attack against Germany (2) international terrorist attack (3) international arms trafficking (4) illegal importation of drugs (5) counterfeiting of money (6) laundering of money	3 + 3 months					
EKIMDZHIEV v Bulgaria	serious offences, if there are no other means	2 months, extendable up to 6 months by fresh warrant - desired aims attained or means proves fruitless	24 hours	State secret!	No	Before: Application to a court to issue the warrant, During & After: NO	Not available

	Nature of offences that may give rise to interception	Limits on the duration of monitoring	Length of non-authorized operational control	Procedure to check whether someone is under surveillance	Notification after completion	Review Mechanism	Remedy
IORDACHI v. Moldova	national security, public order, economic situation, maintenance of the legal order or prevention of very serious offences (15yrs and more), protection of health, morals, interests of others	30 days, total duration is 6months but renewable -- aims are accomplished, or it is proven that it is impossible	24 hours	State secret!	Yes	Before: investigating judge During & After: unclear the powers of the judge	
UZUN v. Germany	sufficient gravity, other means have less prospect of success	1month, extension by only by judge	1 month in the case of GPS but approved by Public Prosecutor	G10	Yes	Same as above	Same as above
KENNEDY v. UK		3 months, national security, econ well-being: 6months	5 days				

Bibliography

BOOKS

Agamben, G. *The State of Exception*. University of Chicago Press. Chicago: University of Chicago Press, 2005.

Beck, U. *Risk Society: Towards a New Modernity*. Sage Publications. London: Sage Publications, 1986.

Garner, B A, ed. *Black's Law Dictionary*. Ninth. Thomson Reuters, 2009.

Gutwirth, S., Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt. "Reinventing Data Protection" (May 2009): 1–356.

Lazarus, L., and B J Goold. *Security and Human Rights*. Hart Publishing. Oxford: Hart Publishing, 2007.

Mill, J S. *On Liberty*. Penguin Books. London: Penguin Books, 1982.

Mills, J L. *Privacy: The Lost Right*. Oxford University Press. Oxford: Oxford University Press, 2008.

Nye, J S. *Soft Power: The Means To Success In World Politics*. PublicAffairs. New York: PublicAffairs, 2004.

Schmitt, C. *The Concept of the Political*. University of Chicago Press. Chicago: University of Chicago Press, 2007.

Solove, D J. *Understanding Privacy*. Harvard University Press. London: Harvard University Press, 2008.

Solove, D J, M Rotenberg, and P M Schwartz. *Privacy, Information and Technology*. Aspen Publishers. New York: Aspen Publishers, 2006.

Sottiaux, S. *Terrorism and the limitation of rights□: the ECHR and the US constitution*. Hart. Oxford: Hart Publishing, 2008.

Thomas,, D., and B. Loader, eds. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge, 2000.

Wilson, R Ashby. "Human Rights in the `War on Terror'" (July 2005): 1–367.

ARTICLES & OTHER

ACLU. "ACLU Backgrounder on Body Scanners and 'Virtual Strip Searches'." *American Civil Liberties Union*, January 8, 2010. http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches.

Adey, P. "Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body." *Environ. Plann. D* 27, no. 2 (January 2009): 274–295.

Allen, A L. *Uneasy Access: Privacy for Women in a Free Society*. Rowman & Littlefield Publishers. New Jersey: Rowman & Littlefield Publishers, 1988.

Aradau, C., and R Van Munster. “Exceptionalism and the ‘War on Terror’: Criminology Meets International Relations.” *British Journal of Criminology* 49, no. 5 (September 2009): 686–701.

Ash, T G. “The Peril of Too Much Power.” *The New York Times*, April 9, 2002. http://www.nytimes.com/2002/04/09/opinion/the-peril-of-too-much-power.html?src=pm.

Ball, K., and F. Webster. “The Intensification of Surveillance.” In *The Intensification of Surveillance - Crime, Terrorism and Warfare in the Information Age*, by K. Ball and F. Webster, 1-16. London: Pluto Press, 2003.

Barak-Erez, D. “Terrorism Law between the Executive and Legislative Models.” *The American Journal of Comparative Law* 57 (2009): 877-896.

Bates, E. “Anti-terrorism control orders: liberty and security still in the balance.” *Legal Studies* 29, no. 1 (2009).

“Biometrics Glossary.” *National Science and Technology Council - Subcommittee on Biometrics*, 2006. http://biometrics.gov/documents/Glossary.pdf.

