Page left intentionally blank

Subject to Predicate

Risk, Governance and the Event of Terrorism within Post-9/11 U.S. Border Security

Mathew Alexander Yuri Kabatoff

Department of Sociology

MPhil/PhD

London School of Economics
and Political Science

Declaration

I certify that the thesis I have presented for examination for the MPhil/PhD degree of the London School of Economics and Political Science is solely my own work, except where I have clearly indicated that it is the work of others.

Final Word Count

82,086

Font

Arial, 10pt, 1.5 spacing

Abstract

As a result of the 9/11 terror attacks, a new and far-reaching form of security governance has emerged within the United States under the heading of 'homeland security'. While this mode of security has brought with it a range of domestic counter-terrorism efforts, such as new methods of preparedness in the event of attacks on American cities, as well as mechanisms to seize and cut off terrorist assets, it has also predominantly been oriented towards the development of a new legal, institutional and technological regime responsible for the management and risk assessment of individual identity and the identities of foreign nationals passing through U.S. borders.

Although this mode of security provides new powers as well as more flexible and collaborative methods for U.S. customs, law enforcement and intelligence to address the threat of terrorism, it has also created political controversy. This controversy has rested upon the perception that homeland security methods embody an unchecked extension of executive power negatively impacting the rights and liberties of the individuals that these very security techniques were established to protect. In order to interrogate this controversy and analyse how this new form of security performs within an extended field of sovereign power, this thesis takes into account the laws, policies and technologies – biometric, data-mining, database – that shape this new form of security at the border.

This new form of security arguably not only embodies a mobilisation and empowerment of U.S. intelligence and law enforcement agencies which understand terrorism as catastrophic and generational, but it can fundamentally be seen as creating a new infrastructure that allows U.S. security institutions to become more 'informationally' aware of the identities of individuals entering and exiting the country. How U.S. security institutions access such identity information, along with how this data is used, is what constitutes the new social and political reality at the border.

Table of Contents

The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition not infrequently — like the effect of a fog or moonshine — gives to things exaggerated dimensions and unnatural appearance. (Clausewitz, 1984)

Carl von Clausewitz

1. Preliminary Considerations

1.1

In a February 2011 article in the New York Times commenting on the 'Arab Spring' that resulted in the collapse of the autocratic regimes of Ben Ali in Tunisia, Mubarak of Egypt and later Gaddafi of Libya, journalist Scott Shane questioned what impact this political movement would have on the future threat of Al Qaeda to the United States and the region. Shane wrote that if the regional locations of Al Qaeda's discontent had disappeared and the political force that brought about this change had been based upon the emergence of a civil and democratic consciousness rather than the values and beliefs of radical Islam,[1] would '. . . the terrorist network shrivel slowly to irrelevance? Or would it find a way to exploit the chaos produced by political upheaval and the disappointment that would inevitably follow hopes now raised so high?' (Shane, 2011, p. 2) While it would be premature to assume that this important political event would have the immediate effect of extinguishing Islamic terrorism, it does present the opportunity for a thought experiment to conceptualise an image of U.S. political and security practise within a post-9/11 era. This conceptualisation can be further supported by a number of events that have taken place since February 2011: namely, the death of Osama Bin Laden; the withdrawal of the U.S. military from Iraq; and the recognition that the war in Afghanistan, despite that country's continued status as fractured nation-state, no longer fulfils specific counter-terrorism goals for the U.S. (Bremmer, 2012) While it would be compelling to speculate or develop a vision of what political or security challenges come after the war on terror, this thought experiment remains useful in grounding an analytic framework in order to ask a counter-factual question or to ask in the extinguishing of the terrorist threat, what form of U.S. domestic counter-terrorism practise and security remains? Or, rather, how can the last 10 years of U.S. homeland security practise, which has undergone a profound transformation in respect to the governance and management of threats, be accounted for?

Admittedly, the broad-based foreign policy goals of the United States can be argued to have shifted away from the Middle East, apart from the threat of Iran obtaining a nuclear weapon, and now concern risks associated with economic stability and competition primarily arising from China (Bremmer, 2012). However, it would be inaccurate to assume that the security practises developed over the last decade primarily by the Department of Homeland Security (DHS) would simply change their mission or wither away. In fact, U.S. constitutional scholar Jack Goldsmith has argued that even the opportunity for U.S. counter-terror practises embodied as part of the war on terror were primed to diminish in the changeover from the Bush to Obama administrations – Obama ran on a campaign deriding the Bush approach to counter-terrorism – the vast majority of domestic and foreign counter-terrorism practises remained (Goldsmith, 2012, p. 3). As a result, it will be argued that the domestic security changes made since 9/11, and in particular those practises associated with the management and risk assessment of the travelling population to and within the United States, not only

[1] For example. the toppling of autocratic rulers such as Mubarak in order to establish an Islamic caliphate.

persists, but has created a new form of security governance based on informational awareness of individual identity that is now a core feature of U.S. homeland security. This identity-oriented security practise as a result continues to shape the empirical realities of post-9/11 border security. Therefore, despite the urge to simply cast away the sociopolitical transformation that has taken place over the last 10 years in the face of a changing Middle Eastern foreign policy outlook, it remains an important task of social science to understand what has constituted the domestic security transformation over the last decade in order to assess the impact that these changes have had on securing the U.S. frontier as well as to obtain generalisable characters that can inform an understanding of the behaviour and actions of U.S. homeland security in the future.

What defines and continues to give analytic relevance to the U.S. homeland security agenda is the change in how threats have been understood and mitigated since 9/11. An important problematic that U.S. homeland security has set out to address is not merely how to guard against identifiable threats residing outside of the country as found with the active global counter-terrorism policy of engagement seen in the cases of the Iraq and Afghanistan wars, but, rather, how to address the problem of identifying threats that are disguised or hidden within the travelling civilian population – as was the case with the 9/11 attacks. As a result, U.S. homeland security has worked to securitise the visa and immigration system as well as create new methods in order to vet and assess primarily foreign nationals prior to and upon arrival to the United States. The main change that has defined this form of securitisation is not the simple or binary of closing of the border to certain ethnic, religious or national groups, but, rather, the emergence of a new form of security centred on the individual that not only allows for threats to be identified – via the collection of identity information and the matching of this information against intelligence databases and watch lists – as well as allows U.S. borders to remain open to flows of goods, capital and people.

To further develop this point, this mode of security departs from past U.S. homeland security practises directed solely towards recognisable national or ethnic groups[2] designated as a national threat. Instead, contemporary homeland and in particular border security is oriented towards the identification of threats associated with specific individuals travelling through the border zone that are masked or disguised as civilians. While U.S. homeland security practises still contain a past cleavage of group profiling – a security practise that dates back to the Second World War and the internment of all U.S.–Japanese citizens on the West Coast, with the contemporary version being the U.S. list of nations recognised as 'state sponsors of terror' – this form of profiling makes up only one attribute of the corresponding security matrix. To illustrate how this works, in the aftermath of the attempted bombing of Northwest Airlines flight 254 from Amsterdam to Detroit in December 2009 by a young radical Muslim, Nigerian Umar Farouk Abdulmutallab, who was radicalised while a student[3]

[2] This notion of security directed at the group can also be seen in the U.S. post-WWII during the McCarthy era, when members of the Communist Party in America were subjected to surveillance, imprisonment and exile.
[3] Abdulmutallab was radicalized while a student at University College London and received further terrorist training as well as obtained a bomb designed to be hidden within his 'underwear' in Yemen.

in Britain, the DHS proceeded to enhance screening of nationals from 14[4] Middle Eastern and North African countries, even though these nations did not have a direct link to the Abdulmutallab plot (Lipton, 2009). However, the security response to this incident revealed that beyond the broad category of national, ethnic or religious affiliation, Abdulmutallab was already listed within U.S. counter-terrorism databases and was to be detained and interviewed by DHS officials upon landing in Detroit. Since he was not placed on the 'no-fly' list – a list described in detail in Chapter 7, which bars high-risk individuals from boarding aircraft bound for the U.S. – he was not impeded by airport security officials and was able to avoid detection from physical airport screening procedures – in this case carrying a concealed explosive device onto the plane. The recourse by the DHS to the incident then called for greater tightening of the watch-list nomination process as well as for further collection of Passenger Name Record (PNR) data so that U.S. border security services were able to more readily intervene upon specific individuals, rather than the upholding of blanket bans on specific groups (Napolitano, 2011). What this example shows is that the new mode of security taken up by the DHS and corresponding intelligence and border security agencies is one that is multi-modal, operating at multiple layers and in this case moving from macro to micro categories of analysis of the individual in order to monitor and identify threats. A key component that makes this form of layering possible is the use of biometric, data-mining and data-sharing technologies, whereby U.S. security services have been enabled since 9/11 to acquire multiple data types from the individual that give clues into present and future behaviour, along with social networks and national affiliation. However, while these new technologies and data acquisition powers given to U.S. security services present a vision of unfettered surveillance, this practise of data collection, analysis and, ultimately, security action is shaped and mediated by economic, technological, constitutional and institutional factors.

As a result, an important observation concerning this mode of security is that while it announces a new form of data-surveillance active at the U.S. border zone, this security practise can be found to be unevenly applied. This is perhaps not surprising. For instance, Bigo and Guild have shown that immigration practises within Europe have had a long history of segmenting and separating travelling populations to not only determine citizenship, but also the right to work, study or asylum, which therefore results in a different experience and application of state power to each particular group or individual (Bigo & Guild, 2005). Despite the more universal claims made as part of U.S. counter-terrorism rhetoric and embodied in the phrase 'war on terror' – conceptually this phrase conflates the particularism of a national war strategy with an unreferenced noun – U.S. homeland and border security has been found to be primarily directed towards foreign nationals with respect to non-U.S. residents where the visa, immigration and border cross systems have taken on prime interest. Here, U.S. law enforcement, intelligence and security services have been granted greater permissions and flexibility in terms of data collection and analysis due to the lack of legal

[4] The 14 nations were Cuba, Iran, Sudan, Syria, Afghanistan, Algeria, Lebanon, Libya, Iraq, Nigeria, Pakistan, Saudi Arabia, Somalia and Yemen.

protections afforded to foreign nationals. Therefore, this mode of security cannot be understood as a universal claim, but, rather, one that is shaped and directed, even though the catastrophic threat imagined does not discriminate between foreigner and national. However, despite the directionality of U.S. border security practises, the interplay between law, technology and governance is importance since it has resulted in a major shift in how populations are managed and threats are assessed at the border.

Taking into account this thought experiment as well as the subsequent rendering of the socio-political implications of U.S. homeland and border security, this thesis asks three questions in order to analyse and interrogate the relationship between executive power, technology and security governance, post-9/11.

1.2 Three Questions

(1) What relationship does this new mode of security have with the theory of the 'state of exception' and the re-emergence of sovereign power post-9/11?

This first question directs us to consider how post-9/11 border security simultaneously embodies and challenges the social science concept of the 'state of exception' where executive power is understood to be divorced from social and legal constrains during a state of emergency. This dual quality of post-9/11 border security is grounded empirically through the consideration of the legal, technological and economic forces that, on the one hand, afford increased flexibility and powers to U.S. security agencies, while on the other they delimit and direct how, where and upon which subjects these powers can be applied. This concept of curtailment or shaping of sovereign power is supported by Burchell's reading of the concept of 'governmentality'[5] developed by Foucault and applied to liberal political systems.[6] In Burchell's view, liberal government operates in response to the behaviour of economic actors while at the same time seeking to establish and enforce political rights, norms and obligations. Addressing specifically classical liberalism and its impact on sovereign power, Burchell argues that liberalism is a 'recognition of heterogeneity and incompatibility of the principles regulating the non-totalisable multiplicity of economic subjects of interest and those operating in the totalizing unity of legal political sovereignty' (Burchell, 1991, p. 118). While the liberal or economic form of government finds itself in opposition to the legal form of government – since the liberal economic rationality is based upon the maximisation of utility as opposed to strictly the enforcement of sanctions – neither completely cancels the other out. Rather, the choice between economy and sovereignty, according to specific political events, informs how political power is exercised. If an update can be made to the duality of economy and sovereignty, it perhaps can be extended to show an opposition between economy, sovereignty and technology where each come to play a

[5] The term 'governmentality' is used by Foucault and later developed by Rose, Miller, Burchell and others to describe and represent the logics or 'rationales' upon which government operates. Govermentality studies then attempt to understand not only the consequence of decisions made by government – whether they are right or wrong – but also the underlying motivations and 'reason' that inform both decision and action.

[6] Of which can be applied to an analysis of the United States which is a dominant participant in the global liberal economic system.

role in shaping how the U.S. border is governed. This third quality of technology, then, is reserved for the second question of this thesis. Therefore, the notion of the governmentality of U.S. homeland and border security that will be addressed concerns not only the relationship of the renewed exercise of executive power – which can be seen as subject to constitutional and legal constraints – or the pressures of global liberal economy on migration flows, but technological capacities that make this new mode of security at the border possible.

(2) How have digital technologies, in particular biometric, data-mining and database technologies, impacted and shaped this new form of security?

This second question will be addressed in two ways. First, as already introduced, the rationale of government that can be found within the U.S. border zone is one that is primarily concerned with the collection and analysis of identity predicates from individuals passing through the visa and immigration system as well as the border zone. This form of knowledge relies, then, on digital tools in order to apprehend, chart and measure the materiality of identity. Identity predicates, however, are not captured solely for the binary operation of identity verification – such as in determining valid claims of identity at immigration controls or as part of the visa issuance process – but are equally oriented towards secondary methods of identity analysis such as watch-list screening as well as to fulfil a forensic purpose in order to be on hand in the case of a future terrorist attack. An analysis of this secondary form of identity processing is central to understanding what makes this new mode of security possible. The origins of this strategy date back to concerns about the ability of Al Qaeda and like organisations to carry out the 9/11 attacks by exploiting the U.S. visa and immigration system. As will be discussed in the further detail in the following pages, the 9/11 hijackers were able to make detailed preparations, moving in and out of the United States up to 13 months prior to the attack, a period in which each was assumed to be a legitimate visa holder. This perception of a fault in existing security arrangements was recognised by U.S. congressional members as well as by U.S. intelligence in their audit of 9/11. It not only contributed to a new security strategy oriented towards identity, but also led to three significant institutional changes. First, the upgrading of the measures used for identity verification and vetting as part of the visa application process to enter the U.S. Second, the creation of a set of policies and laws to facilitate the collection and sharing of identity data collected primarily on foreign nationals where this data includes biometric and biographic data associated with the immigration and travel processes. Finally, the adoption of methods of analysis and sharing data to allow U.S. security services the opportunity to find actionable information that can be distributed between the law enforcement, intelligence and customs communities. What this reveals is that U.S. homeland and border security not only functions through the establishment of a new set of standards and norms that enforce stringent requirements to pass through U.S. borders; it also works to create a new analytic regarding the behaviour and attributes of those travelling to and within the U.S. This analytic is viewed as significant since it not only reveals how U.S. border security functions at the micro level,

but it also acts as a framework for understanding how rationales of risk come to inform and shape border management and control.

(3) How effective is U.S. homeland and border security in respect to its stated aims of counter-terrorism?

The third question this thesis asks is: How well does homeland and border security work to achieve its stated policy aim of reducing or nullifying terrorist attacks on U.S. soil? One of the obstacles in answering this question is the question of measurement. As will be argued in Chapter 3 concerning methodology, while cost-benefit or quantitative methods of analysis are not without merit, they alone cannot grasp the full impact of border security measures post-9/11. This is due to the understanding of contemporary terrorism as an event that is infrequent, catastrophic and generational. These three attributes are important since they represent a threat that is at odds with scientific measurement yet occupies a central place in national security and public policy decision making. As a result, this new mode of security more easily lends itself to an analysis of the institutional, legal and technical changes that have impacted security governance at the border post-9/11. For instance, a key finding described in Chapter 7 that concerns PNR data collection is shown to be more pervasive in respect to foreign nationals planning to enter the U.S. versus U.S. citizens due to a lack of legal protections. One can only surmise that, given further terrorist activity or the issuance of a state of emergency by the U.S. government, domestic security might plausibly wish to apply such measures to U.S. citizens as well. However, until this unlikely yet plausible event takes place, U.S. homeland security is still left vulnerable to 'home grown' terrorism that is not explicitly checked for within the context of the border. Understanding how these bifurcated security practises have emerged and perform, in respect to their security gains, obstacles and limitations, provides insight into future forms of security governance along with the politics concerning data acquisition and surveillance given a sustained future terrorist threat.

With these three questions, this thesis maps and evaluates the emergence of a significant form of security governance that has taken place within the United States and has impacted Western Europe as well as the 36[7] member nations of the Visa Waiver Program (VWP). What this thesis seeks to establish is not only a description of a new set of institutional, legal and technological developments that have taken shape since late 2001, but how these very developments have shaped a new form of security governance. In order to address the research locations that compose the multi-dimensional space of the U.S. border, and in particular air travel to and from the U.S., it is important to understand the set of rationales that the U.S. executive branch, namely the presidency has operated under in response to 9/11. In order to define these rationales, it is important to revisit the account of the 9/11 terror

[7] Andorra, Australia, Austria, Belgium, Brunei, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, United Kingdom.

attacks and the security holes within the U.S. immigration and border control process that allowed for the 9/11 terror attacks to take place.

1.1 Changes within homeland security and its dominant rationales since 9/11

During the Bush administration – from 2000 to 2008 – U.S. counter-terrorism practises were most visible outside the United States as exemplified by the wars in Iraq and Afghanistan as well as the controversial and highly visible practises of enemy combatant detention in Guantánamo Bay, and rendition (Goldsmith, 2012). While this global counter-terror strategy met with substantial international criticism[8] and therefore has garnered significant political and academic attention, the United States has also engaged in a quieter[9] but no less substantial defensive domestic counter-terrorist and preparedness strategy under the title of 'homeland security' (Heng & McDonagh, 2009). This strategy has primarily been motivated by the development of preventative and precautionary counter-terrorism measures that actively seek to break up and thwart terrorist plots, logistical capabilities and actions. As a result, the most significant structural changes that have taken place in respect to terrorism have involved the reconfiguration and reformation of America's domestic intelligence, immigration and law-enforcement institutions in order to become more 'informationally' aware of the identity and affiliations of individuals, primarily foreign nationals wishing to travel to and within the country. What is important to consider, however, is that despite the dramatic change that took place within domestic national security infrastructure post-9/11, pre-9/11 U.S. national security policy was already coming to be aware of threats inherent to globalisation and technological change such as open borders as well as the increasing availability of inexpensive yet catastrophic biological and even nuclear weaponry.

With this in mind, although U.S. Congress passed the 'Homeland Security Act' in 2002 – a bill used to create what is now known as the Department of Homeland Security (DHS) – the bill was informed largely by the recommendations made by the Hart-Rudman Commission on National Security, conducted from 1998 to 2001. In its pre-9/11 conclusions, this commission determined that U.S. domestic security would be challenged not only by novel developments of new weapons technologies such as bio- or cyber-weapons but more significantly at the structural level where the U.S. would become increasingly vulnerable to 'asymmetric' threats. Despite American military pre-eminence in respect to arms and munitions, U.S. intelligence would face more challenging adversaries where not even 'excellent intelligence would not be able prevent all surprises'; and the U.S. homeland would become a target due to porous borders as a result of globalisation, both challenging and calling for the reaffirmation of sovereignty (Hart & Rudman, 2001, p. 118) (Chertoff, 2008, p.

[8] In respect to controversy surrounding the international and political strategy of the war on terror: the Iraq war was heavily opposed by millions of British and U.S. nationals; the Afghanistan war, while smaller, continues to this day and has led to the destabilisation of Pakistan due to retaliatory strikes by the Taliban; Guantánamo Bay, the holding center for suspected terrorists, has been linked with unlawful detention and torture; and the media campaign and public statements made by the Bush administration have not necessarily endeared the Middle East and the Muslim world to the United States.

[9] The term 'quieter' is only used in respect to media attention. The changes that have taken place in respect to domestic security post-9/11 have, as this thesis will argue, been extremely substantial and equally political.

1). Given these recommendations, as well as with a view that U.S. domestic intelligence and visa and immigration services were severely compromised in the lead-up to 9/11, the DHS and the policy platform for homeland security were developed not only to ensure resilience in the event of an emergency, but to provide a new networked and intergovernmental national security infrastructure that would enable U.S. security services to identify and track threats as they interfaced with U.S. immigration and the border crossing process. In order to achieve this goal, the DHS, as the institution charged with the homeland security mandate, was to be created out of the consolidation of 27 government agencies, including the Federal Emergency Management Agency (FEMA), the Customs Service (renamed the Customs and Border Protection agency [CBP]), the Border Patrol, the Coast Guard, and the Immigration and Naturalization Service (INS), with the expressed intent of having closer communication and data-sharing ties with U.S. domestic intelligence and law enforcement (DHS, 2008). The DHS was also intended, as described in the Homeland Security Act, to prevent terror attacks within the United States; reduce the vulnerability of the United States to terrorism; and minimise the damage from terrorist attacks should they occur (Homeland Security Act, 2002). Coinciding with the development of this bill was the announcement by President Bush of an increase in funding for homeland security from $19.5 billion – earmarked pre-9/11 as part of the Y2002 budget – to $37.7 billion. The bulk of this funding was directed at first responders, bioterrorism prevention efforts, border security and 'technology reflecting an increased emphasis on homeland security' (DHS, 2008, p. 5).

Along with the creation of the DHS, the Federal Bureau of Investigation (FBI) was also tasked with its own set of institutional reforms to make it more effective in the face of terrorism. It must be recalled that the FBI was singled out along with the INS in the *9/11 Commission Report* for its intelligence failures in the lead-up to 9/11, where these failings were the result of both inadequate intelligence-gathering techniques as well as self-imposed institutional barriers that prevented the sharing of actionable intelligence[10] (Grewe, 2004). As part of its process of reform, which saw the departmental allocations of agents shift heavily towards national security,[11] the FBI acquired a new set of law enforcement tools and adopted an investigatory orientation based upon information sharing, communication and prevention (FBI, 2005). The new law-enforcement tools consisted of not only technological upgrades – that is, new digital methods for the analysis and collection of information – but a legal and institutional retooling as well. For instance, the Department of Justice (DoJ), the branch of government responsible for the prosecution of criminal and national security cases brought forward by the FBI, was granted the ability to prosecute terror cases on the basis of more general or minor offences such as identity theft, immigration violations and the making of false statements in the context of immigration hearings. The rationale behind this shift was

[10] The three members of the 9/11 plot in question were Khalid al Mihdhar, Nawaf al Hazmi and Zacarias Moussaoui. Moussaoui has been described by the U.S. State Department as the '20th hijacker', since he was arrested and deported from the U.S. on immigration violations during the late summer of 2001 after arousing suspicion of hijacking intent at a flight training school in Minneapolis, Minnesota. Mihdhar and Hazmi were two of the five hijackers on American Airlines Flight 77, which crashed into the Pentagon on September 11, 2001.

[11] In 2001 49% of agents and departmental resources were focused on criminal investigations and 32% on national security matters; 44% were focused on national security and 32% on criminal matters in 2005 (FBI, 2005).

one of prevention and precaution described by the FBI as beneficial, since 'prosecution on such charges is often an effective method, and sometimes the only available method, of deterring and disrupting terrorist planning and support activities' (FBI, 2005, p. 1). Second, with the passing of the USA Patriot Act[12] (USA Patriot Act, 2001) (USAP), the FBI was also granted institutional licence to share information with greater ease between the intelligence community and law enforcement – the problems in respect to data-sharing and 9/11 will be discussed in greater detail in the following pages. Finally, the FBI's budget was doubled, much like that of the DHS over the period of 2001–08, from approximately $3.5 to $7.1 billion, and has been used to develop a new set of counter-terrorist units that allow for a broader range of intelligence gathering, analysis and sharing in respect to both foreign and domestic threats. These units, consisting of the Joint Terrorism Task Force (JTTF), the Terrorist Screening Center (TSC), the National Counter Terrorism Center (NCTC) and the Foreign Terrorist Tracking Task Force (FTTTF), have not, however, been created simply as discrete investigatory bodies each with their own singular mandates; rather, each has been designed to be networked not only with each other but with the broader law-enforcement community and the DHS in order to provide timely intelligence when required. As a result, in the acquisition of new law-enforcement tools and a change in institutional rationale towards a rationale of prevention, the FBI has moved from a practise of veiled and targeted intelligence gathering on a case-by-case basis to a mandate based on the daily monitoring of civil institutions alongside a more targeted intelligence-gathering approach in order to intervene upon potential threats. This technological and institutional shift, which can be described as allowing the FBI to perform actions of non-particularised search, will be addressed in detail in Chapter 5.

1.3 9/11 and Terrorist Travel

> . . . Just yesterday, the Department of Justice released information indicating that 13 of 19 terrorist hijackers had entered the United States legally with valid visas. Of the 13, 3 of the hijackers had remained in the United States after their visas had expired. The INS had no information on six of the hijackers. [. . .] . . . Today, I see three areas of vulnerability in our immigration system: first, an unregulated visa waiver program in which 23 million people arrive in this country annually from 29 different countries with little scrutiny; second, an unmonitored non-immigrant visa system in which 7.1 million tourists, business visitors, foreign students and temporary workers arrive. To date, the INS does not have a reliable tracking system to determine how many of these visitors left the country after their visas expired. Third, among the 7.1 million non-immigrants, 500,000 nationals entered on foreign student visas. The foreign student visa system is one of the most under-regulated systems we have today. (Feinstein, 2001, p. 3)
>
> Senator Diane Feinstein

[12] The full title of the Patriot Act is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

As it has been described in both the 9/11 Commission Report (Report) and the 9/11 Terrorist Travel Monograph (Monograph), the narrative of the 9/11 attacks was one of not only shock and tragedy, but missed opportunities on the part of U.S. intelligence and visa and immigration control.[13] While each report features many recommendations concerning broader aspects of American foreign policy related to the war on terror and the threat of radical Islam, each places significant emphasis on the securitisation of the travel visa, immigration and travel process as a way to enhance homeland security. The Report and the Monograph argue that systematic weakness in American domestic defence that allowed the 9/11 terrorists to coordinate the attacks from within the United States was the result of the lack of a well-developed counter-terrorist strategy applied to American border security practises. For instance, it was found that on separate occasions five hijackers were selected for secondary screening, but these inspections did not look for terrorist predicates or evidence of terrorist intent; rather, they were designed to identify drug smuggling or determine whether the individual was an 'intending immigrant' (9/11 Commission, 2004, p. 526). Second, the U.S. immigration system was unable to fulfil basic institutional duties such as identifying fraudulent or manipulated identity documents – for example, Mohand al-Shehri, one of the 14 'muscle-hijackers'[14] who were tasked with guarding the Al Qaeda pilot of each hijacked flight, obtained a two-year B-1/B-2 tourist/business visa from the U.S. Consulate in Saudi Arabia, despite submitting a passport that lacked an expiry date; al-Shehri was also not interviewed by the Consulate as part of the visa administration process despite being legally required to do so in order to obtain a visa (9/11 Commission, 2004). Finally, it was found that U.S. intelligence agencies not only failed to exchange and share important counter-terrorist intelligence inter-departmentally, but this information was not passed onto U.S. customs and immigration, who were in the position to intercept the 9/11 hijackers. For instance, the CIA was aware of another muscle-hijacker, Khalid al-Mihdhar, as early as 2000, yet his name was not placed on a terror 'watch-list' nor was notification of terrorist affiliation given to the consulate responsible for issuing his B-1/B-2 visa in Saudi Arabia (9/11 Commission, 2004) (Eldridge, et al., 2004). These errors in the eyes of the Commission and congressional testimony post-9/11 gained even more significance when considered alongside the devastation of the 9/11 terror attacks as well as the fact that out of the 23 visa applications made by the nineteen 9/11 hijackers, 22 applications were successful, thus allowing the hijackers to remain within the country or even exit and re-enter unimpeded.[15]

[13] It may seem to the reader that the terms 'domestic security' or 'border controls' should be included in this list; however, the U.S. government pre-9/11 had not assigned a specific agency the duty of providing domestic defence or border security that included counter-terror measures.

[14] The term 'muscle-hijacker' refers to those hijackers who were not pilots. Their role was to protect the pilots and intimidate and keep order amongst the air passengers.

[15] The four 9/11 pilots passed through immigration and customs inspections a total of 17 times from May 29, 2000, to August 5, 2001: Ziad Jarrah was the most frequent border crosser, entering the U.S. seven times; Mohammed Atta and Marwan al-Shehhi each entered three times; and Hani Hanjour was the only hijacker to enter on an academic visa. Thomas R. Eldridge, Susan Ginsburg, Walter T. Hempel II, Janice L. Kephart, Kelly Moore, 2004, '9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks upon the United States,' ed. National Commission on Terrorist Attacks Upon the United States. Washington, D.C.: U.S. Government Printing Office.

A further fault identified by Congress and the Commission was the lack of an entry/exit system in order to track visa overstays as well as a basic system to monitor visa violations, in particular those violations related to the student visa issuance and compliance. Out of the 19, two hijackers violated the terms of their visas. For instance, Ziad Samir Jarrah, the pilot of United Airlines Flight 93, which was shot down by U.S. fighter jets over a field in Pennsylvania, entered the United States on a valid tourist visa but immediately took up flight training, thus violating his visa terms (Eldridge, et al., 2004). However, these two hijackers were not tracked down, nor was the violation enforced due to the lack of a monitoring and enforcement mechanism to determine the whereabouts of the individuals or whether or not an individual had left the country. Congress made the admission that in 1996 a bill had been passed requiring the establishment of an entry/exit system at all American ports of entry – land, sea and air – under the Illegal Immigration Reform and Immigration Responsibility Act 1996.[16] This directive, handed down from Congress to the Attorney General was, however, never enacted due to pressure from trade lobby groups, who argued that additional identity-verification requirements at the border would lead to longer wait times and negatively impact the American economy. There were two attempts at a provision for an entry/exit system, first in 2000 with the Immigration and Naturalization Service Data Management Improvement Act, and then post-9/11 with the Patriot Act, with each attempt proving to be unsuccessful. Surprisingly, as of 2012, despite a further attempt within the framework of US-VISIT, the U.S. border still lacks the infrastructure to determine if and when a foreign national has left the country (Hite, 2007). Again, within the framework of the 9/11 narrative, the interruption of one terrorist attempting to travel to United States based simply on proper due diligence of the U.S. immigration system could have potentially disrupted the terror attacks.

For the 9/11 Commission, these four examples: a lack of counter-terrorism awareness amongst customs agents; the inability of the U.S. immigration and visa process to perform due diligence in the issuance of visas; the lack of timely sharing of terror information; and the inability for the INS to enforce immigration violations, not only led to a faulty immigration and border system but allowed for repeated abuse of the immigration system. While it is evident that this form of analysis by the Commission is clearly retrospective and may even suffer from hindsight bias, it does present a problematic of the securitisation of civil institutions that will be highlighted in coming chapters. This understanding of the security faults leading up to 9/11 conflates terrorism and terrorist planning and logistics with everyday civil practises of the visa, immigration and passport process.

1.4 9/11 and Intelligence Sharing (FBI)

Unlike the faults attributed to the INS and U.S. border security, those attributed to the FBI were focused on the agency's inability to share actionable information that was already in its

[16] Section 110 - Automated Entry/Exit Control System Requires the Attorney General to develop, by September 30, 1998, a system that will: (i.) collect a record of departure for every alien departing the U.S. and match the record against the record of the alien's arrival; and (ii.) allow the identification of non-immigrants who remain beyond their period of authorized stay.

possession internally between its intelligence and criminal investigation units. This inability to share has been termed the 'the wall' (FBI, 2002, p. 3). 'The wall' refers to the unwritten institutional barriers that governed the sharing of intelligence information obtained by FBI agents through the use of a FISA[17] warrant[18] that prevented the sharing of this information with other divisions of U.S. intelligence and law enforcement as well as with criminal prosecutors from the Department of Justice (DoJ) responsible for bringing FBI-led cases to trial. This institutional norm originated in the late 1970s in response to the Watergate inquiry, where it was revealed that the FBI, acting under the direction of the Nixon administration used its investigatory power to monitor political opponents of the White House. Further elaborated by the Church Committee[19] from the 1930s until 1976, the FBI had been responsible for intelligence gathering in relation to both national security and law-enforcement matters. For instance, during World War II President Roosevelt directed the FBI to expand its national security duties to include anyone suspected of 'espionage, sabotage or subversion' (Grewe, 2004). It has been further argued that during the postwar period the domestic intelligence-gathering activity of the FBI under Director J. Edgar Hoover expanded greatly, with the FBI establishing a covert action programme that operated from 1956 to 1971 against domestic organisations and, eventually, domestic dissidents. For instance, over the period of 1960 to 1974 during the height of the Civil Rights and anti-Vietnam peace movements more than one million files had been created on Americans and more than 500,000 investigations had been carried out by the FBI without a single court conviction' (Johnson, 2008). In 1976 the FBI's ability to use its intelligence gathering for purposes other than legitimate criminal or national security matters was curtailed. Up until 1976, in order for the FBI to gather intelligence for a criminal investigation, therefore obtaining a search warrant or warrant to perform electronic surveillance, agents were required to obtain the approval of a federal judge by presenting a case displaying probable cause. The FBI was not required, however, to obtain court approval for the same methods of search and seizure if the Bureau claimed that it was investigating 'agents of a foreign power'.

In 1975 this unregulated space of intelligence gathering came to an end and resulted in the creation of the Foreign Intelligence Surveillance Act 1978 (FISA) and corresponding Foreign Intelligence Surveillance Court (FISC), which required FBI agents wishing to collect foreign intelligence information to seek court approval – thus making foreign intelligence collection consistent with the procedures required for criminal investigations. The main purpose of FISA was to clearly define how intelligence gathering could be carried out so that the powers of search and seizure could not be applied to any such persons that were not clearly defined and court sanctioned. FISA also had implications for the DoJ since it was the department

[17] FISA refers to the Foreign Intelligence Surveillance Act that was passed in 1978 in response to the Watergate hearings and the subsequence Church Committee review on intelligence that found that President Nixon, along with a host of senior government officials prior to the Nixon presidency, had in fact obtained warrants for surveillance and wiretapping of American citizens under the guise that these citizens were connected to a 'foreign power'.

[18] A warrant that regulates the acquisition of surveillance information on those individuals who are deemed agents of a foreign power.

[19] The Church Committee was formally known as the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, a U.S. Senate committee chaired by Senator Frank Church in 1975.

responsible for the prosecution of criminal cases brought forward by the FBI. With the establishment of FISA, the Justice Department 'understood' that it could be briefed by FBI agents who had collected FISA-related intelligence but in no way could it direct or influence how the FBI carried out its investigation despite the obvious benefit to the DoJ to direct the FBI in order to maximise the evidence collection process and increase the chances of successful prosecution (Grewe, 2004). As a result, FISA created not just two, but three partitions in respect to the collection and sharing of intelligence. First, internally between FBI agents working on criminal investigations; second, between FBI agents gathering foreign intelligence; and third, between the Justice Department and their criminal prosecutors, who were responsible for turning both types of investigations into prosecutable criminal cases.

This tri-partitioning functioned more or less without problems until 1994, when during the prosecution of Aldrich Ames, a CIA counterintelligence agent accused of espionage, it was found that the FBI and Attorney General's office had signed a number of authorisations for foreign intelligence gathering after Ames had been indicted and where the intelligence gathered was to be used as part of the prosecution. This fact came to the attention of Richard Scruggs, head of the Office of Intelligence Policy Review (OIPR),[20] a unit that functioned as an internal regulatory body within the DoJ. Scruggs raised the concern that, since there had been steady communication between DoJ prosecutors and the FBI agents who had collected intelligence information under FISA, the judge presiding over the Ames case would throw it out on grounds of tampering, allowing Ames to walk free. Attorney General Reno was notified of this potential hazard, and in 1995, after Ames had been convicted, the OIPR was designated as the 'gatekeeper' that would determine under which conditions information could be shared between the DoJ and FBI when gathering intelligence specifically through FISA. In order to strengthen its regulatory standing, the OIPR sought an opinion from the Office of Legal Council (OLC) – also housed within the DoJ, who stated that 'although the law did not clearly require a primary purpose standard [outside of the standard already applied by the FISC], [the] courts were likely to apply such a standard anyway' (Grewe, 2004, p. 15). Therefore, the OLC recommended that the OIPR create a 'primary purpose' test in order to establish a consistent set of practises governing the acquisition of foreign intelligence by the FBI, and the subsequent communication of pertinent information to prosecutors within the DoJ. In July 1995 these guidelines were officially incorporated into the FISA court to govern information sharing. These procedures, however, applied only to the FBI and not the CIA or the National Security Agency (NSA), and they did not restrict information sharing within the FBI itself – that is, between criminal and intelligence divisions of the FBI – but only between the FBI and prosecutors. Sharing then could only take place when there was evidence of a criminal offence obligating the FBI and the OIPR to notify criminal prosecutors. Rather than leading to direct and clearly defined regulation of the communication between the FBI and the DoJ, hypersensitivity to the potential legal problems of sharing foreign intelligence information created a set of unintended consequences that

[20] The OPIR is now called the Office of Intelligence as part of the National Security Division with the U.S. Department of Justice.

were identified as institutional impediments involved in the intelligence response to the 9/11 threat.

FBI Director Robert Mueller III and former Attorney General John Ashcroft (2001–2005) have made numerous references to ‘the wall’ as a legal barrier that prevented the criminal and foreign intelligence divisions from sharing potentially pertinent intelligence information. However, as just described, no such law preventing the exchange of intelligence information gathered under FISA existed as an enforceable statute; rather, ‘the wall’ was created as a result of institutional internalisation of the sensitivities expressed by OIPR, along with the ‘guarding of one’s own [institutional] turf’ (Grewe, 2004, p. 35). This internalisation of unwritten rules, though thought to make intelligence collection more just, had negative consequences with respect to 9/11. The partitioning and establishment of a discrete approach is described as working quite well for traditional cases of espionage where an individual could be identified as an agent directed by a foreign power. Terrorist cases were different and presented additional levels of complexity. For instance, intelligence gathering in terrorism cases was likely required for multiple individuals, and pressing criminal charges against one or a group of individuals did not mean that the threat was necessarily extinguished and further intelligence no longer required. For instance, Osama Bin Laden was criminally indicted for his involvement in the 1998 bombings of U.S. embassies in Tanzania and Kenya, but he continued to remain at large. When confronted with further FISA requests for the monitoring of Bin Laden in the lead-up to the millennium, the OIPR was faced with a dilemma because it normally did not allow FISA requests to be made once a criminal case had been started. In order to work around this problem, and with the realisation of the urgency of monitoring Bin Laden, the OIPR and FISC resolved that the FISA requests could be granted, but the FBI agents working on collecting the foreign intelligence remained barred from sharing any relevant information with agents working on the Bin Laden criminal case without first seeking court approval.

During the summer of 2001 on two such occasions ‘the wall’ had a negative consequence in respect to intervention in the 9/11 plot. The first event involved the laptop and possessions of Zacarias Moussaoui, otherwise known at the 20th hijacker; the second related to information obtained by the NSA in December 1999 pertaining to Khalid al Mihdhar and Nawaf al Hazmi, the hijackers on American Airlines Flight 77 that was flown into the Pentagon. In August 2001 the Minneapolis FBI field office was notified by a local flight-training school that an individual, despite having very little knowledge of airplanes, wanted to learn how to ‘take off and land’ a Boeing 747 (Grewe, 2004, p. 28). The Minneapolis agent who received the call was concerned that the individual, Moussaoui, intended to hijack a plane, but since there was no sign of criminal wrongdoing, it was not certain whether or not Moussaoui could be charged and arrested. Lacking grounds for arrest, the agent decided to open an intelligence investigation and place Moussaoui under surveillance, whereby it was learned that Moussaoui was a French national and had overstayed the terms of his visa. On August 16 the INS detained him and on August 17 he was served a deportation order. Upon

Moussaoui's arrest, the FBI was presented with both his laptop and bag containing personal belongings. However, because Moussaoui was arrested for an immigration violation, the FBI agent was unable to access either of these items without a search warrant. Realising that a criminal warrant could not be obtained, the agent decided to pursue a warrant under FISA, remaining consistent with the parameters of the intelligence case he had opened. In order for a FISA warrant to be granted, however, the agent had to show that Moussaoui was an agent of a foreign power. The FBI agent could not, and Moussaoui was then deported along with his belongings, unopened and intact.

The second 'missed opportunity' concerned the sharing of information pertaining to Khalid al-Mihdhar and Nawaf al-Hazmi. In 1999 the NSA identified al-Mihdhar at a known terrorist training camp in the Middle East and tracked him to Kuala Lumpur, where he met Hazmi and one other unknown individual – later identified as Fahd Mohammed Ahmed Al-Quso, who is known to the FBI as involved in the Al Qaeda bombing of the USS *Cole* in 2000. The three men travelled to Bangkok on January 8, 2000, at which point the surveillance ended. The NSA relayed information to the intelligence community concerning the travel routes and terror links pertaining to each individual, but the information came with a set of 'caveats' or guidelines that prevented sharing it with FBI agents working on criminal investigations without first obtaining permission from the OIPR. In May 2001 an FBI analyst assigned to the intelligence investigation of the October 2000 USS *Cole* bombing in Yemen – a criminal case was also opened on the bombing at the same time by the DoJ – was able to review the photos gathered by the NSA and identified Al-Quso. The analyst was also aware that Al-Quso had travelled to Bangkok to deliver money to a man named Tawfig Bin Attash, who was known to have links with Bin Laden. When the analyst spoke with a CIA agent who was also working on Cole-related matters, the agent suggested that she talk to FBI agents in New York involved in the Cole criminal case. The analyst, accompanied by the CIA agent, proceeded to show three photographs of the meeting between al-Mihdhar, al-Hazmi and al-Quso to the FBI, after which she was confronted with a series of questions: 'why were these photographs taken, why were these people followed, where were the rest of the photographs' (Grewe, 2004, p. 31). Aware of the NSA caveats, the analyst refused to provide any further information regarding the context and underpinnings of the photographs, citing that she was prevented from doing so as a result of 'the wall'. Surprisingly, the CIA agent present also had quite detailed information of the Kuala Lumpur meeting, but he was not asked about what he knew, nor did he offer any of this information to agents – later stating that the CIA was not authorised to answer intelligence-related questions from the FBI. Agents left the meeting without learning that al-Mihdhar had a U.S. visa indicating he planned to travel to New York, that al-Hazmi had travelled to the United States in 2000 or that it was in fact al-Mihdhar and al-Hazmi who were in the company of Al-Quso in the Kuala Lumpur meeting.

1.5 A layered Approach to Security

These examples show that the security breakdown that played a role in 9/11 cannot simply be attributed to the tactics of an intelligent adversary or the fulfilment of a radical ideology oriented towards the destruction of the United States. Rather, 9/11 was made possible in part due to the discontinuity within operational governance of U.S. intelligence, law enforcement and immigration services. What is significant about this attribution of fault to both the INS and FBI is that the reaction post-9/11 has seen the DHS take on an active role in counter-terrorism practises, whereas the FBI has moved more directly into the civil sphere. This closure of the gap between civil administration and intelligence practises has been made possible through an interconnected set of legal, policy and technological developments. First, there has been the creation of new legal definitions allowing for the designation of identity information on foreign nationals as subject to collection and analysis. Second, the DHS has deployed biometric, data-mining and data-sharing technology in order to provide a greater amount of information on the behaviour and social networks of individuals entering the country. Finally, civil and intelligence institutions have shifted towards a counter-terrorism mandate or the wholesale placement of civil institutions under supervision of intelligence agencies. As a result, these multiple layers provide a greater number of opportunities for intelligence, law enforcement and civil service to monitor and intervene on a threat while simultaneously raising issues concerning the use and extension of executive power.

Empirically, this process of reform, most visible within U.S. border security and immigration practises, has resulted in the development of a series of interrelated programmes and technologies to better manage foreign nationals at the level of the individual, the subclass or nationality. These initiatives, to be taken up sequentially in this thesis, can be identified as:

- [Layer 1] The development of a legal framework that allows for the appropriation, analysis and sharing, when appropriate, of foreign national identity information. This legal framework allows for a much more permissive and flexible environment through which U.S. intelligence, law enforcement and immigration can identify threats and manage the foreign national population travelling in and out of the United States.

- [Layer 2] The creation of the Student and Exchange Visitor Information System (SEVIS), the first programme developed after 9/11 responsible for the tracking of all foreign students and exchange visitors that places minimum requirements on enrolment as well as the certification of the educational institution itself.

- [Layer 3] As mentioned, the establishment of US-VISIT, first installed at all air and sea ports of entry, to collect fingerprint biometrics from all foreign nationals entering the country in order to verify the identity of the individual to be matched against subsequent enrolments upon re-entry into the United States and to be matched

against FBI terrorist and criminal watch-lists; where this process of biometric has been expanded to include the U.S. theatre of war, such as Iraq and Afghanistan.

- [Layer 4] The collection and analysis of Passenger Name Record (PNR) data that is understood as all of the biographical information – passport number, credit card number, meal preference, seating preference – entered by a traveller wishing to board a flight to the U.S.

This new security logic, one that seeks to close the security gaps exploited by the 9/11 hijackers as well as create a space where new technologies and methods can provide U.S. security services with greater understanding and realisation of terrorist threats, cannot only be seen as interconnected, but can be understood as being composed of multiple layers. These layers operate from the macro to micro levels. Each layer then reduces the probability that a known terrorist would be able to travel to the U.S. undetected. However, the use of the term 'layered' should not be understood as a 'stack'; that is, this term seems to suggest that there is one security feature after another through which the unsuspecting international traveller must pass. Rather, each function can be understood as concerning the analysis and scrutiny of different aspects of the individual based on the different population categories in which they are found. For instance, changes in the visa application process are pronounced in respect to those individuals who require a visa to enter the U.S. – students, members of non-VWP countries, and those entering for business reasons. The collection of biometrics comes to include this first category of visa holder but is directed primarily at VWP country nationals, who make up the bulk of the population of international travellers crossing U.S. borders. The analysis of PNR applies not only to foreign nationals but to U.S. citizens whereby a distinction is made over the extent of data gathered on foreign vs. U.S. citizens – for instance, U.S. citizens can only have the information that is printed on an airline ticket gathered, whereas for foreign nationals the DHS collects all information associated with the travel process. This form of layering adds not simply greater or more astringent security functions to the understanding of border security, but security functions that can provide dimensionality with respect to the individual. This dimensionality then allows for security services to make a multiple set of decisions or evaluations of the individual given the collection of predicates associated with a given individual or population.