Brysk, A, and G Shafir, eds. *National Insecurityand Human Rights - Democracies Debate Counterterrorism*. University of California Press. Los Angeles: University of California Press, 2007.

de Burca, G. “The European Court of Justice and the International Legal Order after Kadi.” *Harvard International Law Journal* 1, no. 51 (Winter 2010).

Clarke, P. “Learning From Experience – Counter Terrorism in the UK since 9/11.” 1–15, 2007.

DeCew, J. “The Feminist Critique of Privacy.” *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)*, 2008. http://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=privacy.

Donohue, L. “Anglo-American Privacy and Surveillance.” *The Journal of Criminal Law and Criminology* 96, no. 3 (May 2006): 1059–1208.

Elliott, M. “United Kingdom: Detention Without Trial and the War on Terror.” *International Journal of Constitutional Law* 4, no. 3 (2010).

“EPIC v. DHS, No. 10-1157.” *EPIC.org*, July 2, 2011. http://epic.org/EPIC_Body_Scanner_OB.pdf.

Espiner, T. “UK airport body scans will not be opt out.” *ZDnet*, November 23, 2011. http://www.zdnet.co.uk/news/security-threats/2011/11/23/uk-airport-body-scans-will-not-be-opt-out-40094486/.

“Europe bans X-ray scanners.” *The Economist*, November 16, 2011. http://www.economist.com/blogs/gulliver/2011/11/body-scanners-0.

Falk, R. “Encroaching on the Rule of Law.” In *National Insecurity and Human Rights - Democracies Debate Counterterrorism*, by A Brysk and G Shafir. University of California Press. Los Angeles: University of California Press, 2007.

Fisher, W. “Privacy Groups Challenge U.S. Airport Body Scanners.” *Interpress Service*, April 22, 2011. http://ipsnorthamerica.net/news.php?idnews=3012.

Garapon, A. “The Oak and the Reed: Counter-Terrorism Mechanisms in France and the United States of America.” *Cardozo Law Review* 27, no. 5 (April 2006): 2041–2077.

Garland, D. “The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society.” *British Journal of Criminology* 36 (1996): 445-470.

Goede, M De. “The politics of preemption and the war on terror in Europe.” *European Journal of International Relations* 14, no. 1 (March 2008): 161-185.

Goold, B J. “Public Protection, Proportionality, and the Search for Balance.” *Ministry of Justice Research Series*, no. 10 (2007).

Greer, S. “The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights”. Council of Europe, 2000.

Haas, E P. “Back to the Future? The Use of Biometrics, its Impact on Airport Security, and How this Technology Should Be Governed.” *Journal of Air Law and Commerce* Spring, no. 69 (May 2004): 459–489.

Hert, P De, and S. Gutwirth. “Privacy, data protection and law enforcement. Opacity of the individual and transparency of power.” *Privacy and the Criminal Law* (February 2006): 61–104.

Hustinx, P. “The moment of truth for the Data Retention Directive”. Brussels, 2010. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

Ignatieff, M. “Is the Human Rights Era Ending?” *New York Times*, February 5, 2002. http://www.nytimes.com/2002/02/05/opinion/is-the-human-rights-era-ending.html?src=pm.

“Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment.” *Department for Transport*, January 2010. http://assets.dft.gov.uk/publications/interim-code-of-practice-for-the-acceptable-use-of-advanced-imaging-technology-body-scanners-in-an-aviation-security-environment/cop.pdf.

Ip, J. “Suspicionless Searches and the Prevention of Terrorism.” In *Counter-terrorism and Beyond*, by A Lynch, N McGarrity, and G Williams, 1–21. London: Routledge, 2010.

Kirby, M. “Terrorism: The International Response of the Courts.” *Indiana Journal of Global Legal Studies* 12, no. 1 (2005).

Levi, Michael, and David Wall. “Technologies, Security, and Privacy in the Post-9/11 European Information Society.” *Journal of Law and Society* 31, no. 2 (June 2004): 194–220.

LIBE. “Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview.” *European Commission Joint Research Centre* (July 2003): 1–189.

Liberty. “Liberty’s response to the Department of Transport’s consultation on the Code of Practice for the acceptable use of advanced imaging technology (body scanners) in an aviation security environment.” *Liberty*, July 2010. http://www.liberty-human-

rights.org.uk/pdfs/policy10/liberty-s-response-to-the-body-scanners-consultation-july-2010.pdf.