❖ ❖ ❖

This opening chapter has laid out the three questions that this thesis will ask as well as identified four 'layers' or empirical sites of security through which post-9/11 U.S. homeland and border security can be evaluated. This chapter has also highlighted several important responses made by the U.S. government to address or correct these problems

that come to define the key socio-political changes in the post-9/11 period. First, formerly civil institutions and processes involving immigration and visa issuance have been securitised or placed under the auspices of the FBI. Second, new and novel sets of technologies have been deployed in order not only to track and verify identity but also to make the visa issuance and travel process less prone to error and abuse. Finally, new legal permissions have been established in order to enable greater sharing of intelligence information and now information gathered as part of the visa and immigration process, between various U.S. security services and law-enforcement bodies. In the coming chapters it will be shown not only how these new innovations and changes perform within the U.S. border security regime but how each are limited and shaped by both external and internal forces. Prior to the empirical analysis of each security layer, a literature review focused on the dominant themes of technology, sovereignty and risk will be presented, as well as a presentation of the methods used to conduct the research presented in the text.

2. Literature Review: Sovereignty, Technology and Risk

2.1

As introduced in Chapter 1, the two major structural changes that have taken place within U.S. transatlantic border security practises as a result of the 9/11 terrorist attacks can be seen as the following: (i) The consolidation of civil institutions responsible for the management of foreign nationals entering and residing within the United States with those institutions responsible for domestic security, intelligence[21] and counter-terrorism; and (ii) the deployment of new technologies for the purposes of identity verification as well as sharing of both intelligence and identity information. Importantly, however, what provides the ground for these transformations are two further operations, namely: (iii) the development of a national security legal framework that allows for greater powers of data collection, sharing and analysis by U.S. intelligence, border security and law-enforcement; and (iv) the shift within U.S. national security policy to a view of the threat of terrorism as not only 'catastrophic' in impact and 'generational' in duration but requiring war-like readiness and response (NSHS 2007).

The question that these four operations necessitate is how does each practise contribute to a strategy of homeland security or an understanding of a new mode of security? In respect to the broader social science literature on homeland and border security and the 'war on terror' (WoT), this answer is presented according to four interrelated discourses or bodies of literature. They can be seen as the discourse of: (i) *Sovereignty*: the role of sovereign or executive power during times of national emergency that is described by the Schmittian phrase 'state of exception' as reconstituted in contemporary social philosophy by Giorgio Agamben; (ii.) *Risk*: the social science discourse of catastrophic risk as applied to terrorism where prevention and precaution have come to play central roles; (iii) *Technology*: the role of identity, knowledge-discovery and database technologies that on the one hand can be described as providing intelligence agencies with greater information on foreign nationals entering the country, and on the other can be viewed as a form of additional surveillance of the civil population; and (iv) *Governmentality*: a fourth branch of discourse that seeks to synthesise the multiple elements of population management and governance that can be imported into the field of security actions. It will be argued that while each of these discourses frames the debate surrounding homeland security strategy post-9/11, each category suffers from a set of limitations. The first is the limitation of unity. The discourses of sovereignty, risk and techno-surveillance each announce themselves to be the dominant mode of operation in respect to defensive measures against terrorism. Here U.S. homeland security is defined solely in terms of sovereign power, risk assessment or surveillance, as opposed to the interrelation of these three attributes as was described in Chapter 1. Second, each suffers from a limitation in scope. Due to the focus on the response of U.S. policy to the threat of terrorism, scholarship has focused primarily on the tactics of lawmakers, law-

[21] Subsequently, this consolidation of civil institutions with those institutions responsible for domestic intelligence has broadened the 'remit' for what domestic intelligence is to include. For instance, while counter-terrorism practises administered by the FBI are oriented towards identifying and investigating threats present within the country, this new approach via the tools employed in respect to the border allows domestic intelligence to gain a greater awareness of threats travelling to the United States.

enforcement and the military. As a result, there has been a lack of attention given to other social factors that can be seen to shape the legal, military and police response to terrorism – namely, economic and constitutional factors or interpretation. The third limitation is that of differentiation. While each of these discourses makes valid arguments and observations regarding how U.S. anti-terror and border security operates, there is a lack of precision as to how law, risk and surveillance work together to impact the travelling population entering the U.S. For instance, although the U.S. transatlantic corridor has been securitised since the 9/11 attacks, the greatest amount of scrutiny has been applied to the subset of foreign nationals seeking to enter the country. Furthermore, within that subset an additional subset can be found that distinguishes individuals from low-risk countries – Visa Waiver Program (VWP) countries – from those considered to be from high-risk countries, which are all non-VWP. These discourses then cannot be understood as universal or applying to all travellers as such. Rather, more specific arguments need to be fashioned in order to match the appropriate set of descriptions in relation to specific practises of border security. This thesis will seek to overcome these limitations in the following chapters. Limitations notwithstanding, each of the four bodies of literature as outlined contributes to a description of a new form of security governance within the context of U.S. post-9/11 border security. This mode of governance is typified not only by its multiplicity, where homeland security strategy is made operational through technologies of identification, institutional prerogatives of risk assessment and legal provisions that afford greater flexibility to intelligence and law-enforcement, but by the motivation of gaining greater informational awareness of the travelling populations travelling to and within the country.

2.2 Two Concepts of Security

Prior to discussing the concepts of sovereignty, risk and technology it is important to consider how the notion of security is defined within the social science literature to determine potential trends inherent in the process securitisation. According to the New Oxford American Dictionary (OAD), 'security' is defined in the first instance as 'the state of being free from danger or threat' (OAD, 2010). Following this notion of threat, security can also be associated with job security, as well as with a form of human security with the natural and technological environment – 'maximum security against toxic spills'. The OAD further defines security to be 'the safety of a state or organization against criminal activity such as terrorism, theft, or espionage' where security is used in the statement 'a matter of national security'. Finally, this definition can be traced etymologically to the Old French *securité* and the Latin *securitas,* which have as their base a definition of 'free from care'. Each of these definitions shows that the condition of security can be applied both to internal threats to the working of the state and to threats that potentially arise from outside the state, such as terrorism and espionage. What this definition lacks is that while it is oriented towards a condition of stasis or equilibrium and points to an end goal free from danger, it does not indicate how the condition of security is achieved by either government, military or law enforcement, nor does it account for the insecurity inherent in any such threat. It lacks a description of how such a

state of equilibrium is achieved. For example, Michael Chertoff, former Secretary of Homeland Security, as pointed out by Heng and McDonagh,[22] hints at the duality of the definition of security – the state of security and those measures that contribute to it – when he says: 'Our ultimate goal is a time when security measures are a comfortable, convenient part of our routine; a time when people go about their daily lives mindful of risks but not encumbered by fear, unwavering in their resolve and full participants in their own protection' (Chertoff, 2005, p. 2). Here the objective of the establishment of a new norm in respect to homeland security can be seen: one that obfuscates the processes through which the state of security is achieved. It is precisely the aim of this thesis then to interrogate and analyse those very process that contribute to the 'new normal' or a state of security that is 'convenient and routine'. As a result, two further competing definitions aid in thinking of security as a process. The first is offered by Weaver, Buzan and Wilde, who argue that security is a response by the government or the military to an emergency situation or existential threat (Buzan, et al., 1998); the second is offered by Foucault, who argues that the condition of security is one of management, where threats are viewed in terms of events that occupy a series that can be statistically understood and brought within acceptable limits or, within a 'limiting bandwidth' (Foucault, 2007, p. 25). Both of these perspectives play a role in the understanding of the rationales of post-9/11 security in that the U.S. government can be seen to struggle with an event that due to its catastrophic nature cannot be normalised like crime control.

In Security: A New Framework For Analysis, Buzan, Wilde and Weaver argue from an international relations perspective that the traditional military/political understanding of security is one that relates to the concept of survival and can be described as a 'function for the state to mobilise' or 'take special powers in response to an existential threat' (Buzan, et al., 1998, p. 21). As a result, this condition of security brings about from the perspective of government a response that can be described as a 'state of emergency' whereby the government must perform certain actions not deemed permissible in respect to 'normal' political situations. For Buzan, Weaver and Wilde (Buzan), this situation of security should be distinguished from one that motivates a process of politicisation – that is, the process of security moves away from solving a problem politically and passes that problematic onto the military, intelligence and law enforcement. While governments can break rules for many reasons – not simply in respect to the emergence of existential threats – existential threats are described as the legitimising condition for the breaking of peacetime rules due to the recognition of the securitising action as a matter of 'priority'. This securitisation process impacts society differently and is seen to be dependent on whether or not the state is strong or weak. For example, Buzan argues that in states with strong bureaucracies as well as checks and balances between various branches of government, the armed forces or intelligence services may carry out actions in order to keep the state secure, yet these actions need not enter into the general political debate. In weak states the process of securitisation becomes more prevalent throughout the society since these states, such as

[22] Heng and McDonagh, *Risk, Global Governance and Security: The Other War on Terror* (Routledge, 2009).

the USSR under Stalin or Nigeria under Abacha,[23] push 'much of normal politics into the security realm' (Buzan, et al., 1998). This point is supported in this thesis and in much of the discourse and debate concerning homeland security and the war on terror, since it precisely demonstrates the placement of normal political practises, such as immigration and international travel under the heading of security. Methodologically, Buzan also states that the process of securitisation carries with it certain rhetorical or semiotic characteristics that at the level of discourse can be further understood as the difference between choice (politicisation) and necessity (securitisation). In respect to security discourse, the politicisation of an issue is one where the 'issue appears to be open, a matter of choice, something that is decided upon and therefore entails responsibility'. The securitizing speech act however works to present an issue as urgent and existential, as containing such importantance that it should not be 'exposed to the normal haggling of politics but should be dealt with decisively by top leaders' (Buzan, et al., 1998, p. 28). While this observation is compelling and of potential interest to this study, the analysis of discourse that is taken up is primarily focused on the identification of regularities within the discursive archive of the short history of U.S homeland security practises – rather than an analysis of the rhetorical system of members of the Bush or Obama administrations. A final point of consideration offered by Buzan is: In the face of an emergency situation, how and with what urgency does a government or institution respond? Or, if the situation truly presents an existential threat or crisis, what motivates an effective response? In order to best answer this question, a more expansive understanding of security is required, since post-9/11 border-security practises do not only operate as a result of the formulation of a discourse of necessity, but are enacted through the interface of this discourse with technological innovation, economic need – in respect to open borders and exchange – and day-to-day institutional practise in fact responsible for enforcement. This additional conceptual support required for the analysis of post-9/11 homeland security practise can be seen to be answered in part by Foucault's description of security.

In the text Security, Territory, Population, Foucault begins by asking the question, 'What do we understand by security?' Unlike Buzan, Foucault does not offer an answer to this question that arises in respect to conflicts or threats emerging from the anarchy of the international system, or the anarchy of individual choice associated with a Hobbesian state of nature (Gearty, 2010); rather, it is located within the technologies and practises the state employs to manage and govern in response to an undesirable or unwanted event (Foucault, 2007, p. 15). For Foucault, this security practise is actualised through the implementation of economic rationales that require an understanding of the event in relation to a given population. Foucault argues that the securitisation concerns how best government can place the given security issue – crime, disease, food scarcity – 'within socially and economically acceptable limits and around an average that will be considered as optimal given social functioning' (Foucault, 2007, p. 16). An 'acceptable limit' can be understood in two ways, historically appearing for Foucault with the arrival of modernity and the nation-state of 18th-

[23] General Sani Abacha was the de facto President of Nigeria from 1993–98.

century France. First, it is discovered that society cannot be governed or made secure by law alone; new 'supervisions, checks, inspections' must be put in place in order to determine whether or not an individual will commit a crime (Foucault, 2007, p. 15). Second, society within the context of the nation-state comes to be understood as a population that is not only defined according to its linguistic, religious or ethnic uniformity or necessarily with the drawing of national boundaries, but through rates that are understood through the use of statistical technologies. As a result, the population comes to be recognised for its own law-like qualities, such as 'death rate, incidence of disease, regularities of accident' that become the object of focus for government (Hacking, 1990). Foucault argues that instead of the sovereign creating a binary relationship between what is permitted and what is prohibited, the 'phenomenon in question' is understood in a 'series of probable events' where this probabilistic rationale lends itself to the development of anticipatory policies as well as the recognition that the event is part of a wider consideration of economic cost and valuation (Foucault, 2007, p. 18). Foucault describes this relationship as the cost of repression versus that of delinquency. This understanding of the event as belonging in a series and the product of a given population forms what Foucault calls a milieu that then can be properly ascertained, defined and modified. What is also of particular interest in the understanding of the milieu is that the effective construction of techniques deployed by government are meant to respond to the very regularities that are determined to be natural to the environment. This means that when security is applied, the objective is not to disrupt or prevent the normal actions of the society to be carried out – the Chertoff quote earlier in the Chapter illustrates this – but, rather, to distinguish negative from positive elements, manipulating those variables that allow for a laissez-faire quality while providing increased security. A prime example of this as applied to post-9/11 border security is the addition of biometric screening of foreign nationals as they enter the United States. The objective here is not to prevent entrance of the entire group, but to alter the border zone from a zone purely oriented towards identity verification to one that concerns intelligence collection and risk assessment.

In contrast to Buzan's conceptualisation of security where security is viewed as a response to an emergency situation that derogates from established norms and rules, Foucault's description works to identify and track how the process of security is carried out as a practise and rationale of government. While Foucault emphasises the practises involved in how the state gains self-understanding and works to manipulate the natural qualities inherent in the population and its relation to economic processes, this definition need not be inconsistent with the definition offered by Buzan & Weaver. When the two definitions are compared, it can be seen, as in the example of the threat of Jihadist terrorism – a threat that exists at the intersection of the national and global – that the response to the emergency is carried out with urgency derogating from established norms and rules, but also operates at the level of the population, employing methods and technologies that allow for both greater awareness and manipulation of that very population. In a departure from the definition offered by the OAD, security is better understood as a process or operation, rather than a state of being.

2.3 Sovereignty

The debate concerning the role of sovereign power during times of emergency has been prominent within the social science circles focused on the post-9/11 period. The figures that feature prominently in this debate are philosopher Giorgio Agamben, who argues against such powers, and the American legal scholars John Yoo and, separately, Eric Posner and Adrian Vermeule, who argue for the exercise of increased executive power. The criticism of this theory is expressed as follows: first, the expansion of sovereign power during times of emergency leads to what is called a 'state of exception' (Agamben, 1998, p. 8) in which emergency procedures that are considered supra-legal override legal mechanisms in place during normal times – this overriding of legality is presented as problematic, since the actions employed by intelligence and law enforcement along with key decision makers are seen to bypass institutional measures of accountability and carry out what in this case Agamben terms 'sovereign violence' or violence beyond the law (Agamben, 1998, p. 20). In contrast, the positive theory of sovereign power contends that emergency powers are warranted and governmental oversight should be muted during times of national crisis for the precise reason that addressing the emergency requires both speed and institutional efficiency, which otherwise could lead to the loss of life if obstructed by bureaucracy (Vermeule & Posner, 2007) (Yoo, 2006). Although each of these positions can be seen as being in opposition with one another, each can be traced to the work of the modern Weimar Jurist Carl Schmitt.

In the text Homo Sacer, Agamben argues that Schmitt's notion of sovereign power creates a paradox as a result of the sovereign's ability to exist both inside and outside the established legal order (Agamben, 1998). Agamben sees this ability to move inside and outside as creating a permanent 'state of exception' whereby the sovereign is given the ability to 'decide if the constitution is to be suspended *in toto*' (Agamben, 1998, p. 12). This concept of the sovereign as the original mode of the state, able to make a decision on whether or not to suspend the constitution in times of emergency, must be placed in context. The basis for this concept can be found in the text Legitimacy vs. Legality written by Schmitt during the height of the constitutional crisis of the Weimar Republic prior to its collapse in 1934. While Schmitt can be read as offering a mode of governance that supersedes the established legal order in Political Theology – the figure of political power highlighted by Agamben – the sovereign power Schmitt argues for is one that answers the perceived problems of excessive deliberation and bureaucracy found within parliamentary democracy. Schmitt argues that rule by majority, satisfied by a simple 51%, creates a system where legitimacy and legal power act as a neutral edifice since the state is only concerned with its own structural characteristics and becomes blind to deeper questions of justice and injustice that impact the minority – or the 49% of the population. As a result, the power afforded to the parliamentary legal apparatus is one that is 'hollowed out' since it is concerned with its own procedural formalities rather than actual needs of all constituents. Schmitt argues that this mode of political and legal calculation is acceptable during normal times, but becomes intractable

during times of emergency or conflict. For instance, concepts such as ‘danger’ and ‘emergency’ are bound to the immediacy of the situation and the legal holder of state power (the parliament) will presume that legality can always provide the solution to such ‘hard cases’. Schmitt, however, argues that solutions to such immediate problems cannot be produced by a system that functions according to excessive deliberation and compromise. An example of such a ‘hard case’ within U.S. counter-terror practises post-9/11 is the case of the detention of suspected terrorists captured shortly after the invasion of Afghanistan at Guantánamo Bay. These prisoners, presumed to have links to terror organisations, are viewed as too dangerous to be released, yet due to the legal framework under which they are held as ‘enemy combatants’, they cannot stand trial so that innocence or guilt can be determined. As a result, ‘in a race between the executive and the judiciary, the judiciary will arrive too late’ (Schmitt, 2004, p. 30). Schmitt further asks of these difficult cases in times of conflict or emergency, who in fact will be given the responsibility to resolve differences of opinion? The answer appears to be straightforward: an ‘impartial third party’ who decides on the conflict ‘whether judicially or otherwise’ (Schmitt, 2004, p. 31).

For Schmitt, the way through this paradox is not found in a contradiction embedded in Article 48 (A.48) of the Weimar Constitution, but, rather, to the permanent establishment of an impartial third party. Article 48 – the impetus for Schmitt critique – known as the ‘emergency decree’ article, allowed the president under special circumstances to create legislative decrees without receiving prior consent from the Reichstag. What provided flexibility to A.48 was that it did not specifically define the meaning or nature of a ‘special circumstances’ and thus, according to Schmitt, was responsible for the creation of a ‘second constitution’ (Schmitt, 2004, p. 78). This contradiction was actively used by the Weimar presidency, first during the period of 1918 to 1919 to quell post-war civil unrest and then frequently throughout the next decade by President Friedrich Ebert, who used it as a tactic to work around the parliamentary process. Schmitt’s critique of parliamentarianism can thus be understood less as a theoretical critique of the constitutional order rather than an expression to correct the inherent contradiction plaguing the Weimar Republic’s political system. As described, the solution proposed is the installation of an ‘extraordinary lawgiver . . . who would hold a dominant place within the legislature and instead of being subject to the detached legal edifice of the parliamentary process would be in direct contact with its subjects though a plebiscite’ (Schmitt, 2004, p. 64). This extraordinary lawgiver would then be granted the powers of parliament – that is, the power to determine the ‘state of exception’ in which certain duties and rights may be suspended, such as basic freedoms and protection of property, and whereby degrees issued by this lawgiver would be constitutionally valid and contain the force of law. The ‘state of exception’ here is defined as an extraordinary situation where the ‘state remains while the law recedes’ (Schmitt, 2006). The lawgiver therefore ‘unites in himself law-making and legal execution and can enforce directly the norms he establishes which the ordinary legislation or parliamentary legislative state cannot do’ (Schmitt, 2004). As a result, the lawgiver rules according to legitimacy rather than legality, which in the context of the Weimar republic had for Schmitt appeared to be contradictory.

This description of sovereignty necessitates two questions that are expressed in the work of Posner/Vermeule/Yoo and Agamben. Posner/Vermeule/Yoo: To what degree is sovereign authority afforded to the U.S. president in his or her capacity as commander in chief of the armed forces in respect to safeguarding national security in response to emergency situations and/or war? For Agamben: If the sovereign stands both inside and outside of the legal order and is effectively able to create new conditions of political practise outside of established legal norms, how can this form of politics be accounted for – made accountable – let alone be curtailed so that it does not occupy the space of sovereign violence?

As presented by Posner, Vermeule and Yoo, an increase in presidential authority during times of war and in the face of an emergency is advocated. The argument is made in two ways. First, in a positive approach by Yoo, who argues that during times of war the president, sanctioned by both precedent and constitutional permissions, is granted the 'authority to decide wartime tactics and strategies' that may or may not require congressional or judicial oversight (Yoo, 2006, p. 6). Second, in a negative approach argued by Posner and Vermeule, who find that due to the unexpected nature of an emergency situation such as a terrorist threat, it is only the president who is in the most efficacious position to respond as a result of the relationship with the military and the various branches of U.S. intelligence. Congressional deliberation or court involvement would lead to delays, harming national security since each of these branches of government, while far-reaching, are deprived of the rich sources of national-security information offered to the president (Vermeule & Posner, 2007). Yoo contends that much of the controversy over national-security decisions made by the Bush administration, such as the stripping of Geneva Convention prisoner of war rights or protections from so-called 'enemy combatants' held in Guantánamo Bay and the lowering of standards for obtaining search warrants and the warrantless wiretapping of major U.S. telecommunications providers (AT&T, Verizon) from 2001 to 2005, was due to confusion over whether or not the war on terror could actually be deemed a war (Yoo, 2006). For Yoo, the catastrophic nature of the terrorist threat made it necessary for the president to adopt wartime powers in respect to national security, thus extending the role of presidential authority during times of emergency. If counter-terrorism were left to traditional law enforcement and the criminal justice system, then the 'U.S. would be limited' in its fight against Al Qaeda with a system subject to 'protections and delays' (Yoo, 2006, p. 10). That is, the criminal justice system would not only require that captured members of Al Qaeda be allowed the right to a fair and open trial with sufficient safeguards regarding the quality of evidence presented, but it would also potentially compromise counter-terrorism programmes due to the release of intelligence gathered as part of counter-terrorist activities. This argument is grounded by a further operative assumption that can act as an introduction to the next section; namely, concerning risk management and preventative practises. For Yoo, not only is the criminal justice system expensive, ridden with delays and prone to mistrial or

acquittal due to the high standards on evidence,[24] but it is primarily posteriori in its orientation. The criminal justice system is concerned with accounting for and bringing to justice those groups or individuals that have already caused harm. What is required during times of war is a future-oriented approach that works to prevent terrorist attacks that carry the potential of catastrophe (Yoo, 2006) (Bobbitt, 2009). How wartime powers are evoked by the U.S. presidency in the case of domestic surveillance and homeland security is the subject matter of Chapter 4, but what is important to highlight is that Yoo's discourse supports the two definitions of security offered by Buzan and Foucault and can be seen to intersect with Schmitt's description of sovereign power. That is, not only should the executive be afforded greater agency in order to address an emergency, therefore departing from established norms and rules, but the end goal is not to bring a fixed end to conflict, but to prevent a future threat or risk from occurring. Post-9/11 anti-terror policy therefore combines both the strategy of the 'exception' and the confrontation of the emergency situation with that of the 'management of the event' extended over the duration of perceived threat. Hence the exception and the exceptional powers afforded to the executive in order to confront the emergency situation, due to a perpetual state or readiness, become the new norm. This new norm is then incorporated into the day-to-day practises come to be understood as the institutional workings, in this case of the U.S. border security system. This is the key point in understanding the governance of U.S. homeland and border security post-9/11, which is a central motif in this study.

Posner and Vermeule offer a further defence of executive agency during times of war or emergency, arguing that the executive should be afforded 'deference' on the part of the judiciary, since it is the government that is best able to provide the security needs to the constituency, where security can be understood as a social good (Vermeule & Posner, 2007). While Posner and Vermeule indicate that deference should apply only if the actions taken by government are rational, they also suggest that government is no less problematic or error prone during normal times than it is in times of emergency[25] and further intervention in the decisions of the executive by the courts or another third party would then lead to additional errors or inefficiencies. This deferential approach is embodied in what Posner and Vermeule describe as the 'security/liberty' frontier, a reciprocal relationship between the amount of security or liberty afforded to a given situation – greater security, less liberty and vice versa. However, this relationship is not one-to-one; security is afforded a greater weight than liberty for two reasons: (i) security is viewed as a greater social good than liberty since it

[24] A further argument supporting the establishment of military tribunals for cases related to terrorism and other forms of national security is due to, in the majority of cases, the inadmissibility of evidence gathered by the intelligence community in order to identify and apprehend a felon. This inadmissibility of evidence into a criminal trial setting is argued to be problematic for two reasons: first, it might reveal intelligence-gathering techniques that would potentially harm national security; second, it might reveal actionable intelligence that could harm ongoing investigations. It also has the potential to reveal inconsistencies between the methods used by the intelligence community and those in law enforcement that would result in certain bodies of evidence not to be considered in a trial.

[25] While this argument on the surface is compelling – government is always error-prone, therefore we need to accept that these errors are aregular occurrence that citizens must cope with – it is problematic, as it is clear that the context of the national-security situation is vastly different, since the government is charged with making decisions that involve life and death scenarios.

affords welfare to the entire polity;[26] and (ii) liberty in itself is an elusive term that cannot adequately be measured due to its many definitions and standards.[27] This distinction is represented in a quote from the work of the sociologist John Elster: 'the metric for liberty is more difficult to determine, since the value including such disparate components as freedom of speech, freedom of association, due process and privacy. To get around this problem we basically have to ignore it' (Vermeule & Posner, 2007, p. 118). Interestingly, Posner and Vermeule appeal to a Schmittian thesis to further support their arguments concerning executive deference during times of emergency due to the conceptual difficulty of defining emergencies ex ante. As a result emergencies must be governed by ex post standards and as a result, due to procedural tendencies of 'legal theorists', the response to the emergency is impeded whereby a strictly legislative approach 'ignore[s] or underestimate[s]' both the costs of the legal process as well as the opportunity-cost of government actions that lead to protracted deliberation and unwanted bureaucracy (Vermeule & Posner, 2007). Posner and Vermeule, however, do not feel that this position in any way contributes to a form of encroaching authoritarianism that would somehow be triggered by the claiming of greater powers by the executive during the emergency. Instead, they offer that, at least within an American context, it is merely civil libertarian panic that is ultimately responsible for this shadow hanging over perfectly rational actions made by the executive in response to an emergency situation.

What the arguments of Buzan, Yoo, Posner and Vermeule, and ultimately Schmitt, show is that a consistent set of arguments in respect to state action accompany securitisation or a response to a national emergency. These issues include the imperative for the monopoly over the decision by the executive, the ability for the executive to act in an unfettered manner devoid of oversight in respect to the execution of this decision on the emergency; and that the actions taken by the executive, even if they curtail liberty or have negative unintended consequences, serve the greater social good. This discourse as presented necessitates two further questions. First, a normative question as represented by Agamben, who argues that this form of sovereign power, one without accountability in respect to rule of law or procedural legislative oversight, inevitably leads towards sovereign violence – the question is whether or not this assertion is valid in all cases as well as in the case of homeland security. Second, although the proscriptive approach adopted by Yoo, Posner and Vermule argues for what 'should be done' in the face of an emergency, what is missing from this analysis is a description of precisely 'how' executive power has functioned since 9/11, and what the impact has been on security. How then are security practises carried out during times of emergency, and do these practises lead to sovereign violence?

[26] This notion of 'welfare for the entire polity' will be argued against in later chapters, because it is the core observation of this thesis that post-9/11 homeland and border security is afforded agency in respect to security operations based on increased scrutiny of the foreign national population. This means that security cannot be afforded to the entire polity since: the polity of domestic citizens does not have the same security measures applied to it and could in essence contain threats; and within the context of globalisation, a small yet substantial percentage of individuals that make up the polity are foreign nationals, precisely those whom this mode of security is intended to guard against.

One of the strongest critiques of the 'state of exception' can be found in Agamben's text Homo Sacer. This argument is based on the term 'bare life' or *homo sacer* – meaning a life that can be killed but not sacrificed – where 'bare life' is seen as the product or outcome of the issuance of the state of exception (Agamben, 1998). How does the state of exception lead to bare life? As noted earlier, Agamben identifies the paradox of sovereignty to be not only the monopoly on the decision held by the sovereign, but that this monopoly allows the sovereign to operate 'at the same time, inside and outside of the judicial order' (Agamben, 1998, p. 15). Agamben argues that this mode of sovereign power is not simply a theoretical construct but is deeply embedded within modern liberal democracy and is activated as form of violence associated with self-preservation and defence (Agamben, 2005). What differentiates this theory from the classical theory of sovereignty articulated by Hobbes in The Leviathan is that while each operates with a similar purpose – the provision of security as a social good during times of emergency – the mechanisms that provide the sovereign/Leviathan with legitimacy exist with a greater conditionality. While the Leviathan obtains political power through the transfer of anarchic self-interest said to be in the possession of all constituents in the form of a political covenant, this covenant indicates that the individual will give up his or her right to self-defence if the Leviathan acts as the sole provider of security. However, this covenant can be overturned if upon transfer of political power the 'artificial person' or state fails to deliver on its promise. However, what binds the multitude to the sovereign as artificial person is that the artificial person seeks to represent the multitude. This is highlighted by the historian Quentin Skinner, who paraphrases Hobbes by indicating that the 'the true status of a lawful sovereign is thus that they are merely "the Person representative of all and every one of the multitude' (Skinner, 2002, p. 198). What is evident from this description is that there is a connection between the sovereign or representative and the represented. The representative must have a close relationship with and be authorised by the multitude not only to possess legitimacy but to act in the multitude's name. How Agamben's rendering of sovereign power differs is that the 'state of exception', while activated according to the same pretence as the Leviathan, does not possess the conditionality of the represented or the multitude in order to bring it into being. This is the essential paradox highlighted by Agamben, that out of a situation of representation or legitimacy the sovereign or representative is able to act or obtain agency outside of the practises and norms validated by the represented.

Empirically, for Agamben, the zones where the sovereign exception is most present are those locations that exist in relation to liberal democracies, yet remain legally undefined or obscured. For instance, border-zones that are jurisdictionally questionable, or a more common feature within recent European and Middle Eastern history, the sequestering of displaced foreign-nationals – Palestinians, paperless refugees that notably congregated in Calais, France, within camps as they attempted to travel to the United Kingdom. The camp exists not only as a site where the sovereign exception can function, but where the sovereign can exert unimpeded violence: 'it is useful to investigate . . . [the camp] . . . [since it is a

place where] the juridical procedures and deployments of power by which human beings could be so completely deprived of their rights and prerogatives that no act committed against them could appear any longer as a crime' (Agamben, 1998, p. 166). What is compelling for this study is that this conceptual description of the exception need not be actualised only within the context of the camp; rather, spatial location of the exception can be attributed to any institutional setting where the jurisdictional rights of the individual are called into question – for instance, in the case of foreign nationals within the context of the border.

Agamben's account of the state of exception has not escaped criticism from social scientists that are concerned with similar state power dynamics regarding modes of governance. Unlike Yoo or Posner, who appeal to constitutional precepts when evoking the primacy of state power, Agamben appeals primarily to the philosophy of Schmitt and Benjamin – that sovereign power is predisposed to violence – and in doing so arrives at a set of conclusions that have brittle empirical support. For instance, the state of exception is a condition through which the sovereign explicitly is able to choose between life and death of a given subject or population; yet, as it has been argued in Chapter 1, sovereign power, even if directed at a population without representation, has not arrived at a decision between life or death; rather, the institution of a layered form of security responsible for the vetting and risk assessment of the travelling population. In a further challenge to this position, Rose and Rabinow argue that Agamben's framework simplifies the empirical nature of government, where Agamben fails to consider the conflicting nature of government that typically works in a counter-productive or fractured manner when seeking to attain its goals (Rose & Rabinow, 2003). Also, while that state of exception can be described as a general form of governmental conduct exerting power from the top down, Rose and Rabinow argue that Agamben does not account for other and perhaps more prevalent strategies of subjection; namely, those modes through which individuals 'can be brought to work on themselves under certain forms of authority in relation to truth discourses' (Rose & Rabinow, 2003, p. 197). For Rose and Rabinow, these truth discourses do not simply include the legal dictates of the state, but the multiple forms through which governance is realised and authority exerted – medical, genomic, economic and penal. It is thus necessary to look at the multiple modes or practises through which the exception is not only embodied, but is realised in a governmental form – a form that while seeking to assert itself is limited, bracketed and directed by other social forces or actors, whether technological, constitutional, economic or otherwise. In the context of post-9/11 transatlantic border security, this governmental form is realised within a risk-based policy orientation – namely, precaution and preclusion – and through the deployment of digital-identity technologies that not only creates new 'circuits' of state power, determining who can enter the United States and who should be turned away, but provides the very evidence or information through which the risk assessment can be performed (Rose, 2000).

2.4 Risk

As presented in the introductory chapter, the policy orientation of U.S. homeland and border security can be seen as motivated by risk-based technologies and rationales of prediction and preclusion. These technologies and rationales seek not merely to allocate security resources in response to a terrorist event but work to prevent an attack while a terrorist plot is coming to fruition, or to preclude the possibility of an attack by denying certain risky individuals from entering the country. This mode of risk, one that is discrete in its orientation and focused on the mitigation of low probability but high-impact events, will be addressed in this section.

Within social science literature, the declaration of terrorism as a catastrophic threat can be found foremost in the work of Ulrich Beck, where terrorism is made analogous to ecological or financial disasters as part of Beck's taxonomy of 'World Risk Society' (WRS) (Beck, 2003, p. 45). WRS is an appendage that has grown out of a discourse developed in Beck's seminal Risk Society (1992), which concerns the potentially uncontrollable or incalculable risks that have accompanied scientific modernity (Beck, 2009). This theory is best illustrated with the example of chlorofluorocarbons (CFCs) and their unknowingly harmful effect on the environment. Although the chemistry behind CFCs was developed in the 1890s and where CFCs made it into mainstream consumer culture shortly after WWII under the trade name Freon – used by DuPont primarily in refrigerators – it was only in 1974 that CFCs were found to contribute to ozone depletion, which ultimately had an impact upon humans and their lived environment at the global level (Beck, 2006). Beck argues that in the response to the unintended consequences created by scientific invention or modernity, it becomes incumbent upon science, the state or military to attempt to find solutions. Problematically, however, these solutions are hard to come by, since many of the problems that arise within the 'risk society' either require expertise that cannot be obtained locally or the problem while diagnosed as local is in fact global in reach and not confined to national borders. For instance, CFCs may be spent in Europe or North America but congregate due to their chemical composition as well as the atmospheric 'jet stream' at or around the South Pole. Nuclear radiation is another such example. Once released into the atmosphere, as in the case of Chernobyl or more recently in 2011 as an effect of the Fujiyama nuclear disaster in Japan, it is difficult to pinpoint the exact site of nuclear contamination since nuclear radiation can travel across borders through the atmosphere or sea. As a result, Beck argues that a new set of institutions or global arrangements are required in order to address the unintended but catastrophic consequences of aspects of modernity. Beck designates the term 'reflexive' modernity as a new phase of scientific and policy development that is largely oriented towards mitigating the risks produced by the first modernity (Beck, 2006).

For Beck, although the spectres of catastrophe connect global threats, the concept and methods of risk analysis are what provide for a space of social action prior to catastrophe, signalling potential outcomes prior to their realisation (Beck, 2006). However, unlike the definition of risk that is associated with the first modernity, as rational calculus that enables the future to be colonised in the present (Hacking, 1990), the risks present in WRS have

grown exponentially and at times become unbounded. That is, the risks of WRS are no longer easily quantifiable and do not allow themselves to fall into limits or boundaries that are bearable for society or even human life. WRS, then, are typified by three qualities. De-localisation: risks are no longer bound to one geographical space, but they are 'omnipresent' as evidenced with CFCs and nuclear radiation. Incalculability: the impact of risks produced by modernity has no coherent, unifying risk calculus since risks are unbounded or discontinuous. Non-compensatibility[28]: the potential consequences of climate change, bio-engineering and terrorist attack using 'dirty weapons' are so great that mechanisms of insurance or compensation cease to function, or if they do function they lack an appropriateness of scale (Beck, 2006, p. 5). As a result, the response to the risks that make up Beck's typology by the state or an institutional response become concerned with 'precaution through prevention' as risk comes to signify the unknown and therefore necessitates retrenchment or a greater claim to security and control (Ewald, 2002, p. 285). When Islamist terrorism is mapped onto 9/11, Beck regards it as not simply a global risk, but one that is an affront to globalisation itself, whereby terrorists have adopted the decentralised and networked strategies that utilise the very infrastructure of globalisation (Beck, 2003). The catastrophic threat of terrorism is revealed not just in the ability to exploit the networks of finance, immigration, telecommunications and travel, but in the fact that terror groups like Al Qaeda do not have coherent political demands that can be mapped onto a framework of negotiation.[29] There is a new potential for terrorist organisations – jihadist or otherwise – to obtain not merely 'dirty atomic' weapons, but inexpensive and more readily available weapons of mass destruction such as cyber or bio-weapons. As a result, Beck has claimed, 'terrorists . . . repeal [or challenge] the monopoly on violence previously enjoyed by states' (Beck, 2003, p. 257) (Bobbitt, 2009). This then creates an intractable problematic for national governments and global agencies, as described in the introduction: How, then, do governments address or manage seemingly infrequent events, actualised by an elusive enemy disguised as members of the civilian population, that have potentially catastrophic consequences?

What can be seen in this account of risk is something very close to what is found within U.S. homeland security literatures such as the National Strategy for Homeland Security (NSHS). This strategy is consistent with Beck's analysis and acknowledges that terrorism prevention, along with effective crisis response to natural disasters, make up the key events or priorities for U.S homeland security. For instance, the NSHS is concerned not only with dirty bombs or the spread of harmful pathogens, but with mitigation of Hurricane Katrina–like disasters (NSHS, 2007). What is important in this account is that in the face of unbounded threats states and other governmental actors have turned to policy measures of precaution through

[28] This notion of non-compensatability has been challenged by social scientist Nikolas Rose who articulates that schemes of compensation and insurance continue to be at work even during times of catastrophe and loss of life. Indeed, as Rose points out, just as there are compensation mechanisms for the loss of life in a traffic accident, so too, as the 9/11 victims' funds revealed, there is also a cost of life associated with terrorism. This empirical grounding is important to consider since it allows scholarship to claw back ground that is perceived by Beck as unintelligible – unbounded risk – in order to find evidence, in this case of how security responds to crises.

prevention where retrenchment becomes an object of sociological study. While this notion of WRS is appealing and will be shown to be consistent with the rationality of U.S. homeland security policy, Beck's account suffers from what appears to be an internalisation of the severity of global risks within his discourse. While it is valid to represent climate change, terrorism and financial turmoil as global risks that are harmful and potentially catastrophic, he fails to acknowledge, as Aradau and Munster point out, the 'the variety of ways in which catastrophe risk are already being governed in this new environment' (Aradau & Munster, 2007, p. 53). For instance, even if risk as terrorism contains a quality of incalculability and cannot be mapped to a rational calculus – as it has been argued in Chapter 1 – it does not mean that an understanding of risk cannot be understood or even formally rationalised. For instance, Lorraine Daston has shown that an understanding of risk in respect to gambling, maritime insurance and annuities was institutionalised within Europe long before the development of probability mathematics (Daston, 1988). Within maritime insurance, insurers were willing to lend money to cover the cost of a voyage even if a sound or adequate model with which to objectively measure appropriate risk for sea travel was lacking. Daston indicates that within the 16th-to 17th-century literature on maritime insurance, there are no 'guidelines' to pricing, but what is taken into account is the type of cargo, the condition of the vessel and the route taken (Daston, 1988, p. 120). As a result, premiums were based on a combination of 'intuition, experience and convention': prices for well-travelled routes remained more or less constant, while return voyages tended to cost more due to the inability for the insurer to inspect the cargo (Daston, 1988). This type of risk perception seems quite similar to how the Visa Waiver Program is regulated between the United States and 36 'low-risk' countries throughout the world, even though a terrorist could arrive from any locale. This arrangement, which allows foreign nationals to travel to the United States without a visa, seems to be based more on experience, established diplomatic ties or economic links rather than a mathematical risk threshold.[30] Here risk can be seen as departing from the simple yet important distinction of catastrophic/preventable put forward by Beck.

A further argument against WRS issued by Aradau and Munster concerns the lack of historicity found in the theory where social, cultural and political factors determine and shape what risks become national priorities (Aradau & Munster, 2007). For instance, terrorism appears to take on a simple logic of agency and threat – terrorists exploit global networks, terrorists do not have rational aims, and terrorists are attempting to obtain and use weapons of mass destruction. This explanation, while at the surface of U.S. counter-terrorist policy, lacks cultural and historical dimensionality since Islamist terrorism has been primarily described as devoid of historical and political origins that could yield further understanding in respect to motivations as well as the purpose and placement of a terror attack. Anthropologist Mahmoud Mamdani has shown in Good Muslim, Bad Muslim that radical Islam and Islamic terrorism have a direct connection to American struggles against the

[30] What is also missing from Beck is an understanding of subjective theories of probability that can also be used to map or rationalise the occurrence of events that are less tangible in respect to data. These methods are known as Bayes' theorem as well as the subjective notion of probability.

Soviets in Afghanistan that marked the end of the Cold War (Mamdani 2004). For instance, the narrative shows that Osama Bin Laden left Saudi Arabia in the late 1980s to support the Afghani mujahedeen against the occupation of Afghanistan by the Soviet Union. The subsequent withdrawal of the Soviet Union brought about through extensive and covert U.S. support of the many different and often rival tribal and Islamist factions inside and outside of Afghanistan therefore left the loose collection of soldiers, mercenaries and militia without a purpose or target; the target quickly became the new 'empire' of the United States. This historical and cultural reading has an important implication for risk perception and risk management bound to homeland security and counter-terrorist practises; namely, it shows that the management of terrorism risk does not simply require the development of enhanced security or safeguards to absorb or intervene upon catastrophe as it is about to strike. Rather, it displaces risk management from an essentially defensive and conservative strategy to one that requires an active form of engagement[31] or even diplomacy, since the threat itself arises from a particular cultural, historical and religious setting filled with its own inherent contradictions and logics for political struggle that act as points of intervention – terrorism simply does not just 'exist' (Zeckhauser & Zaluar, 2002). This active form of engagement would also be one that would appear to require diplomatic and political tools along with the military and intelligence tools that have been primarily utilised in the address of the threat. Economists Zeckhauser and Zaluar make this point, arguing that a host of new transnational threats, such as terrorism, human trafficking and organised crime, require a strategy of mitigation in global locales, rather than simply at the border. Terrorism as a threat also radically disrupts the understanding of U.S. and Western European security policy, since for the last 50 years it has been concerned with how best to protect Europe from a Soviet invasion and how best to contain the expansion of Soviet influence and power by displacing and spreading the threat of terrorism across a broader geographic domain composed of diffuse tactical elements – networks of covert operatives as opposed to columns of tanks or the stockpiling of nuclear warheads (Zeckhauser & Zaluar, 2002). As a result, a new form of security policy has been made manifest, one that, like Beck, acknowledges the possibility of catastrophe, but, unlike Beck, does not regard this threat as a Cold War–style threat, defined by a single almost messianic event, but one that is multiple and possesses various degrees of magnitude. It is instructive then to look at the work of Ewald, who considers risk-based practises not only in respect to their meta-characteristics, but to how they are activated within an institutional and social context.

In his genealogical analysis of the concept of risk, Ewald argues that the social understanding of risk has moved from a the notion of 'responsibility' in the 19th century to 'solidarity' in the 20th century to a paradigm of 'security' in the 21st century, where risk is

[31] The distinction raised by Zeckhauser and Achilles in U.S. security policy is the distinction between containment and engagement. Unitary threats such as the Soviet Union or present-day North Korea and Iran can be 'contained' since the risks are far too great to actually engage these entities. However, with the new host of transnational threats, while a certain form of catastrophic potential remains, the threats are diffuse enough to have a lower cost for security agencies or the military to engage with these threats in the field This argument of 'engagement', while compelling, will not be emphasised, since it is a normative recommendation of how U.S. security policy should perform – and in many ways it has already – post-9/11. What this study is ultimately concerned with is not necessarily the recommendations, although these are compelling points of reference, but how the institutions, technologies and policies of U.S. homeland security work to manage risk.

understood as precaution (Ewald, 2002, p. 273). Each concept of risk for Ewald is pegged to a particular style of social consciousness or style of thought. For instance, in the 19th century risk as responsibility, otherwise termed as 'prudence', became a pivotal concept for the emergent political theory of liberalism, since it placed legal rights, moral obligations and economic interests onto the individual. While it is widely accepted that there are many risks that may befall the individual, liberalism insists that what accompanies individual freedom or liberty requires that the individual become aware of the future so that he or she can ensure well-being. Insurance becomes the institution of 'rational providence' where individual compensation as a result of loss is what safeguards against unwanted future events. The second concept of risk is what Ewald designates the concept of 'solidarity' that accompanies not only the rise of the welfare state but due to (i) the recognition that society possess its own law-like qualities or rates revealed through the technical innovation of enumeration and statistics; and (ii) that these law-like qualities show that unwanted events, such as accidents in the workplace, are endemic to the workplace itself and therefore shift the burden of responsibility for fault or compensation from the individual to the employer, government or firm (Ewald, 2002). Ewald cites an example of this displacement found in the French legal code of 1898, which acknowledges that 'all work has its risks; accidents are said but inevitable consequences of work itself"[32] (Ewald, 2002, p. 277). The shift to precaution as the third dominant mode of risk does not arise until the 1980s, when it came to be known as a defining principle within the environmental protection movement and ultimately identified by social scientists, such as Beck. Ewald argues that precaution, unlike prudence or solidarity, is concerned not with compensation in respect to loss, applied to the individual or the firm, but with the prevention of catastrophic events that impact a population as a whole, whether these disasters are natural or man-made. Ewald argues, in reference to Beck, that the rationale of precaution cannot be applied to all situations, but, rather, only to those that contain both scientific uncertainty, and irreversible danger[33] (Ewald, 2002). Ewald's precautionary rationale functions much like Beck's conception of WRS, where risks that require a precautionary logic are those that change the 'understanding of injury' where traditional insurance-based modes of compensation break down. Precaution, too, is also bound with modes or practises of prevention where, despite uncertainty, actions can be taken in order to intervene upon unwanted events. Although this precautionary logic can be seen to appear within the work of Beck, its mode of functioning and societal response brings with it several attributes discussed in the section concerning sovereignty and the concept of necessity in the face of the decision. For instance, Ewald acknowledges that with catastrophic events there is *a priori* uncertainty, therefore any response to the event can only take the form of *posteriori* decision-making – or decision-making based on past practises as opposed to rules that anticipate the future. Furthermore, as a result of placing the given event against a backdrop of the worst-case scenario, precaution brings with it the practise of the 'decision' into public policy practises in order to determine what is considered the 'best'

[32] Foucault has also spoken about this notion of solidarity in respect to 'social security' as a form of governmental rationality of the state.