Lodge, J. "Quantum Surveillance and `Shared Secrets' A biometric step too far?" *Centre for European Policy Studies*, no. July (July 2010): 1–43.

Loewenstein, K. "Militant Democracy and Fundamental Rights." In *Militant Democracy*, edited by A Sajo, 231-262. Eleven International Publishing. Utrecht: Eleven International Publishing, 2004.

Lombard, E. "Bombing Out: Using Full-Body Imaging to Conduct Airport Searches in the United States and Europe Amidst Privacy Concerns." *Tulane Journal of International and Comparative Law* 19, no. 337 (May 2010): 1–25.

Lyon, D. "Biometrics, Identification and Surveillance." *Bioethics* 22, no. 9 (November 2008): 499–508.

Lyon, David. "Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies1." *International Political Sociology* 4, no. 4 (December 2010): 325–338.

Manners, I. "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 40, no. 2 (May 2002): 235–58.

Mock, T W. "The TSA's New X-Ray Vision: The Fourth Amendment Implications of 'Body-Scan' Searches at Domestic Airport Security Checkpoints." *Santa Clara Law Review*, no. 49 (May 2009): 213–251.

Mordini, E, and S Massari. "Body, Biometrics and Identity." *Bioethics* 22, no. 9 (November 2008): 488–498.

Mordini, E, and C Petrini. "Ethical and social implications of biometric identification technology." *Ann Ist Super Sanita* 43, no. 1 (2007): 5-11.

Mythen, G, and S Walklate. "Criminology and Terrorism: Which Thesis? Risk Society or Governmentality?" *British Journal of Criminology* 46, no. 3 (April 2006): 379–398.

"National Strategy for Combating Terrorism." *CIA.gov*, 2003. https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

O'Harrow, R. "Privacy Eroding, Bit by Byte." *Washington Post*, October 15, 2004. http://www.washingtonpost.com/wp-dyn/articles/A34098-2004Oct14.html.

"Poll: 4 in 5 Support Full-Body Airport Scanners." *CBS News*, n.d. http://www.cbsnews.com/8301-503544_162-20022876-503544.html.

"Privacy Impact Assessment for the Screening of Passengers by Observation Techniques (SPOT) Program". Department of Homeland Security, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_spot.pdf.

"Privacy Impact Assessment Update for TSA Advanced Imaging Technology". Department of Homeland Security, 2011. http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf.

Prosser, W L. "Privacy." *California Law Review* 48, no. 3 (August 1960): 383-423.

"Review of terror laws: New name for an old problem." *The Guardian*, January 27, 2011. http://www.guardian.co.uk/commentisfree/2011/jan/27/review-terror-laws-liberty.

Risen, J, and E Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." *New York Times*, December 16, 2005. http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

Roach, K. "Anti-Terrorism and Militant Democracy: Some Eastern and Western Responses." In *Militant Democracy*, edited by A Sajo, 171-208. Eleven International Publishing. Utrecht: Eleven International Publishing, 2004.

———. "Sources and Trends in Post-9/11 Anti-Terrorism Laws." In *Security and Human Rights*, by L. Lazarus and B J Goold. Hart Publishing. Oxford: Hart Publishing, 2007.

Sajo, A. "From Militant Democracy to the Preventive State?" *Cardozo Law Review* 27, no. 5 (2006): 2255-2295.

Salter, M B. "Governmentalities of an Airport: Heterotopia and Confession." *International Political Sociology* (January 2007): 1–18.

Savage, C, and J Risen. "Federal Judge Finds N.S.A. Wiretaps Were Illegal." *New York Times*, March 31, 2010. http://www.nytimes.com/2010/04/01/us/01nsa.html.

Sprokkereef, A., and P De Hert. "Ethical Practice in the Use of Biometric Identifiers Within the EU." *Law, Science and Policy* 3 (November 2007): 177–201.

Star, G. "Airport Security Technology: Is the Use of Biometric Identification Technology Valid Under the Fourth Amendment?" *Temple Environmental Law and Technology Journal* 20 (May 2002): 251–265.

Steiker, C S. "Foreword: The Limits of the Preventive State." *The Journal of Criminal Law and Criminology* 88, no. 3 (1998).

Strossen, N. "The Fourth Amendment in the Balance." *New York University Law Review* 63 (1988).

Sullivan, B. "Privacy under attack, but does anybody care?" *MSNBC*, October 17, 2006. http://www.msnbc.msn.com/id/15221095/ns/technology_and_science-privacy_lost/t/privacy-under-attack-does-anybody-care/#.To897px1-dE.