[33] This dual notion of scientific uncertainty and irreversible danger is what is meant when Beck uses the compound statement, arguing that risks within WRS have become 'unbounded'. This implies that they yield catastrophic results and can no longer be mapped according to a rational calculus.

or most 'appropriate' way forward in respect to the event (Ewald, 2002). What is interesting is that the decision regarding the event, due to its uncertain nature, is pried from the expert or scientist and placed in the hands of the politician. It would be erroneous to suggest that any type of control over the decision leads to a Schmittian form of sovereign power – monopoly over the decision – however, it is evident that given the appropriate situation this concept can be easily transferred and imported into a political framework of decision making when confronted with the emergency. It will be shown that the precautionary principle is active and at work as part of the 'no-fly' lists that make up one of the several defence features of U.S. transatlantic border security. Here foreign-nationals travelling to the United States are screened as no-risk, selectee or no-fly. If an individual is deemed 'selectee', he or she is required to perform additional screening upon entering the United States; if a person is deemed no-fly, he or she is barred from travelling to the United States. What is precautionary about this is that while individuals who appear on the no-fly list are assumed to present a terror threat, these individuals are not arrested in their countries of origin. Rather, they are simply barred from travel, meaning that there is not only uncertainty in respect to the threat they pose, but also uncertainty concerning their legal status that therefore necessitates a decision on 'bare life' rather than a deliberative legal or legislative response (Schneier, 2008).

2.5 Identity Technologies and Surveillance

While an analysis of the legal and policy framework informing U.S. homeland security can provide an understanding of the overarching rationales employed in the 'war on terror', it is essential to understand how these aims are embodied technologically at the border. The bulk of the literature concerning identity and identification as a technique of statecraft has concerned the pre-modern and modern uses of fingerprinting and passports. Here both of these technologies can be seen not only as a means to ascertain and fix an individual identity, but as technologies used to define, organise and account for a given population. For instance, fingerprinting historically can be seen to have a dual functionality, not only to identify recidivist criminals that flocked to expansive and relatively anonymous cities, such as London in the 1800s, but when taken outside of the prison setting were also used to account for subjugated populations either within colonial India or for immigrant communities[34] in the United States (Sengoopta, 2003) (Cole, 2001). Although these primarily historical accounts pose a similar set of problematics concerning identity that can be transposed onto Western nation-states in an era of globalisation with the dominant theme of the destabilising effects of mass migration, this literature can only partially account for the recent introduction of networked digital technology that has come to play a central role in post-9/11 U.S. security due to the analytic capacity that these technologies provide – that is to not only fix identity within space and time, but to perform a series of secondary and tertiary processes that provide value to security agencies.

[34] For instance, fingerprinting was applied to 'indistinguishable' Chinese migrants during the 1820s as a form of population and labour control.

A starting point for this discourse on the social impact of security technologies can be found within the work of social scientist David Lyon who has put forward a unifying concept termed 'surveillance society' or 'everyday surveillance'. For Lyon 'surveillance society' is constituted not by a top-down or centripetal form of power, but, rather, is typified by multiple and interconnected modes of surveillance termed 'assemblages'[35] borrowed from Deleuze's philosophical work on concept of the rhizome[36] (Lyon, 2002, p. 27). Forms of surveillance can be found not only within law enforcement but are designated as part of 'everyday experience': video cameras are stationed on street corners or inside ATM machines, monitoring software works to track the Web-browsing habits of individuals to be used for crime-prevention purposes or simply sold to marketing agencies; licence plates are captured by surveillance cameras built into street lights in order to monitor traffic flow and assign speeding tickets or other such fines. Despite the multiple ways in which surveillance can be carried out, Lyon identifies two consistent properties: (i) new surveillance technologies work to obtain 'abstracted' data or information from individuals, such as biometric data, DNA or video imagery; and (ii) once this data is collected, it is organised and classified in order to create risk profiles that directly impact the 'choices and [life] chances of data-subjects' (Lyon, 2002, p. 11). Lyon's first premise is based upon the idea that work, communication, commerce and governance are done more often at a distance and therefore have led to a need to compensate for a 'fading face' and 'disappearing body' from instances of human communication and exchange. Furthermore, due to the relative anonymity of major cities as well as the tendencies of globalisation that has resulted in mass migrations and travel throughout the globe, new methods of identification are deemed necessary by governments to standardise identity across multiple national domains to create recognition and trust. Lyon identifies a paradox in this practise, noting that the very systems used to claim identity or build trust are also those technologies that track the very details of concerning the behaviour and social relations of the very identity in question to be used for secondary and tertiary purposes. Lyon argues that these practises do, however, have political implications whereby identity details are not only aggregated but classified and used to make inferences about behaviour of individuals and lead to profiling. Here preventative decision making on the part of an institution, security agency or corporation becomes based on a probability threshold that cannot necessarily be attributed to the actions, history or choices of the individual but can become based on institutional biases or prerogatives that function to limit the choice and potentiality of the individual. However, while referring to the potential political problems of classification, Lyon tends to lack substantive examples describing how the mechanisms of classification or surveillance work to create a power differential that explicitly curtails self-determination. For instance, while it can be inferred that classification takes place within schemes of insurance – where individual attributes contribute to an overall risk score determining an insurance premium – or within a post-9/11 British context that can lead to

[35] 'Assemblages' here refers to the multiple set of surveillance technologies that capture and track individual identity as it moves across multiple geographies, jurisdictions, linguistic categories and digital domains.

one social group being targeted by law enforcement over others – such as with the stop-and-search laws in Britain that have since 9/11 primarily targeted young men of South Asian appearance and origin[37] – Lyon fails to trace or map the mechanics of each of these processes. It is noble to point to unfair practises of insurers or biases against minorities exhibited by the state, but what is lacking from his analysis is an account of the scientific, institutional or legal mechanisms that contribute to this imbalance of power. Where Lyon connects with the analysis that is present in this thesis is through emphasis on classification that appeal to very modern notions of state monitoring and state self-awareness that can be traced to Hacking's analysis of the development of statistics as the 'science of the state' (Hacking, 1990, p. 16). However, it will be shown that with the rise of distributed, networked and database-oriented digital practises employed by the state, the means of state awareness or knowledge of its subjects has moved away from strictly classification but towards prevention and precaution that allow this mode of security at the border to respond to new information that challenges pre-existing notions of what a terrorist should be or should look like. For instance, within the context of the border individuals are matched against terrorist or criminal predicates as it relates to past or present intelligence and law enforcement activities. Therefore, while there is a process of categorisation that takes place by U.S. security services – for example, the category of foreign nationals singled out for biometric processing or any national from those countries deemed to be state sponsors of terrorism – whether or not an individual is arrested or prevented from travelling to the U.S. is based upon matching specific predicates associated with terrorism or criminality. Therefore, this notion of categorisation is accommodated in this analysis of the border, but strict categorisation that allows U.S. security to arrive at a stable definition of what constitutes a terrorist, is updated and changed due to the nature of the terrorist threat and the past example of 9/11 – asymmetric, clandestine and catastrophic. This change in security practise can be linked to the increased digitalisation and information awareness of security services, and as Lyon has pointed out, through the amassing of greater and greater amounts of information on the individual.

With this theoretical context a rendering of the use of biometrics within the U.S. border zone post-9/11 can be found in the essay 'Embodying Risk: Using Biometrics to Protect the Border' by Charlotte Epstein. Epstein, who addresses the material conditions of the Department of Homeland Security programme US-VISIT,[38] argues that biometrics for the purposes of border security work to scrutinise the body not as a political subject, but, rather, as a 'mobile object' that possesses characteristics of risk (Epstein, 2008, p. 171). While a formal definition of how biometrics function will be presented in Chapter 6, it must be pointed out that biometric technology works by performing pattern recognition of a distinct bodily feature – fingerprint, iris, hand geometry, voice – that can be used to verify that an individual 'is who he says he is' (Wayman, et al., 2005). As a result of the requirement for a physical

[37] In fact, in 2011 the *Guardian* newspaper uncovered U.K. government data revealing that ethnic minorities, and in particular Southeast Asians, were 42% more likely to be held in custody than 'white' people, as part of the 'stop and search' powers enabled in schedule 7 of the Terrorism Act (2000) (Dodd, 2011).

[38] US-VISIT was introduced in Chapter 1 and will be addressed in full in Chapter 5.

body, biometrics has found use as a control technology that is designed to provide access to a space, whether real or virtual (Epstein, 2008). Epstein argues that biometrics function as a risk-assessment tool as much as an access tool by means of the requirement of biometric enrolment and subsequent biometric identity verification. During biometric enrolment an individual present at the U.S. border or at a Consular office outside of the United States must not only present his or her fingerprint biometrics for the purposes of identity verification but must also have these biometrics matched against terrorist and criminal databases held by the FBI. Epstein refers to this process as 'negative enrolment' or 'weeding out' (Epstein, 2008, p. 173). What is consistent with the argument presented in this thesis as found in Epstein is that the use of biometrics within the context of US-VISIT are used to distinguish between the body of the national or U.S. resident with that of the foreign national. However, while this programme attempts to manage a large population travelling through the border, it also allows for a process of individuation to take place. For Epstein, not only can biometrics be viewed as an access-control or risk-assessment technology, biometrics can be seen to initiate a new logic of governance. This mode of governance, due to the distinction between citizen and non-citizen at the U.S. border, signifies the exercise of sovereign power within the narrow band of the border region (Epstein, 2008). This mode of sovereign power, Epstein argues, is realised through the added scrutiny towards immigration violators, as well as those efforts to attempt to intercept not only terrorists passing through U.S. borders, but individuals with criminal convictions as well. However, Epstein acknowledges that while biometrics seek to not only verify identity but intervene upon high-risk individuals passing through U.S. borders, biometrics themselves do not significantly curtail economically crucial border flows – although fingerprint biometric systems are required to lower their matching thresholds in order to reduce the number of false non-matches, therefore ensuring less economically detrimental queues at the border. While many of the claims Epstein makes can be supported and are consistent with the analysis made in this thesis, what is lacking from Epstein's analysis is a description not only of how biometrics work to identify individuals at the border, but how the database infrastructure operated by the DHS and FBI works to identify threats at the border. While the deployment of biometrics at the border marks an important change in U.S. security practises, these practises are only maximised when combined with a data-sharing and data-matching infrastructure. It will be shown in Chapter 6 that the database infrastructure supporting biometric matching is also responsible for extending or exporting the border from specific U.S. points of entry, to U.S. Consular offices worldwide, along with the U.S. 'theatre of war', such as Iraq and Afghanistan.

The security layer that directly involves the use of distributed database technologies can be seen to be those practises that involve the use of data-mining technologies and techniques. As presented in Chapter 1, not only do U.S. border security practises rely on biometric data from foreign nationals, but U.S. security also collects and analyses PNR[39] data in order to determine both 'patterns' and social networks of interest. It will be argued in later chapters

[39] PNR is understood as all of the information required by an airline to make a flight booking. This includes an individual's credit card number or seat number, but also his or her food preference, frequent flyer number and point of departure, amongst other information.

that this practise, along with the collection of biometrics, is made possible due to the lack of legal rights and protections afforded foreign nationals; however, the surrounding literature concerns itself with two other issues of interest to this thesis: (i) how to understand the new mode of security governance that is based on the aggregation and analysis of disparate sets of data previously kept within discrete databases and used for purposes other than law enforcement; and (ii) what type of political or ethical questions this aggregation and corresponding analysis brings where the literature primarily concerns the transparency of the algorithms and processes involved. In an influential[40] paper published in the Columbia Science and Technology Law Review, K. A. Taipale argues that data-mining research for the purposes of U.S. domestic security can and should be developed as long it is done with an understanding of individual privacy. What is of interest in this analysis is not the normative suggestion of how data-mining should or should not be used, but, rather, the supporting analysis that shows how data-mining can be used for anti-terror purposes that have come to be understood according to a logic of search. Taipale first argues that data collection and analysis has become a central pillar of post-9/11 domestic security due to the impoverishment of intergovernmental data sharing that significantly hindered the ability of U.S. intelligence to prevent the terror attacks[41] (Taipale, 2003). However, it must be recognised that the introduction of data-mining tools to aid in anti-terror and crime prevention performs not only the task of data-sharing, but also data analysis that allows for the discovery of novel insights buried within massive data sets. While data sharing can be seen as an essential function to distribute names of criminals or terrorists to multiple disparate intelligence or law-enforcement agencies, or as a way to gather further evidence in respect to ongoing terror investigation, data-mining performs a different task where data-mining or knowledge-discovery technologies reveal new knowledge from a data set that appears to be innocuous and benign (Taipale, 2003). With the introduction of data-mining tools, intelligence and law-enforcement move from the simple yet important activity of sharing information amongst agencies to the application of a set of techniques that enable intelligence to identify individuals of interest along with 'patterns' of behaviour amongst the data collected (Taipale, 2003). The basis for this argument by Taipale has two components. First, as a result of the adoption of digital technology, there is simply too much data produced related to the identity of individuals moving in and out of the country to be accounted for by traditional means; as a result, new forms of automation are required to process, organise and make such information useful. Second, data-mining is already and has been for some time developed and used not only within commercial sectors such as marketing, but in many branches of applied science, such as healthcare. Taipale asks, if data-mining techniques can be used to inform 'multi-billion dollar health care decisions', why can they not be used within the context of law enforcement? (Taipale, 2003, p. 45).

For Taipale, the use of data-mining techniques to aid in domestic security does, however, raise a set of privacy concerns that can be understood in respect to U.S. constitutional

[40] United States Senate Committee on the Judiciary. Testimony of Kim Taipale, Executive Director Center for Advanced Studies in Science and Technology Policy. January 10, 2007.

[41] This lack of data-sharing by and within the FBI was described in detail in Chapter 1.

provisions, in particular Fourth Amendment procedures concerning lawful search and seizure,[42] that rest on the distinction between particularised and non-particularised search. As described, data-mining allows for new knowledge to be discovered within large data sets. How this new knowledge is discovered, both in respect to how the data is collected and what methods or modes of analysis are applied, then takes on paramount importance for counter-terror purposes. Taipale identifies two analytic methods that can be employed with data-mining tools: (i) subject-based inquiry, where once a subject is known to intelligence his or her identifiers can be searched for and traced across multiple databases and where the key aim is to gain further evidence of wrongdoing; and (ii) pattern-based inquiry, where a hypothetical pattern for terrorism is applied to a data set in the hope that it will be able to produce a match – an example of this form of pattern matching can be seen with the analysis of PNR; for instance, if a traveller is identified as purchasing a one-way ticket in cash, he or she may become subject to increased scrutiny at U.S. borders (Taipale, 2003, p. 33). The privacy concerns that accompany these methods are twofold. When used for the purpose of security, the question is raised as to whether or not it is viable for intelligence services simply to lay down a pattern or algorithm onto a data set in order to look for suspicious activity when no concrete suspicion exits. Second, whether the aggregation of government databases, each holding data collected from individuals for specific purposes unrelated to counter-terrorism efforts, when brought together constitutes 'unreasonable search'. The specific legal attributes regarding search will be discussed in Chapter's 4, 6 and 7,[43] but Taipale's representation of how search can be thought of, even if incomplete, is instructive for these later chapters. What can be seen almost immediately from Taipale's analysis is that it departs from the understanding of 'everyday surveillance' proposed by Lyon since it takes into account the actual 'algorithms' responsible for the activation or achievement of a specific type of security practise. Surveillance within this context is not simply assumed to be an 'assemblage', a multitude of surveillance devices that simply work together in an exponential fashion; rather, security, surveillance or even risk assessment can be seen to be actualised along these narrow bands of practise. That is, the accuracy of a subject-based inquiry, the quality of the data that the algorithm is using, the margin of error that a pattern-matching algorithm is allowed to have are the qualities that shape the actual dimensions of governance that Lyon hints at but does not develop.

However, before these data-mining tools can be deployed, a legal space needs to be created for their operation. For instance, for subject-based inquiries, where the purpose is to maintain additional information about a known terrorist that is 'lawfully subject to investigation', the legal channels for tracking their data trail already exist via FISA. Domestic intelligence using this method, under the supervision of the FISA court, is permitted to apply

[42] The Fourth Amendment will be addressed in Chapter 4, concerning the legal permissions that direct the type of search that can take place at the border; for instance, Fourth Amendment provisions are what prevent the collection of biometrics and other airline data elements from collection at U.S. borders, while remaining silent in respect to those very search procedures being carried out against foreign nationals.

[43] Chapter 4 will focus on the legal conditions and permissions that allow for the collection and analysis of foreign-national data that is consciously bracketed or made distinct from data obtained on U.S. nationals. Chapter 6 will address how data-mining is used in respect to the analysis of PNR. Chapter 7 will address the legal conditions as well as the new form of security governance resulting from the aggregation of foreign national data from a range of U.S. intergovernmental databases.

for a warrant that allows access to electronic sources to aid in an investigation. However, the distinction between particularised and non-particularised search becomes blurred in two scenarios. The first scenario concerns whether or not a search is justified in the case where intelligence have suspicions that a terrorist 'may' be on a specific flight or found at a specific location – here a search would be performed by running the names of all passengers of a flight or all guests at a hotel against a watch-list. The second scenario involves simply the collection of data – flight manifests, credit card numbers, hotel records, immigration information and so on – and mining that data with the hope that a suspicious pattern will emerge that is either historical or in real-time. Taipale does not answer directly whether each scenario is a violation of Fourth Amendment rights; rather, he attempts to rationalise how each scenario can be understood in respect to legal precedent and technological development. For instance, he argues that law enforcement have the legal right to stop an individual on the street in order to perform a search if there is a reasonable degree of suspicion. This is what enables search to move from non-particularised to particularised, as illustrated in the 1974 Supreme Court case *Terry v. Ohio.*[44] Rhetorically, Taipale asks 'whether one considers the database equivalent to the street?' (Taipale, 2003, p. 47); 'if so', he answers, then individuals should have an expectation of privacy where intervention by law enforcement is only based on reasonableness of suspicion. As it will be argued throughout this text, non-particularised search is most prevalent in respect to the foreign-national, despite being an individual who arrives to the United States from a country that also places strict guidelines on surveillance and data-collection by intelligence services.

It can be seen from this body of literature that U.S. domestic security functions not simply through new laws or policy orientations, but through the ability of new 'sense-making' technologies that both fix the identity of an individual at a particular time and place, and also provide insight into an individual's social network and behaviour. Furthermore, these technologies not only enable U.S. security services to allow or deny physical access to the United States to individuals viewed as high- or low-risk, but also act as a forensic tool, providing information to U.S. security services that can potentially be used for future terrorist investigations. It is evident from the analysis of these types of identity technologies that not only do they provide their own logics of security, but each technology, as well as the permissions to collect, analyse and share personal information, must be placed within a legal and political context that makes it possible. Beyond the theoretical assertion of terrorism as a catastrophic threat where terrorists operate by disguising themselves as members of the civilian population, this legal and political context is the intricate institutional working that allows or makes the application of these technologies possible. In order to understand or create a well-defined security definition, such as with U.S. homeland and border security, not only government action must be analysed, but also the conditions, motivations, rationales and permissions that make that action possible.

[44] *Terry v. Ohio* will be addressed in further detail in Chapter 4.

2.6 Conclusion

In the introduction to this chapter, security was defined sociologically in two ways: as a practise that responds to the emergency and in doing so breaks established norms and rules; and as a practise of government that views the negative event in question as a probability that it seeks to limit or prevent. It must be acknowledged, however, that while each quality of U.S. border security – legal, policy-based, technological – brings with it its own social practise, how the law is shaped and how border security comes to be realised is not only related to national security needs. Rather, U.S. homeland security, despite the exercise of sovereign power, is still shaped by numerous social forces. These social forces can be seen to include the preservation and enhancement of America's position within the global economy, the respect of constitutional norms and precedents, and recognition, even by conservative lawmakers, of America's tradition of liberal values, freedom of movement and an 'open door' policy. U.S. border security, then, is placed in a paradoxical situation. Not only must it meet the demands of national security, scrutinising all foreign nationals entering the country, but it must also make sure that this scrutiny is done in such a way that it keeps its borders not only open, but also economically efficient. A concept that has been referred to in this chapter and speaks to the twinning of sovereign and economic rationalities is the concept of 'governmentality' developed by Foucault. To be specific, governmentality cannot be understood merely as governance as such, accounting for simply the passing of laws or crafting of policy. Instead, Foucault argues that governmentality as a form of 'modern political reason' seeks, on the one hand, to make a 'tricky adjustment' between 'totalizing legal-political forms' and, on the other, the exercising of an 'individualizing form of power through a "pastoral government concerned with the concrete lives and conduct of individuals' (Burchell, 1991, p. 145). What takes on primary importance once this frame is established, however, is to ask precisely to what degree do both sovereignty and the economic, social and legal interests of the individual come to be realised. How this practise operates legally, strategically and technologically will be addressed in the following chapters.

3. Research Design and Methodology

3.1

As introduced in Chapter's 1 and 2, this thesis concerns how the strategic aims of U.S. homeland and border security are realised through the interplay of legal, technological and institutional practises. This interplay further raises the question of how each can be seen to work together not only with coherence but in a way that contains explanatory power. For instance, while it can be understood as straightforward to assess U.S. border security practises at a single operational or causal level – U.S. counter-terrorism policy solely as an expression of national sovereignty or the incorporation of digital-surveillance technology within homeland security strategy as the emergence of a 'surveillance society' – the dimensionality of the border-security environment is increased when technology, law, institutional prerogatives are not only seen to work together, but are shown to contain their own internal limitations, contradictions and discontinuities. A useful methodological approach to account for and accommodate both congruence and discontinuity is that of 'governmentality' developed by Foucault, which accommodates the multiple techniques and procedures used to govern human and institutional behaviour (Rose & Miller, 1991). This approach, made possible through the empirical analysis of U.S. homeland and border security, otherwise allows for an analysis according to three operations. First, the identification of the 'problematic' of government; second, the mapping of how this problematic results in the development of a political rationality or strategy of action for government; and third, an account of how this political rationality is used to motivate the use of different technologies of government taken up for the purposes of counter-terrorism. It must also be noted that the motivation of this research project carries with it a set of acknowledged boundaries due to the sensitive political nature of the subject matter. U.S. homeland security agencies, while required to be accountable to the public, also have a tacit interest in obscuring the details of how counter-terrorist practises are performed. This is done in order to maintain the integrity of criminal cases against suspected terrorists and to preserve the agency afforded to the intelligence and law-enforcement community.[45] In order to work around this barrier, research materials have been obtained primarily from open-source sites as well as from expert interviews, primarily from the scientific community, that compose an accurate empirical image of homeland security.

3.2 Research Question (Motivations and Problematics)

In the text Problems and Methods in the Study of Politics, editors Shapiro, Smith and Masoud identify three interpretive modes or approaches that can be followed by political and social scientists when addressing and studying political situations. The first mode is defined as 'problem-oriented' or a problematic 'throw[n] up' by the world and in turn requires the

[45] These rationales have been contested with both the U.S. and U.K. legal systems. For instance, the 2005 case *Ibrahim v. DHS* involved a request by Ms. [ ] Ibrahim, a doctoral student at Stanford University, who was wrongfully arrested at San Francisco airport due to her name appearing on a no-fly list and appealed to the DHS to release the information concerning (a.) how her name appeared on the no-fly list in the first place, and (b.) what was the decision-making process that led to her wrongful arrest and the subsequent disqualification of her student visa. A response to each point was withheld by the DHS on the grounds of 'national security' even though Ibrahim was early on determined not to be a terrorist threat. Although these rationales are contested, it does not prevent national-security agencies from blocking access to details about their internal decision-making process.

social scientist to identify the appropriate methods for analysis of analysis. Second, a 'method-based' approach, where the analyst is armed with quantitative and structured analytic tools to identify a problem in the world that can be interpreted with the tools at hand; and third, a mixed or 'pluralist' approach whereby both methods and interest areas can be matched in order to determine the best fit (Shapiro, et al., 2004, p. 21). While these approaches can be seen as valid in and of themselves, each lends itself to different research questions and a different understanding of the event of interest. For example, a problem-oriented approach is valid in the event that a political or social problem can be seen to be a 'single-case' or containing such complexity and uniqueness that it cannot easily be measured. Methodological approaches on the other hand, whether concerned with rational choice, statistical frameworks or even solely interview analysis, can be used to discern patterns of interest in respect to a given social phenomenon given a sizeable enough data set. However, the appropriateness of the approach taken as part of the research project is not simply based on what data is available, but, rather, on what the social scientist holds to be of analytic interest and hopes to achieve with the research project. Examined in respect to the best approach to address the aim of this thesis, a problem-based or methodological approach could potentially be useful. For instance, the problem-based approach allows for a reading of counter-terrorist technologies and practises to be a unique and heterogeneous configuration that has been assembled in order to guard against future high-impact, but low-probability events. Quantitatively, this research question could also be interpreted as answering a measurable question of how effective those very technologies and practises are in preventing terrorism, where a cost-benefit analysis can be considered, asking questions, for instance, to understand how many suspected terrorists or criminals were captured at the border in order to make the investment in enhancing security technologies worthwhile. When these two approaches are placed side-by-side, it becomes clear that a problem-based approach is more appropriate for the examination of how and with what impact U.S. trans-Atlantic border security functions or performs. However, a problem-based approach need not preclude the analysis or consideration of quantitative data or the incorporation of other method-based approaches.

In the case of this thesis, additional modes of analysis are required since the object of study is not limited to a single subject matter. In order to accommodate the multiple empirical locations as well as multiple data types that contribute to an understanding of post-9/11 border-security practises, a problem-based approach, one that allows for the later entrance of other methodologies, is most suitable for this given study and its aims. What gives weight to a problem-based approach over a method-based approach is the nature of the problem itself. As has been mentioned, terrorism, while it can be seen as a worldwide occurrence, exists as an event with relative infrequency given the social situation. For instance, since 1980 there have been on average 2,000 terror attacks per year worldwide (GTD, 2011). In particular, because in the U.S. terrorism has come to be understood as an infrequent or low-probability event since the rash of airplane hijackings in the 1970s, it becomes difficult to analyse terrorism as an event according to standard modes of time-series analysis as well

as cost-benefit analysis since from a rational perspective the costs are always far greater than the perceived benefits of counter-terrorist practises.[46] This difficulty can be further highlighted by briefly considering the influential 1978 economics essay by William Landes, who analysed the causal variables involved in the decrease of airplane hijackings within the United States after 1973, as well as more recent quantitative work on the political economy of terrorism carried out by Enders and Sandler.

To introduce his 1973 study, Landes observes that on May 1, 1961, a National Airlines flight en route from Miami to Key West was successfully hijacked and diverted to Cuba, marking the very first time a hijacking of a U.S. registered aircraft had taken place. Over the next six years, the United States experienced seven more such hijackings, but from 1968–73 the hijacking rate became 'unprecedented', with 174 hijackings taking place, only to come to an abrupt halt in 1972 with only one hijacking and a mere ten over the next three years (Landes, 1978, p. 3). In order to orient his analysis, Landes asks what was responsible for such a decrease in hijackings. In doing so, he offers three hypotheses: that hijacking over this period was merely a fad – Landes indicates that until 1972 the main objective of hijacking was safe transport to Cuba, but in 1971 a 'new breed' of hijackers emerged called 'para-jackers' who would hijack planes with the demand of a cash payout and a parachute (Landes, 1978). Second, that hijacking decreased due to increased penalties for those convicted of hijacking – for instance, in 1973 the United States entered a treaty with Cuba whereby hijackers landing on Cuban soil would be arrested by local authorities and flown back to the United States for sentencing. Finally, that hijacking decreased significantly due to the introduction of metal detectors and screening procedures for all passengers and their carry-on luggage. What is evident from these three hypotheses is that they cannot be asked of contemporary terrorism within the United States or in respect to the intervening years since 9/11, because there has been only one large-scale terrorist event, followed by two high-profile attempts in the decade following the terror attack. Nonetheless, Landes' study acts as a useful methodological backdrop for the analysis of U.S. border security due to the similar, though dated, approach to securitisation of air transit consisting of a political dimension. Landes also asks, if the installation of metal detectors can be seen as a significant factor in the decrease of hijackings, how can the use of this new technology be understood in terms of costs and benefits for the individual air traveller? Before addressing his findings, however, Landes raises an important point concerning data quality. Although there were 174 hijackings between 1968 and '72, or 192 over the period of 1961 and 1976, he points out that the relative annual number of hijackings was relatively small, making it difficult to perform an annual time-series analysis. In order to work around this, Landes divided the 16-year span into quarters, finding still further problems with the time-series analysis given that there were quarters where no hijackings took place. Despite these misgivings, Landes was able to develop a set of results. They are as follows:

[46] As a result, different arguments or rationales of governance are forwarded in order to accommodate the discrepancy between actual monetary values spent and the number of criminal or terrorists apprehended at the border. Here the rationale that is put forward is consistent with the understanding that terrorism is catastrophic and generational.

i. Landes found no relationship between hijacking as a fad and the decrease of hijacking in the United States, because hijackings continued to take place at relatively high levels after 1972 throughout the rest of the world.

ii. Deterrence, in the form of ex-ante methods of pre-screening carry-on luggage prior to boarding, and ex-post methods where more stringent penalties were created for the crime of hijacking, were responsible for the most significant gains in the reduction of hijackings after 1972.

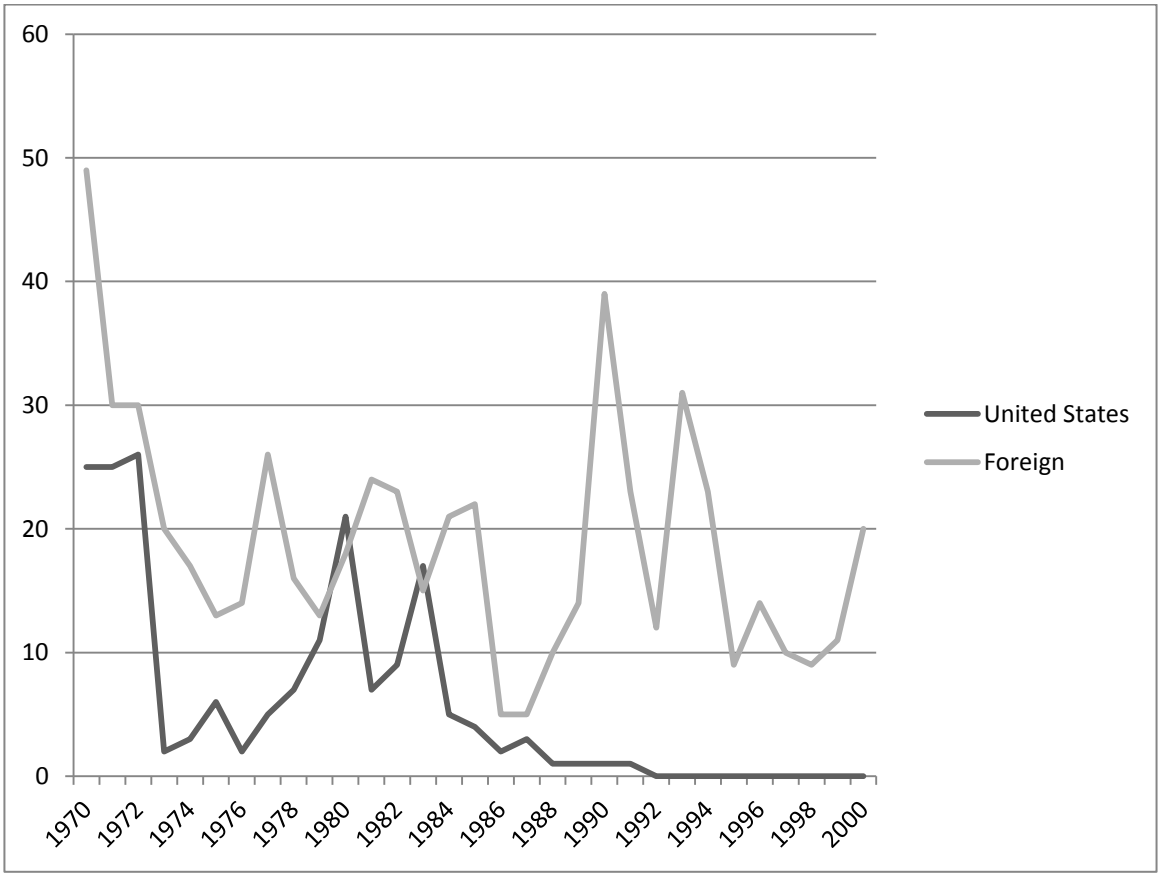
iii. When performing further analysis in an effort to determine which deterrent had a greater impact – ex-ante or ex-post – Landes performed a forecasting measure on the data set and found that ex-ante*,* or the installation of metal detectors at U.S. airports, were responsible for 55% of the security gains made after 1972. For example, if metal detectors and stiffer penalties were not put in place, there would have been between 52 and 71 hijackings between 1973 and '76 instead of the 11 that took place.

iv. When performing a cost-benefit analysis of the installation of metal detectors, Landes found that U.S. air carriers spent approximately $230 million — 1978 U.S. dollars — on the technology upgrade, making the average cost of apprehension of an individual hijacker to be between $3.25 and $4.7 million. However, while metal detectors provided significant gains in reducing the number of hijackings, they only reduced the probability of hijacking from 0.000003449 to 0.000001207%. (Landes, 1978, p. 21)

Furthermore, this analysis raises three important methodological questions. First, Landes is quick to point out that due to the lack of data on terrorist activities, it is difficult to develop either predictive or causal models in respect to dominant variables that can prove the effectiveness of techniques of deterrence. When this same problem is placed within the context of the 9/11 hijacking, this problem becomes glaringly obvious. For instance, according the U.S. Department of Transportation, between the periods of 1991 and 2000 there was not a single hijacking in the United States (USDT, 2001) – see Figure 3.2.a. Furthermore, since 9/11, an event where five simultaneous hijackings took place, there also has not been a single hijacking in the United States – nor for that matter has there been an actual terrorist attack. Second, it can be seen that even preventative measures such as the use of metal detectors for mandatory pre-boarding screening, or within the post-9/11 context the capturing of biometrics and Passenger Name Record (PNR) at the border, come at a cost far beyond what a risk-neutral investor would spend for the relative gains. In a more recent study of the political economy of terrorism, Enders and Sandler have pointed out that the budget of the Department of Homeland Security had grown by 60% in 2004 to $36.2 billion and was given a further 10% budget increase in 2005 (Enders & Sandler, 2006). This leaves the problem when addressing homeland security of developing a set of measures to assess practises of deterrence or changes to the physical security environment due to the infrequency or extremely low probability of a terrorist attack taking place. Second, based simply on a cost-benefit analysis, the individual costs – presumably to the U.S. taxpayer – far

outweigh the perceived benefits in monetary terms; however, these perceived benefits may be seen as acceptable if terrorism is deemed as an existential and catastrophic threat. This as a result is precisely the empirical location that this thesis occupies – a space of sociological analysis outside of standard economic measures. Perhaps further analysis could be performed over the long run to better understand the trade-off between securitisation and deterrence, but from a vantage point of a decade since 9/11 the time horizon for such analysis is too short. The question to ask, then, since an analysis such as Landes' study is not altogether possible, is how can this new security setup be accounted for, a setup that involves law, policy, technology and institutional practise? How does it function or perform, what is its impact, and how can it be understood as a new mode of governmental practise? In order to answer this question, we can return to the earlier description of the problem-based approach, information research design.

Figure 3.2.1: The Number of Airplane Hijackings within the United States and Worldwide: 1970–2000



(Transportation, 2001)

NOTE: There were no hijackings in the United States after 1991 until 09/11/2001.

3.2.2 Problems and Problematics

As it was shown in Chapter 1, 9/11 was not only unexpected and unprecedented, but it provoked a security reaction that has worked foremost to prevent further exploitation of the

U.S. immigration system. If the political manifestation of U.S. homeland and border security can best be interrogated and understood according to a problem-based research design, it is important to arrive at a definition of 'problem-based' that can support methods or data sources when appropriate in order to produce results. Returning to Shapiro, Shapiro argues that the purpose of the problem-based approach is to 'start with a problem in the world . . . [and] . . . com[e] to grips with previous attempts made with the study' and to define the 'research task by reference to value added' (Shapiro, et al., 2004, p. 17). This research approach, while pragmatic, is opposed to grounding itself in a prescribed methodological form, since its purpose is to 'identify, criticize and suggest plausible alternatives to . . . interpretations of political conditions [through the] specification of problems that underlie prevailing account of research programmes' (Shapiro, et al., 2004, p. 17). This explanation of problem-oriented research, as a result, allows for a reading of the situation that pursues and acknowledges the uniqueness and heterogeneity of a given situation. While Shapiro places the problem-based approach in opposition to a method-based approach, he recognises that the problem-based approach comes with its own set of issues; namely, how these basic or primarily empirical elements come to be interpreted by the social scientist. In order to work around this problem, Shapiro argues that while 'all observation is theory laden', the job of the political or social scientist is to be able to identify and compare which theory or set of theories can work to best provide explanatory value (Shapiro, et al., 2004). For instance, it will be argued at later in this chapter that a Foucaultian approach, where governmentality is taken as a central motif enables the analysis of discursive formations and the regularity of such formations within an archive whether this archive is a historical archive or is composed of the grey material of the present (Deleuze, 1988). The role of the social scientist, then, is not one in which the research practise is oriented towards the validation and defence of pre-established theoretical supports, but it seeks to superimpose the best-fitting theory pertaining to the data available in order to support an argument.

Shapiro appeals to several examples where methodological assumptions have led 'us to undervalue reappraisal of accepted descriptions of reality' (Shapiro, et al., 2004). Here Shapiro turns to the theoretical debate of the 1970s concerning the drivers of capitalist democracies. For instance, the dominant methodological trend was to focus on political voting records along with campaign pledges, as opposed to how and under what direction post-election legislation was in fact enacted. This shift of emphasis led to the discovery that significant portions of legislation were written by the business community or organised labour, therefore shifting the debate from one regarding pluralism to one regarding the functioning of the liberal corporatist model. A second example that exposes the problems of a methodology-only approach is that of prediction. While Shapiro contends that prediction is nearly impossible to achieve due the contingent nature of political affairs, prediction can be seen have some use value. For instance, the quantitative work of Przeworski has shown that economic development alone cannot function as a predictor for democratisation; however, there is a strong relationship between the survival of democratic regimes and per capita income (Przeworski, 2000).

For Foucault the problem-based approach is challenged by the term ‘problematisation’ where it can be seen as a deeper formulation of a political or social situation since it is concerned not simply with the novel appearance of an event, but with the ‘critical analysis in which one tries to see how the different solutions to a problem have been constructed’ (Foucault, 1997, p. 284). How this notion of a problematic challenges the definition outlined by Shapiro is that while Shapiro calls for an approach that identifies the causal and explanatory mechanisms that produce novel political events, Foucault seeks to describe the new social, ethic and political conditions that a political event makes possible. In many ways, this is the inverse of what Shapiro is describing. While both utilise the political situation as a point of reference, Shapiro’s political situation is an endpoint, whereas in Foucault this endpoint is opened up into an active point of deliberation, choice and emergence of new forms of social practise that may lend to ethical, scientific and further political implication. Here Foucault argues, ‘I have never tried to analyse anything whatsoever from the point of view of politics, but always to ask politics what it had to say about the problems with which it is confronted’ (Foucault, 1997, p. 283). This statement provides an indication of a type of social science reading that attempts to understand the logics and rationales that in themselves are motivated to confront a political situation, as opposed to offering a strictly normative assessment derived from reading the situation. Taking the example of psychiatry, Foucault argues that his approach was never to address strictly the formation of the epistemology of psychiatry, nor the political structure through which psychiatry operates, nor for that matter the ethical implications of particular psychiatric techniques. Rather, his approach is oriented towards how psychiatry when confronted with epistemological, political and ethical constraints developed within the context of Western Europe in the 18th century into its own moral practise – one that ultimately rested on the distinction between normal and abnormal. ‘Psychiatry could not have existed without a whole interplay of a political structure and without a set of political attitudes; but inversely, the establishment of madness as a domain of knowledge [savoir] changed the political practices and ethical attitudes that concerned it’ (Foucault, 1997, p. 284). According to this approach, it is not the arrival of a political definition of democracy, security, or discipline that is important, but, rather, under what conditions of knowledge, moral conduct and political action make a social process possible. In respect to this study, it allows for an account of how U.S. post-9/11 homeland and border security operates, not only in its response to the threat of terrorism, but how it is shaped by scientific and technical knowledge, constitutional imperatives and economic considerations.

3.2.3 Governmentality

This notion of problematisation when applied to a specific political issue gives way to what Foucault calls ‘governmentality’. As Rose, O’Malley and Valverde have described, the notion of governmentality can be seen to take shape within Foucault’s later work when he began to

address the processes and practises of political power[47] and in particular the birth of liberalism and a general logic of modern states that took shape towards the middle of the 18th century (Rose, et al., 2009). What is particular about the approach of governmentality is that when considering political processes, these processes are never reduced to classical expressions of sovereignty, economy or welfare, but, rather, focus on the multiple sites, strategies and technologies of government that are in fact responsible for the performance of a given political order. What further demarcates this approach from the one advocated by Shapiro is the style of questions that are asked of the political subject matter; for instance, a governmentality approach asks: 'what governs what, according to what logics, with what techniques, towards what ends' (Rose, et al., 2009, p. 3). This 'meta' reading of government seeks to determine how government responds to the situation and upon what grounds, rather than offers a direct assessment of what government should or should not do. Furthermore, as a method it contains two aims: to develop an 'alternate analytic of political power', one that acknowledges that government is made up of a heterogeneous, discontinuous, contradictory and at times self-defeating set of interests and practises; and second, to determine how these elements, when mobilised in specific and targeted ways, can be accounted for by analysing the strategies or 'political rationalities' that are brought to bear within the act of government (Rose, et al., 2009, p. 4). These two processes then enable government to be understood not as a totality responsible for the order of a given domain, but, rather, as a strategy amongst many. It is precisely how this strategy is composed that provides insight into the quality and efficacy of the governance of a specific population in respect to a specific set of political priorities or problematics. For Foucault, rationalities or strategies of governance are not based solely upon political or legal precept, but are informed by a relationship between knowledge/power – scientific methods that allow for an understanding of birth rates, mortality rates, health of population, number of thefts within a given municipality and the new forms of actors that are associated with the creation of such tools that inform political decisions – and come to be realised precisely at the point of intervention within the socio-political field. As described by Rose and Miller, governmentality then comes to be associated with '. . . [the] assorted attempts at calculated administration of diverse aspects of conduct through countless, often competing local tactics' (Rose & Miller, 1991, p. 3). What becomes the object of study for indeed political rationalities are the mobile and mutable discursive fields through which the exercise of power is conceptualised, and moral justifications for the exercise of power are transformed into statements that signal intent. Rose and Miller further observe that the question posed by governmentality is 'no longer one of accounting for government in terms of 'power of the state' but of ascertaining how and to what extent, the state is articulated into the activity of governmentality . . . [and] . . . what relations are established between political and other authorities' (Rose & Miller, 1991, p. 5). This is instructive because it displaces an analysis of the state from one that is numeric – state power measured according to how many police are provided for a given population, how many nuclear weapons are housed in the arsenal, or how many guards are stationed at the border – and it evaluates government according to how its aims involving the

[47] See: Foucault's seminar series: Security, Territory, Population and Society Must Be Defended.

instantiation of coercion and legitimacy are achieved. Furthermore, this achievement is not measured in respect to 'good' or 'bad', 'effective' or 'ineffective' – although value judgment on the part of the social scientist after empirical assessment is warranted – but, rather, through the ways in which government copes with these successes or failures that in turn lead to additional new forms of government. Government then muddles through and on, and it is a tracing of this practise that allows for the understanding and apprehension of political practise to take place.

3.3 Methodology: Discourse Analysis (Statement, Strategy, Archive)

As described, the concept and methodological approach of governmentality is through the analysis of language, in particular the analysis of the archive.[48] In The Archaeology of Knowledge, Foucault argues that the analysis of language does not imply the grammatical or semiotic formation of the sentence,[49] but, rather, is performed through the identification of statements understood as regularities even within a disparate data-set map to the same 'grid' (Canguilhem, 2003, p. 78). In order to understand the full implications of this methodology, it is important to understand how Foucault defines the terms 'archive', 'statement' and 'discursive formation' in respect to the earlier discussion concerning political rationales. Drawing on the work of Nietzsche,[50] Foucault argues that the archive should not be viewed as a neatly organised and successive historical construct, but, rather, as made up of a 'field of tangled and confused parchments' and of 'grey' 'documentary' materials (Foucault, 1984, p. 77). As pointed out by Canguilhem, what is further taken from Nietzsche is that to correctly understand a word or statement, an analysis must be conducted addressing who in fact provided the word, within what context and with what intention[51] (Canguilhem, 2003). The way through the archive for Foucault is via genealogy. The term 'genealogy', however, is not meant to describe a strict historiography of an event, but, rather, the identification of the 'accident, minute deviations, complete reversals . . . false appraisals, faulty calculations that give birth to those things that continue to exist and have value to us' (Foucault, 1984, p. 3). Here genealogy attempts to arrive at the identification of a grid across a set of records and objects – cultural, historical, scientific, artistic – separated both by time and by discipline, where a connection is made through a continuity or similarity of method, or amongst statements. This is what allows for regularity to be discovered amongst seemingly disparate types of data that compose the archive. Foucault points out that when applied to

[48] While Foucault understands the archive to be a historical archive, the understanding of an archive can equally apply to what Rose and Miller call 'the history of the present', where the multitude of documents that inform and make up contemporary political, social or scientific practises are used as source material.
[49] For instance, the meaning resulting from the logical construction of the sentence itself such as what is found as part of the deconstructive method used by Derrida.
[50] The Genealogy of Morals.
[51] This notion of the origins of meaning becomes clear when addressing a word and, in fact, a concept such as 'liberty'. For instance, the political theorist Isaiah Berlin argued that liberty could be defined not simply as the right to a form of freedom, but that this form of freedom was defined in positive and negative terms – positive in respect to the pursuit of goals; negative in respect to lack of intervention. This term, however, can be seen to be further contested by Heidegger – freedom not simply as positive versus negative but in respect to creativity and expression – and Rose, who has argued that freedom is in fact governed in a particular way via technologies of government within advanced liberal society – i.e., it is the appearance and belief in freedom rather than the material conditions that define the term.

social or political events, ‘the successes of history belong to those who are capable of seizing the rules, to replace those who had used them, to disguise themselves so as to pervert them, invert their meaning, and redirect them against those who had initially imposed them; controlling this complex mechanism, that will make it function so as to overcome the rulers through their own rules’ (Foucault, 1984, p. 4). This shows that the notion of the formation of a political rationality or diagram of government can be composed of a set of competing and discontinuous strategies, methods and initiatives. It is, however, only through a reading of the archive and the disparate regimes of knowledge that make up this archive that the motivations for government in respect to a socio-political event are revealed. Therefore, the question must be asked: If the archive is what yields an understanding through the analysis of discourse, how is this done? Are we not simply left with a multiplicity of elements that, while present in the field related to an event, do not allow for a coherent understanding of the event? For this, Foucault’s notion of the statement and discursive formation becomes important.