"Surveillance Under the PATRIOT Act". American Civil Liberties Union, 2011. http://www.aclu.org/national-security/surveillance-under-patriot-act.

Tham, J C, and K D Ewing. "The Continuing Futility of the Human Rights Act." *Public Law* (2008).

"The NSA Program to Detect and Prevent Terrorist Attacks - Myth v. Reality." *Department of Justice*, January 27, 2006. http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf.

Travis, A. "Control orders: home secretary tables watered-down regime." *The Guardian*, January 26, 2011. http://www.guardian.co.uk/law/2011/jan/26/control-order-review-theresa-may.

Tridimas, P T. “Terrorism and the ECJ: Empowerment and democracy in the EC Legal Order.” *Queen Mary University of London, School of Law* (March 2009): 1–37.

Walker, C. “Neighbor Terrorism and the All-Risks Policing of Terrorism.” *Journal of National Security Law & Policy* 3 (December 2009): 121–168.

———. “The threat of terrorism and the fate of control orders.” *Public Law* 4 (2010).

Warren, S, and L D Brandeis. “The Right to Privacy.” *Harvard Law Review*, no. 193 (1890).

Wood, D., E. Konvitz, and K. Ball. “The Constant State of Emergency? Surveillance after 9/11.” In *The Intensification of Surveillance - Crime, Terrorism and Warfare in the Information Age*, by K. Ball and F. Webster, 137-151. London: Pluto Press, 2003.

Yost, P. “Rise in FBI use of national security letters.” *Washington Post*, May 10, 2011. http://www.washingtonpost.com/politics/rise-in-fbi-use-of-national-security-letters/2011/05/09/AFN6xLdG_story.html.

SUPREME COURT CASES

Berger v. New York 388 U.S. 41 (1967).

Goldman v. United States 316 U.S. 129 (1942).

Griswold v. Connecticut 381 U.S. 479. (1965).

Haig v Agee 453 U.S. 280, (1981).

Hamdan v. Rumsfeld 548 U.S. 557 (2006).

Hamdi v. Rumsfeld 542 U.S. 507 (2004).

Korematsu v. United States 323 U.S. 214 (1944).

Katz v. United States 389 U.S. 347 (1967).

Olmstead v. United States 277 U.S. 438 (1928).

Smith v. Maryland 442 U.S. 375 (1979).

Terry v. Ohio 392 U.S. 1 (1968).

Whalen v. Roe 429 U.S. 589 (1977).

FEDERAL COURT CASES

Elli Lake v. Wal-Mart Stores, Inc. 582 N.W.2d 231 (Minnesota 1998).

United States v Davies, 482 F.2d 893, 9th Circuit (1973).

United States v. Duggan 743 F.2d 59 (2nd Cir. 1984).

EUROPEAN COURT OF HUMAN RIGHTS CASES

A and others v United Kingdom, 29 EHRR 29 (2009)

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (62540/00) (2008)

Gillan and Quinton v the United Kingdom (4158/05) (2010).

Iordachi and Others v Moldova (25198/02) (2009).

Kennedy v. the United Kingdom (26839/05) (2010).

Klass and others v. Germany (5029/71) (1978).

Liberty and others v the United Kingdom (58243/00) (2000).

Malone v. the United Kingdom (8691/79) (1984).

Uzun v. Germany (35623/05) (2010).

Weber and Saravia v. Germany (54934/00) (2000).

EUROPEAN COURT OF JUSTICE CASES

T-194/04, *Bavarian Lager v. Commission* (2007).

Joined cases of C-402/05 P & C-415/05 P *Kadi & Al Barakaat International Foundation v Council and Commission* (2008).

Cases T-228/02 and T-256/07 *Organisation des Modjahedines du peuple d'Iran v Council* (2008).

Case T-47/03 R, *Jose Maria Sison v Council and Commission* (2003).

Case C-355/04 P *Segi and Others v Council of the European Union* (2007).

Joined cases of C-465/00 and C-138/01, *Rechnungshof v. Österreichischer Rundfunk* (2003).

Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and European Parliament v Commission of the European Communities* (2006).

HOUSE OF LORDS JUDGMENTS

A v Secretary of State for the Home Department, UKHL 56 2 AC 68 (2004).

Campbell v. MGN Ltd. [2004] UKHL 22.

Douglas v. Hello! Ltd. [2005] HRLR 27.

R. *(Gillan) v. Commissioner of Police of Metropolis* UKHL 12 (2006).