To answer this question, Deleuze provides a framework for the understanding of the statement through his reading of Foucault. Here the statement in Foucault functions as a regularity that can be found within the archive possessing the quality of rarity that allows for comparisons to be made with like statements within different contexts and historical levels (Deleuze, 1988). This description further emphasises that historical analysis is not necessarily required in order to identify the consistency of the statement. Rather, what is required is an archive that is deep enough in respect to the subject even if it can be truncated in respect to time. In order to further formalise this notion of rarity and the role the statement plays within discursive formations, Foucault offers four hypotheses:

i. That statements pertaining to political economy or science may refer to a similar object, yet may take on a different form. For example, citing the concept of ‘madness’, Foucault argues that during 17th and 18th centuries numerous statements belonging to psychopathology point in a direction to what is later formally understood as madness. It is here, then, that the explanatory value of madness can be found, in the competing, contradictory elements that allow for a mapping between various choices, propositions and practises leading to a cohered term. In the case of this research project, madness could easily be replaced with the notion of ‘homeland security’, understood not as term signifying the strength or fortitude of the U.S., but, rather, as the multiple practises, failed attempts and minor successes associated with a broad range of activities taken up by U.S. security, law-enforcement, immigration, customs and Consular services.

ii. Foucault identifies how these various and multiple statements are connected as a shared style or orientation (Foucault, 1972). Speaking of 19th-century medical science, Foucault indicates that for the first time medical practise

oriented itself around a consistent set of methodological principles and a grounded body of knowledge derived from those principles rather than the informal or overly theoretical approaches favoured previously. An example within the context of border security is the concept of identity. Up until 9/11, the identity of a foreign national was determined by either a passport and accompanying visa or driving licence[52] at the border; and, in fact, Americans crossing the Canadian or Mexican border could provide one of approximately 8,000 forms of identity to re-enter the country (Chertoff, 2007). After 9/11, the notion that identity could be reduced to several, let alone 8,000, different documents was found to be deeply problematic due to the opportunity for abuse; instead, what was asserted was that identity should be intrinsically linked with physical bodily identity. However, this bodily identity had nothing to do with the uniqueness of individual subjectivity, but, rather, with distinctive features found on the body that are not simply distinct in and of themselves but meet a scientific criteria of uniqueness. Here, when a fingerprint or iris is measured, it is required that it have a degree of statistical complexity that enables a fingerprint or iris code to be matched against itself in a different time and location. Identity can, then, be seen to become formalised both within the context of immigration and border security and according to scientific method that provides a general degree of certainty.

iii. The system of statements under analysis is not a permanent formalization. Here it is simply acknowledged that concepts pertaining to medicine or political economy, however fixed they appear, can be displaced or change meaning when transferred from one discursive domain to the next.[53] For instance, within the discourse of homeland security the notion of liberty cannot be seen as an immutable term; while liberty when grounded in political philosophy is taken as containing both positive (freedom of pursuit) and negative (freedom from interference) attributes, the notion of liberty and openness post-9/11 has consisted of a hybrid discourse that attempts to make liberty conditional upon enhanced security and the techniques that provide such security.

iv. Finally, this orientation towards the impermanent and contingent nature of the statement does not simply allow for an understanding of the emergence of a given social or political event, but it reveals a ‘field of strategic possibilities’ afforded to actors in respect to how governance is in fact

[52] Such as with Canadians passing into the U.S. or with Americans themselves crossing the border from Canada or Mexico.

[53] An example of this is the concept of ‘Brownian motion’, first developed in biology and named after Scottish botanist Robert Brown. Brown observed the seemingly random and continuous movement of particles suspended in fluid. This observation, which he made in 1827, was later imported into physics in 1880 in order to describe the general movement of particles, and then into mathematics and in particular the theory of financial speculation – random movement of stock prices – in 1900 by Louis Bachelier.

carried out. (Foucault, 1972)

Outside of discursive formations, the question that remains to be answered is: How can the technologies used at the border, such as biometric and data-mining technologies, be accounted for in respect to its performance and functioning within an institutional setting? This question is important because it is argued that alongside the charting of the political rationalities that post-9/11 U.S. border security comprises, the day-to-day functioning of technology used to achieve policy aims is also considered. The attention given to technology takes place in three locations: (i) within a discursive field – that is, scientific and political documents that represent the given technologies and attributes, along with their purpose of use; (ii) within the institutional setting itself, where identity technologies can be seen to trigger a set of events such as the identification of a threat leading to an arrest or the denial of entry to the United States; and (iii.) in respect to the rationales and patterns that inform threat models that are enacted by biometric or data-mining technology. The first and third representation of technology can be approached using the discursive methods described. For instance, technical diagrams and representations can be located within a broad array of scientific and government literatures; the threat models can also be seen to be constructed from prevailing social attitudes towards the risk of certain countries – Pakistan, Yemen, Iran – as well as certain passenger behaviours. However, how can the second representation of technology be accounted for, one that involves the functioning of the technology itself, and through this functioning sets off a causal chain as part of the institutional machinations and, in fact, a politics at the border? It will be argued that, while it is possible for this functioning of technology to be represented in the form of an account, the account still must presuppose the existence of a form of technological realism, because how these objects perform make the account possible. Canguilhem also raises this point in his reading of Foucault and his notion of discursive formation, where he questions an approach based solely on discourse:

> . . . this is not a mistaken approach, at least for mathematics, but it is questionable for physics, where theories, when they succeeded one another by generalization and integration, have the effect of detaching and separating, on the one hand, the change discourse and concepts it uses, and other the other hand, what has to be called and this time in a strict sense, the resistant mathematical structure. (Canguilhem, 2003, p. 85)

This implies that while language and discourse can be seen as mutable in respect to political or social circumstances that possess either deep or shallow historical underpinnings, language slows down and discursive formations potentially solidify when encountering objects of thought that are potentially more fixed – such as scientific objects. The further implication is that, even though the nominal world of discourse attempts to reflect upon, describe and compose new rationales for action based upon external events, these events contain an agency that is reflexive. This line of argument, however, wishes to avoid the well-trodden distinction between realism and constructivism; rather, it seeks to argue that in the consideration of scientific objects that contribute to a political project, the reality of such

objects and the fixity of the discourse that accompanies them further impacts how political rationales are initially composed, delimited and come to be further developed.

Here a form of scientific realism is required, because it provides a way to define a set of objects that are motivated to enact a particular type of politics – identification of threats while allowing efficient flow through U.S. borders to remain possible. For instance, Hacking argues that 'Weapons are making our world, even if they never exploded. Not because they spin off new materials, but because they create some possibilities and delimit others . . .' (Hacking, 1999, p. 167). The appeal to a form of scientific realism to account for the technology and technical systems used in the context of post-9/11 U.S. border security stems from the research aim to track and trace how biometric and data-mining technology functions within and contributes to the production of the security environment. While these technologies rest within a broader political or security rationality, or are deployed with the motivation to identify particular risks, these technologies can be seen to 'alter the spectrum of possibilities in which people act' (Taipale, 2003, p. 11). This means that while it is important to investigate the consequences of the use of particular technologies, it is equally important to account for the details of the technological operation and configuration in order to determine which potentialities are opened up and which are shut down. This focus on realism allows for a further understanding of the functioning of technologies at the border, not only in respect to how they match up with broader political aims, but how it works to trouble those aims and create an alternate set of politics. This notion of an alternative set of politics based on the function or performance of technology at the border then has three interrelated implications.

First, technology can be seen to either fulfil or deviate from the political or security aims set out by policy makers at the borders. In many ways, this is a naïve reading of how technology performs within a social science context since it merely acknowledges its existence or presence, while lacking an interrogation of its functioning. Second, technology when viewed according to its implicit mode of operation, as Hacking and Taipale suggest, opens up and closes down new possibilities and potentialities that can be shown to have particular political effects or can be regarded as security assets. Third, and more amenable to this study, is that technological or scientific artefacts bring with them a set of truth conditions, or causal mechanisms that can be seen to shape the institutional or security setup in which they are involved. Here it can be seen that the installation of biometrics not only carries a set of historical connotations concerning the application of fingerprinting techniques to subjugated populations, but, more pertinent to understanding of U.S. security practises, biometrics distinguish true identity claims from false identity claims; they can tell U.S. security services with certainty when an individual has entered the country; they can be used to distinguish the individual from other individuals held on suspect watch-lists. This causal property then creates a new set of values that co-determine[54] how security comes to operate at the border. Fourth, due to the statistical and experimental nature of the technology used at the border,

[54] 'Co-determine' is used here in order to distinguish this discourse from that of technological determinism, as well as to show that technology is only one part of the border security environment – as seen alongside legal, policy and institutional prerogatives.

biometrics, but more so data-mining and watch-list matching technology, produce a considerable number of false-positives that, when enacted in a high-security environment, have been shown to lead to false arrests, wrongful interrogation or denial of entry into the United States. As a result of this error rate, a secondary set of political and institutional responses has been created around the notion of 'redress'. For instance, if a foreign national feels that he or she has been wrongfully identified by the U.S. security computer system as having a terrorist affiliation, he or she can appeal this determination through the DHS.[55] The reading of technology that accounts for causal mechanisms, in the case of U.S. border security, can be seen to be essential, since it allows for an understanding of the practical and unintended consequences of the border security setup.

3.4 Proposed Outcomes: Security Governance

This methodology chapter has sought to outline the approach taken in respect to the reading and representation of the implication of digital-identity technology on U.S. border-security practise post-9/11. This reading involves an orientation towards case-study analysis, the analysis of language seen as a discursive formation comprised of policy, legal, scientific and institutional documents as well as the analysis of the performance of digital technology within a given security setup. Each of these sites then contributes to a broader framework described as the framework of 'governmentality', where each textual and technological process is considered to form a political rationality or diagram of government. This diagram does not, however, seek to produce a reading that affirms normative political or philosophical positions concerning such concepts as sovereignty or liberty, but seeks to establish a new mode of social and political understanding that is based on the multiple, competing and discontinuous forces at play within the border security environment. At the macro-level, this analysis seeks to place a reading of U.S. border-security practises in relation to broader phenomena or trends that comprise the political economy of the United States; on a micro-level this analysis to seeks to uncover a new set of politics and ethical conditions that are not only governed by the use of digital technology, but made possible through a permissive set of legal decrees and institutional mandates. Although the security practises of the border are amenable to broader political goals and aims that are a part of the constellation of practises making up the war on terror, it is at the border checkpoint, in the interrogation centre and within FBI biometric and PNR databases that the real politics and practise of U.S. border security can be found.

[55] It will be shown that the redress process is not as straightforward as it appears, since many individuals who have appealed terrorist determination, primarily in respect to the terrorist watch-list, have not had their names removed on grounds of national security.

4. [LAYER 1] Governance and War: Legal and Institutional Rationales Governing Search and Data Collection within Post-9/11 U.S. Border Security

4.1

Post-9/11 U.S. border security operates under the dual assumption that the threat posed by terrorism is catastrophic in impact and generational in duration. As a result, since 2001 U.S. homeland security has been organised under a new set of legal rationales based on principles of prevention and precaution.[56] This set of prerogatives constitutes the first layer of security that governs or informs institutional action within the context of the border, which is not only intrinsic to an understanding of how homeland security operates, but provides a grounding for the set of permissions of further homeland security practises discussed in the following chapters. What makes homeland and border security of interest from a legal and policy perspective is that, unlike traditional military threats emanating from the nation-state, contemporary terrorism is understood as global in its reach and asymmetric in its method. This can be seen not only with the 9/11 attacks, but with the bombing of the World Trade Center in 1993, where radical Islamists were able, much like their counterparts less than a decade later, to exploit the U.S. immigration system in order to develop and carry out a terror attack. This has had two consequences in respect to U.S. domestic security. First, significant legislation has been passed that has provided homeland security agencies with a new set of investigatory powers, oriented towards the collection and analysis of identity information held within public government repositories or obtained as part of the immigration process. Second, the policy orientation of war developed by the Bush administration has not only been directed outside the country but has turned inward in order to identify and uncover terrorist threats. This domestic application of counter-terrorism measures developed under the pretext of war has, however, resulted in domestic political controversy due to the application of increased executive power.

It will be shown that these two policy and legislative practises, working together have led to paradoxical consequences in respect to how U.S. domestic security is governed. First, in an effort to identify and uncover terrorist plots within the country, U.S. security services have adopted an approach towards search and intelligence gathering that has moved from one that is particularised – based on the identification and tracking of a singular subject of interest – to one that is non-particularised – based on the analysis of a population or database in order to identify patterns or individuals of interest. This non-particularised mode of intelligence gathering and surveillance has been taken up in respect to counter-terror in the domestic surveillance of Internet and telecommunications data of U.S. persons and foreign nationals alike through the access of domestic telecommunications services providers AT&T and Verizon. Second, this mode of non-particularised search is expressed in the analysis and collection of Passenger Name Record (PNR) and immigration data from nationals and non-nationals within the context of air travel to and within the U.S. The first programme, consisting of the data-mining of domestic telecommunication service providers, was cancelled in 2007 as result of potential infringements on Fourth Amendment provisions

[56] The notion of prevention and precaution is described in detail in Chapter 5 [Layer 3], focused on the collection and analysis of PNR data.

protecting U.S. persons from 'unreasonable or unwanted' search and seizure[57] even though the intended targets were not U.S. citizens but foreign national data held on U.S. servers. The second programme, the collection of traveller data, has proven to be a central pillar of U.S. border security, yet in circumvention of European law that affords protections to European citizens and the transfer of personal data to third-party countries. These examples show that, while on the one hand executive power involved in counter-terrorism is legally curtailed within the domestic context, it is granted greater agency and displays a practise of unbounded executive power when exercised upon those individuals who are obfuscated jurisdictionally and not afforded the same rights and protections as U.S. citizens.

4.1 9/11 and the Discourse of War (Executive Authority, Information Collection)

> Yesterday our nation observed the five-year anniversary of the September 11th attacks. For most Americans, 9/11 remains a defining moment in our lives and for our nation. Even today, it is difficult to fully comprehend the devastation and loss of life flowing from the senseless murder of nearly 3,000 men, women, and children of all backgrounds and faiths, and this premeditated act of *war* [italics mine] against the United States. (Chertoff, 2006, p. 1)
>
> First, screening people at the border. Our perimeter defense depends on keeping dangerous enemies out. Before 9/11, we had to rely on fragmented databases of biographical information to determine whether a person posed a security threat or should be allowed to enter our country. This process was often cumbersome for travellers, inefficient, and fraught with security vulnerabilities. The entry of terrorists before 9/11 tragically illustrated the cost of those vulnerabilities.
>
> Today, we have substantially transformed screening capabilities at our international ports of entry to prevent terrorists and criminals from successfully entering our country. We have integrated our counter-terror databases and together with the State Department have dramatically enhanced visa issuance processes. As important, we have implemented US-VISIT biometric entry capabilities at 117 airports, 16 seaports, and 153 land ports of entry. Within seconds, we can positively confirm a person's identity by checking their two digital finger scans against terrorist and criminal watch lists and immigration records. (Chertoff, 2006, p. 3)
>
> Secretary Michael Chertoff, Department of Homeland Security

> The intelligence services must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented. (Posner, 2006, p. 5)
>
> Richard A. Posner

[57] This program was cancelled, even though the Bush administration argued that the intended target was not U.S. citizens but members of Al Qaeda.

The political[58] debate concerning the American response to the 9/11 terror attacks can be seen as one that has centred not only on the opposition between security versus liberty, but more profoundly on the type of agency exercised by the executive branch during times of emergency. The events that define this debate have primarily resulted from the engagement by the U.S. military in Afghanistan and Iraq during the three years following 9/11. Although the American public regarded the military operations in Afghanistan with some consternation, a deeper political insecurity was felt in respect to the early product of the Afghanistan war; namely, the creation of the Guantánamo Bay prison camp used to hold what the Bush administration defined[59] as 'enemy combatants'. At the outset of the Afghanistan war the Department of Defense (DoD) issued a memorandum that deemed members of Al Qaeda and the Taliban captured on the field of battle in Afghanistan not to be entitled to prisoner of war (PoW) status under the framework defined by the 1949 Geneva Conventions (Rumsfeld, 2002). Since neither Al Qaeda nor the Taliban represented the Afghan state, members of each group could not be understood to participate in recognisable and governed armed conflict. This articulation had two implications: (i) as a result of a lack of this nation-state affiliation, the U.S. military saw it to be within their right to hold approximately 900 members of the Taliban and Al Qaeda who were captured on the battlefield of Afghanistan since 2002 at Guantánamo Bay 'indefinitely' with only with the prospect of a military tribunal if and when an individual has been deemed either non-dangerous or no longer possessing intelligence value;[60] and (ii) it has allowed the U.S. military and U.S. security to not only engage in combat and security operations that are divorced from a legal codification – that is, they exist and function as the political expression of executive wartime authority – but these operations have been made possible by utilising the space created by the lack of rights provisions, when viewed from the perspective of American interest, afforded to foreign nationals[61] (Bigo, 2010). Here what is revealed is an example of a zone or state of exception described by Agamben. Empirically, this zone is tied to a location of jurisdictional ambiguity; theoretically it reveals a location where the law has receded yet political practise remains intact. Agamben further points out that the state of exception rests at the 'ambiguous and uncertain fringe at the intersection of the legal and the political' constituting a 'point of disequilibrium between public law and political fact' (Agamben, 2006, p. 1). How, then, can this notion of executive privilege or sovereign capacity be accounted for in more specific ways in respect to the war

[58] This debate has also been an academic debate, and perhaps the use of the term 'academic' is a more suitable term than 'political' since, while the war on terror has resulted in political opposition in respect to the legacy of the Bush administration, particularly in respect to the detention without trial of 'enemy combatants' at Guantánamo Bay, rarely has there been a questioning of the ontological functioning of executive power within mainstream U.S. or E.U. political discourse. Indeed, this discourse has focused primarily on perceived illiberal actions taken by the Bush administration, directed at a potentially dangerous foe that, while unsavory, have potentially led to an increase rather than a decrease in security. The academic debate concerning executive power has been much more pointed in questioning the validity and limits of executive action.

[59] This definition of 'enemy combatant' has been held in the transition from the Bush to Obama presidencies.

[60] The issue of holding enemy combatants not only challenged the application of the Geneva Conventions, but also worked around such things as the reading of 'Miranda' rights to the accused held at Guantánamo, as well as habeas corpus for those who were changed by military tribunal of terror crimes.

[61] This is an important point that can be carried over into post-9/11 U.S. border security, whereby U.S. intelligence action and/or agency has been framed and enabled by the distinction between national and non-national – where nationals are given by Fourth Amendment rights protections in respect to search whereas foreign nationals are not. This distinction, then, has provided for the development of a security practise that while deemed as 'homeland', thus providing security to every American, can in fact be understood as a securitisation of foreign national populations moving in, out and within the country.

on terror and specifically to homeland security? To answer this question, a brief re-rendering of the work of Bush administration legalist John Yoo is required.[62]

War

The first assertion is based on the belief that the United States is in fact at war with Al Qaeda and that as a result the response that is required from the executive is one that is unilateral and departs from the political deliberation process found during normal times (Yoo, 2006). For Yoo, this notion of war has been understood not simply to be an academic or policy argument that could be interpreted in the previous quotation by Secretary Chertoff, but as a result of the passing of the Authorization for the Use of Military Force (AUMF) by Congress on September 18, 2001. As presented, the AUMF authorises the U.S. military, whereby the president is understood as commander in chief, to use military force against those 'responsible for recent attacks against the United States' (Congress, 2001, p. 1). Furthermore, the AUMF specifically grants the president the authority to use force against those 'nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001' (Congress, 2001). For Yoo and for the Bush administration, this assertion by Congress, while technically not an official declaration of war, provided the executive branch with the tactical and strategic flexibility that it viewed as necessary in order to neutralize the threat.

Intelligence

This notion of flexibility and unilateral decision-making during times of emergency leads to the identification of a second rationale outlined by Yoo: the emphasis on intelligence gathering as an effective way to support security and military efforts. Appealing to a game-theoretic definition of risk – action based on incomplete information – Yoo argues that intelligence gathering is not only a way to predict and prevent future threats, but a fundamental pragmatic attribute or quality of war (Yoo & Sulmasy, 2007). Whether gathered from humans via informants or intelligence officers (HUMINT) or obtained via signal interception (SIGNIT), intelligence is a way for the executive branch to reduce uncertainty in the decisions it makes (Yoo, 2006). In the case of Al Qaeda, Yoo argues that an intelligence effort drawing from both HUMINT and SIGNIT is essential, since not only does Al Qaeda have operatives in over 50 countries; it practises an art of warfare that is clandestine and asymmetrical. As a result, not only the executive branch, but also the intelligence community, Yoo asserts, must collect and share information in order to remain flexible in the face of this potential danger (Yoo & Sulmasy, 2007). The outputs of this argument in respect to changes in counter-terrorist practise post-9/11 can be seen in to take place in three areas:

[62] This is not to say that this approach is inherently problematic. Indeed, as Agamben rightfully identifies, a serious political issue is raised given the situation of unmediated sovereign violence even during times of emergency. However, the main aim of this chapter, as well as one of the goals of this thesis, is to chart the governmental rationale that accounts for the very modes of social practise Agamben speculates exist. That is to say, by looking at an advocate of the war on terror, we are able to identify the key assumptions that have framed many of the actions taken by the White House against or beyond the implicit will of Congress, which appear not only in the foreign zones that have come to define the war on terror, but domestic intelligence and border security practises as well.

intelligence-gathering reform, whereby the FBI has been granted greater flexibility to carry out surveillance of foreign agents through amendments to FISA 1978; the initiation of new domestic intelligence programmes that have tested legality whereby the aim has been to identify agents of foreign powers amongst large-scale communications data warehouses residing in the United States; and, finally, the linking up of the DHS – and within it the institutional functions of immigration, customs and border control – with domestic intelligence in order to analyse biometric and biographic data collected at the border.

Search

What follows from these two assertions by Yoo, and, in fact, the empirical transformations in respect to U.S. homeland security, is the further advocacy for a type of counter-terrorism practise that provides security services with additional freedoms and relative detachment from the criminal justice system. This assertion is based on two factors already mentioned, that during times of war the president and the executive branch indeed have the authority to carry out actions deemed necessary to successfully realise their security goals – in this case, the prevention of a terrorist attack and/or the apprehension of terrorists, whether in the United States or abroad. Second, since intelligence gathering and surveillance play a central role in this established aim, adherence to criminal-justice protocols, such as the issuing of Miranda[63] rights upon the arrest of a suspect and/or the establishment and verification of probable cause in order to obtain a search warrant, would only hamper and interfere with intelligence and law-enforcement efforts directed at a nimble and unpredictable foe. This requirement to pass all 'wartime' surveillance activities through the filters appropriate to the criminal justice system has a further set of consequences; not only does it reduce the speed with which domestic intelligence and law enforcement are able to respond, it also qualifies what counts as a legitimate pursuit for an intelligence investigation/surveillance operation – as with the application of a FISA warrant[64] and outlined through legal texts that may or may not correspond with needs on the ground. Therefore, it interferes with what are viewed as necessary wartime surveillance actions that may or may not be conducted in secret and, as a result of entering a terrorist case into the criminal justice system, is not only extremely lengthy and costly, but it is viewed as creating the risk that the individual charged may not be brought to justice due to procedural technicalities.[65]

[63] Miranda rights are required by U.S. law to be applied during the arrest of an individual so that the suspect is informed of the charge placed against him or her and given both the right to remain silent as well as the right to an attorney.

[64] The parameters afforded to intelligence investigations will be described in greater detail in the following paragraphs.

[65] A further complication has been created as a result of the prolonged detention of Guantánamo Bay detainees and their entrance into the criminal justice system. Because these detainees have since 2001–02 been held for purposes of perceived risk and intelligence value, they have not been treated according to a set of methods and routines concerning evidence afforded to individuals who enter the criminal justice system – this includes the use of 'enhanced interrogation techniques' that have been regarded as having borderline legality. As a result, the evidence gathered, while it has been taken up by the intelligence community, is viewed by the courts as either unreliable – evidence obtained during physical or psychological distress can only be viewed as partially reliable since the person under interrogation will have a tendency to tell interrogators 'what they want to hear' in order for the interrogation to stop – or as a national security risk, since the revelation of sources and methods used in evidence gathering as well as the evidence itself could potentially reveal the plans and activities of U.S. intelligence itself.

These assertions that urge a movement away from the conduct of counter-terrorist practises, in particular domestic surveillance, from the established practises of the criminal justice system, can be seen to be taken up not only in specific counter-terrorism programmes such as the wiretapping of AT&T and Verizon by the National Security Agency (NSA). Here these practises reveal a new mode of governmental logic whereby domestic surveillance is seen to move from one based on particularised to non-particularised forms of search. It will be shown, however, that this movement to non-particularised search is not unbounded; and therefore, despite its movement away from highly regulated monitoring and supervision, U.S. intelligence and the way in which intelligence information is gathered is in fact governed and limited due to legal, technological and institutional factors. However, despite these limitations the affordance of greater agency to domestic intelligence as a result of a wartime rationale has provided greater flexibility in conducting surveillance, whether in respect to nationals or foreign nationals. This has had two consequences: first, in respect to the governmentality of this non-particularised form of search, while it can be seen to be deployed as a new counter-terror technology, it has since 2001 been bracketed in its use due to Fourth Amendment protections barring unwarranted search and seizure of American citizens, to be deployed primarily in respect to the border zone, where traveller data, and primarily foreign national customs and immigration data, have become a site of active analysis. Second, as a result of the deployment of this mode of investigation, U.S. intelligence has developed a new typology of threat that exceeds practises aimed at identifying those who have already committed or could potentially commit an offence — identifying, blocking, tracking and interrogating individuals deemed as threats, revealing a precautionary rationale at work within homeland security. In order to understand how this rationale of non-particularised search performs and to determine its implications, it is important to identify how the FBI conducted intelligence pre-9/11.[66]

4.1.2 Domestic Intelligence Practises Pre-9/11

> [W]hen it comes to deciding whether and when to bring charges against terrorists, I am comfortable knowing this: I would rather explain to the American people why we acted when we did, even if it at a very early stage, than try to explain why we failed to act when we could have, and it is too late. (Justice, 2008, p. 1)
>
> Attorney General Michael Mukasey

Although it may appear to be a diversion to discuss the role of the FBI in respect to domestic and in particular border security operations, as it has been argued in Chapter 1 as well as at the outset of this chapter, an understanding of U.S. domestic intelligence practise serves two purposes. First, it provides an orientation as to where and in what manner U.S. domestic security strategy originates; second, while the DHS administers the customs, immigration

[66] These intelligence practises were touched on in respect to the 9/11 terror attacks themselves, but it is important to consider the broader culture of intelligence present pre-9/11 in an effort to chart the movement not only to the adoption of new rationales and policy prerogatives to conduct domestic security, but also how U.S. intelligence has been able to accommodate the use of new technologies primarily data-mining tools and biometrics.

and border-security process, the information that DHS/CBP officials act on as well as the ultimate determination of threat is administered by the FBI and surrounding agencies within the Department of Justice – for instance the National Security Agency (NSA), National Counter Terrorism Center (NCTC) and Terrorism Screening Center (TSC). It can be seen that U.S. domestic intelligence agencies provide the ground or framework through which the more visible public institutions, such as the DHS, operate. Furthermore, a suspected terrorist is also integrated into the U.S. criminal justice system through the development of case materials performed by the FBI, because terrorism, whether conducted by a U.S. national or non-national, falls under the FBI's mandate. However, it is precisely this intersection between the intelligence-gathering efforts against 'foreign agents', as governed by FISA; the softer intelligence gathering and analysis of foreign national data, such as at the border; and the repurposing of this intelligence information gathered from either source for either criminal investigations or for counter-terrorism efforts that has proven to be a site of contention. This is due not only to the act of intelligence gathering itself, but as a result of the movement by the FBI, identified in the early 1990s towards a strategy of prevention from one of case building, where a response to a threat took place only after the event was realized (9/11 Commission, 2005).

In 1993 after the bombing of the World Trade Center, an attack that killed six people and injured more than a thousand, the FBI adopted a policy orientation of prevention, stating that 'merely solving this type of crime is not enough; equally important that FBI thwart terrorism before such acts can be perpetrated' (9/11 Commission, 2005, p. 76). While this movement towards prevention was intended to be a reform felt agency-wide, the actual development and implementation of this institutional capacity was held back for two reasons. First, counter-terrorism within the FBI – despite the 1993 World Trade Center bombing, the uncovering of the 1993 'Landmarks Plot', the 1995 Manila Airlines Plot and the 1996 Khobar Towers bombing in Saudi Arabia, amongst several other Al Qaeda–related attacks leading up to 9/11 – was not viewed as a major priority in the department. For instance, as was mentioned in Chapter 1, the focus of customs officials at U.S. airports was on identifying drug smugglers or 'intending immigrants' – in fact, addressing America's other war, the 'war on drugs'.[67] For instance, in 1998 when the DoJ reviewed the priorities established by the FBI, it found that the bulk of its financial and human resources were directed at preserving national economic security. At the time of the 9/11 attacks, 1,300, or 6%, of the total FBI staff were assigned to counter-terrorism – the number of analysts assigned to counter-terrorism has increased to 2,100 in the post-9/11 years (Justice, 2008). However, this lack of resources and attention was not only confined to analysts assigned to counter-terrorism, but it was found that the FBI had deficient institutional and technical systems for knowledge management. For instance, due to the decentralised nature of the FBI, where active analysis is passed on to agents working out of any number of 56 field offices, it was extremely difficult to disseminate this information agency-wide (9/11 Commission, 2005). This inability to

[67] Catch-phrase for an effort to battle the smuggling of drugs from Central and South America to the United States; this phrase was first used by President Richard Nixon in 1971.

adequately communicate and share within as well as outside of the agency, for instance between the FBI and the DoJ or the CIA consists of the second challenge faced by the FBI pre-9/11 and what has already been described in Chapter 1: the establishment of informal institutional prohibitions on sharing described as the 'wall'. The key institutional barrier represented by the 'wall' was the result of the determination by the FISA Court (FISC) that intelligence gathered via a FISA warrant obtained from surveillance of 'agents of a foreign power' could not be 'seized upon by prosecutors from the Department of Justice, in their attempts to make a criminal case' (9/11 Commission, 2005, p. 4). FBI agents could use FISA warrants to build criminal cases themselves – to be later passed onto the DoJ – however, they were not allowed to collaborate with the DoJ in order to direct the application of surveillance so that it would impact that direction of a case. This led to the self-creation of internal barriers that were in part a direct result of FISC intervention and in part based on a lack of understanding about how and if information could be shared, not only between the FBI and the DoJ or CIA, but within the FBI itself. FISA and its surrounding guidelines also had further unintended consequences. Not only has it been criticised by a host of legal theorists (Yoo, Posner, Taipale) for its lack of compatibility for the digital age but attorney general guidelines from 1978 – revised in 1995 – further prohibited the FBI from utilising publicly accessible information[68] unless it had a specific purpose for an investigation (9/11 Commission, 2005). This limitation, while intended to curb governmental abuses of power in the 1970s, was seen to foster an intelligence culture that lacked a particular ambition or drive to find new sources and leads.

As represented in the quote at the head of this section, the strategic orientation of prevention can be seen to have its origins in the early 1990s with this mode of security practise only to be realised post-9/11. The question that must be asked, however, is how far does this preventative/precautionary practise move away from the principles of criminal justice by U.S. intelligence, where non-particularised search can be seen to be this new security logic? And, second, how can this twin notion of war and exception be accounted for in respect to the legal and policy prerogatives of domestic and homeland security? The answer to this question is threefold: (i) it can be seen that the criminal justice system has not been abandoned, but, rather, has been utilised as a preventative technique to intervene on suspected terrorists – these interventions can be seen as both disrupting major terror plots as well as using immigration violations or other such minor offences to ban foreign nationals from the country; (ii) where the criminal justice system has been avoided is in respect to FISA, where mass domestic intelligence gathering in 2006 conducted by the NSA of telecommunication servers held by AT&T does signal the emergence of this new logic of non-particularised search, yet it also shows that constitutional limitations deflect this form of search away from U.S. citizens and towards foreign nationals; and, finally (iii.), in the case of U.S. border security practises domestic intelligence and homeland security are granted the greatest amount of flexibility in respect to search and risk assessment of foreign nationals

[68] Such as information found on the Internet or other such public records.

entering the country – however, here it can be seen that both criminal justice measures oriented towards past crime as well as preventative measures are at work.

4.1.3 Domestic Intelligence Practises Post-9/11 (Legal Precepts)

> [T]he overriding priority in these efforts is preventing, pre-empting, and disrupting terrorist threats to the US; in some cases this priority will dictate the provision of information to other agencies even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. (Ashcroft, 2003, p. 1)
>
> Attorney General John Ashcroft

The major changes applied to the FBI consisted not only of further articulating preventative policies towards terrorism, but also passing legislation to make domestic intelligence gathering efforts more flexible and encourage information sharing[69] between the FBI and DoJ as well as within the FBI. As a result of these two factors, since 9/11 the FBI has not only articulated an active practise of sharing intelligence information with DoJ prosecutors, but has turned to prosecutors in order to aid FBI counter-terrorism efforts by charging those individuals suspected of terrorism with relatively minor offences – immigration violations, false statement charges, identity theft (Justice, 2008). While this form of counter-terrorism practise can be described as preventative, for the FBI it is referred to as 'neutralization' of the terrorist threat, where if prosecutors fail to establish a case based upon terror-related crimes, the FBI and the DoJ not only work to find a lesser charge, but act politically utilising alternative methods at their disposal, such as the seizure of financial assets located within the United States, deportation or sharing intelligence information with the security services of the individual's home country (Justice, 2008). While this type of counter-terrorism practise appeals to principles of criminal justice, it can primarily be seen to incorporate preventative measures in respect to how, in fact, that law is carried out.

Ericson describes this form of counter-terrorism practise as a 'counter-law' or the use of legal precepts such as immigration law, to achieve counter-terrorism claims aims. Ericson establishes that these infractions, whether related to immigration or to other forms of civil law, allow for the circumvention of procedures of due process, since individuals charged with immigration-law offences are not entitled to a defence attorney as with criminal law (Ericson, 2008). This claim can be supported by looking at the FBI's use of immigration law immediately following the 9/11 attacks. According to a report produced by the Office of the Inspector General (OIG), in the 11 months following 9/11, the FBI, working with DoJ prosecutors, detained 762 aliens who were believed to have a connection with Al Qaeda, or were discovered through the course of the investigation, on minor immigration infractions such as entering the country illegally, making false statements or overstaying the visa

[69] The legislation in question is: (i.) the 2008 FISA Amendment Act, which made the FISA warrant process more appropriate to be applied to digital communications technologies; and (ii.) the 2005 USA Patriot Reauthorization Act, which sought to formally remove the 'wall' established between the FBI and DoJ, whereby the Patriot Act mandated greater sharing between intelligence and criminal justice for the purpose of counter-terrorism.

duration (Ervin, 2003). Beyond simply detention for the suspicion of terrorist links, which could seem reasonable if conducted for a short duration after such an event, the OIG found that the FBI made little attempt to distinguish within this group between those who were detained as a result of credible evidence suggesting terrorist ties and those who were 'picked up incidentally as part of the investigation' (Ervin, 2003). Furthermore, since the detentions were warranted against foreign nationals even if initiated by the FBI, the INS was made responsible for carrying out the detentions. However, since the individuals identified by the FBI were viewed as high-value suspects, they were given 'hold and release' orders, whereby each individual had to be cleared by the FBI before being released. Also, due to the national-security priority assigned to each detainee, the FBI was reluctant to share information regarding the degree of suspicion each detainee was held. As a result, the INS was unable to indicate to the detainee the exact reason for his or her detention, apart from the fact that it was related to an immigration violation, until some 72 hours after the arrest; moreover, detainees were denied the ability to post a bond for provisional release from detention. As a result of the 'hold and release' orders, as well as the rather spurious information under which many of the 762 detainees were held, the average release time reached approximately 80 days (Ervin, 2003). How does this example match up with Yoo's argument that executive action, here including domestic intelligence, should work around or outside the criminal-justice system during times of emergency? Clearly, in this example although criminal justice practises are appealed to, the use of law during a time of emergency has a preventative and precautionary orientation, and within such a rationale, it has been short-circuited or compromised here by the lack of due process whereby individuals held on immigration violations would be fully informed of the charge against them. This security and intelligence rationale is instructive, because while the FBI, for domestic intelligence and security purposes, can be seen in this instance to take advantage of the lack of protections afforded to foreign nationals in respect to immigration-related violations, this same security logic is present within the context of the border. The border, however, is not only seen as an active site to identify and intervene upon individuals who have been determined to have already committed a crime, such as the detention of foreign nationals post-9/11, counter-terrorism practises and, in particular, those that use non-particularised forms of search seek to prevent suspected terrorists from entering the United States, not to arrest them.

4.2 From Particularised to Non-Particularised Search

A substantial part of the modernisation of domestic intelligence and border security is the integration and incorporation of technologies of data sharing and analysis. Although the specific technologies used within post-9/11 border security are addressed in Chapters 5, 6 and 7, data-analysis technologies can be seen as a new institutional capacity afforded to the FBI, enabling it to manage, assess and share its own internal data in order for this data to contribute to ongoing terror investigations as well as to counter-terrorist operations at the border. As a result, the FBI's data-sharing and data-analysis capabilities act as the central

processing hub for counter-terrorist information, which in coordination with the NCTC and the TSC is distributed to customs, border and immigration control along with domestic law enforcement. Alongside this newfound orientation allowing U.S. security services to become more self-aware, the databases utilised for sharing information can be seen to contain novel information only realised through the use of data-mining or knowledge-discovery tools. For instance, the use of a data-mining technique called 'link analysis' allows the mapping of the social network of a known or suspected terrorist by analysing identity information – phone, credit card and frequent flyer numbers – that can be used to build associations. A further use for data-mining[70] technology is 'predicate triage'. The data-mining expert and IBM scientist Jeff Jonas argues that predicate triage can be a useful technique if a government has limited resources for enforcement. If a government is able to see that 100,000 individuals remain in the country with expired passports, it is able to determine with the addition of search criteria who poses a national security risk and, given enough information, who is simply in the country attempting to find employment[71] (Rosenzweig & Jonas, 2005).

In order to address the implications of these forms of search as well as those two forms of search described in the Chapter 2,[72] it is important to understand past legal precedents that informed intelligence and law-enforcement action and that share the same 'grid' or diagram as current practise (Canguilhem, 2003). The basis for non-particularised search can be found within the 1968 U.S. Supreme Court case *Terry v. Ohio,* where it was found that Fourth Amendment protections[73] — to be free of unwanted search and seizure – are not violated in the case of police questioning and search if the arresting officer has reasonable suspicion of criminal activity (John W. TERRY, Petitioner, v. STATE OF OHIO, 1968). The basis for this decision, otherwise known for granting 'stop and search' powers to police officers, was upheld by the U.S. Supreme Court, which sided with an off-duty Cleveland police officer in 1968 who noticed three men 'casing'[74] a general store in advance of a daylight robbery. The off-duty officer proceeded to question and search the trio after they walked down the street away from the store. This action resulted in the discovery of two

[70] They are applied to a greater degree to the collective of foreign nationals who are interested in travelling to or residing within the United States, for the primary reason that they lack constitutional protections in respect to data acquisition and data sharing – search and seizure; where data is collected from U.S. persons – nationals and green card holders – as in the case of travel data, the amount of data collected, unlike with that of foreign nationals, is limited as a result of constitutional protections. As a result, the ability to analyse, share and store data on foreign nationals for intelligence purposes, whether to do with travel data, biometrics or visa/passport information, is made more flexible and permissive.

[71] A clear distinction must be made between these data collection and analysis efforts – where they incorporate new techniques of search – and those ongoing efforts by U.S. intelligence to monitor and investigate individuals suspected of terrorism through the FISA warrant process. Despite the indication in this chapter as well as in Chapter 1, the FISA process, though amended by the USA PATRIOT Act to allow for FISA warrants to be obtained upon the basis of 'significant' rather than 'primary purpose', still remains a valid vehicle for domestic intelligence and counter-terrorism efforts to take place. For instance, FISA applications can be seen to rise from 932 in 2001 to approximately 2,100 each year over the period of 2005–07 and then back down to approximately 1,300 in 2008–09 (EPIC, 2008) (Weich, 2010). What this shows is that FISA warrants and the FISA process remain a vital tool in respect to counter-terrorism, but it also represents a striking contrast in respect to the mass data collection efforts for intelligence purposes at the border that make up the passenger screening process.

[72] Subject- and pattern-based analysis or data-mining.

[73] The U.S. Constitution's Fourth Amendment is defined as: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

[74] Arresting police officer detective McFadden witnessed the assailants peering into the windows of a general store 24 times over the course of 12 minutes, throughout which they were also seen conferring with one another.

loaded pistols, prompting an arrest of the individuals in question (John W. TERRY, Petitioner, v. STATE OF OHIO, 1968). The petitioner, John W. Terry, argued that police search that led to his arrest was a Fourth Amendment violation, that the off-duty police officer did not have the right to search and then seize the weapons he and the second accomplice, Richard Chilton, had in their possession[75] due to lack of probable cause.[76] The courts determined that the search was reasonable on the following grounds. First, it is was reasonable for an officer who was 'on the beat' to quickly respond to what was deemed suspicious activity based on 'on the spot observations' and as a result of the speed required for intervention did not require a warrant. Second, via an appeal to 'government interest' where it is in the interest of law enforcement to work on behalf of the public to detect and prevent crime and therefore approach an individual for the purposes of 'investigating possibly criminal behaviour without probable cause for arrest'; and, finally, due to the circumstances of the case, the police officer believed that Terry, Chilton and Katz were planning to perform a daytime robbery and therefore would potentially be armed, thus it was entirely reasonable for the arresting officer to assume such a scenario and search for weapons (John W. TERRY, Petitioner, v. STATE OF OHIO, 1968). What is compelling about the arguments presented by the Supreme Court is their relationship to those assertions offered by Yoo, which can also be located within the preventative policy framework of the FBI. That is, given a national threat such as terrorism, it is reasonable for U.S. law enforcement and domestic security to stop and search individuals who are believed to exhibit signs or predicates of suspicion. This preventative posture is also supported by the argument that due to the unpredictable and time-sensitive nature of terrorism and, in this case, crime, actions taken by law enforcement or intelligence are permissible even if they do not stick with standard investigatory procedures since they serve a higher purpose. Furthermore, it would also be reasonable to apply this set of principles to the collection and search of personal data or identity information, from an individual or a group, given reasonable suspicion on the part of law enforcement. In the case of *Terry v. Ohio,* this mode of search can be considered as particularised, where the arresting officer identified the suspicious actions of Terry, Chilton and Katz and acted on them. However, this notion of reasonableness of search need not apply to given individuals, but can also be localised in order to apply to groups. For instance, there is a reasonable expectation that an individual boarding an aircraft must submit him- or herself to a series of screening procedures of their person,[77] or, as the legal theorist Jonathan Zittrain has pointed out, that it is acceptable for the government to lower Fourth Amendment protection standards if it has the interests of public safety in mind; for instance, in setting up a checkpoint to catch drunk drivers or allowing housing inspectors to enter private premises in order to determine safety violations

[75] The third accomplice, who is simply referred to, as 'Katz', was not charged with possession of a weapon or any other crime as part of this case.

[76] Probable cause, used within U.S. criminal law, is defined as 'a reasonable belief that a person has committed a crime'. Furthermore, the test applied to determine if probable cause exists for the purposes of an arrest is the determination of whether or not 'facts and circumstances within the officer's knowledge are sufficient to warrant a prudent person to believe a suspect has committed, is committing or is about to commit a crime' (Lectric Law Library, 2010).

[77] As it was shown in Chapter 3, Methodology, not only were metal detectors introduced into airports in 1974 reasonable, they were determined to be vital to reducing the number of aircraft hijackings that plagued U.S. airlines during the 1960s to '70s.

(Zittrain, 2006). Here the search that is performed can be understood as non-particularised; that is to say, the population in general is known to contain certain risks, therefore police action is warranted even if the risky factors are not necessarily known to be present in this case. The question then remains: If this notion of reasonableness can work to accompany modes of non-particularised search, what are the limits of government interest in respect to suspicion and crime prevention? Or, in the case of post-9/11 domestic and border security – clearly a situation of heightened security and suspicion whereby a new asymmetrical threat has blended itself into the foreign national population, not only entering but residing within the country – what limits can be drawn? It will be argued in the following paragraphs that while airport and border security has become more involved since 9/11, search in respect to mass data collection has been permissive and flexible in respect to foreign nationals and restricted or regulated although still problematic in respect to search of American persons.[78]

4.3 Domestic Spying Program: AT&T/Verizon

In 2005 the New York Times uncovered a secret warrantless domestic-surveillance programme conducted by the National Security Agency (NSA), authorised by the Bush administration shortly after 9/11, which was designed to discover terrorist activity within the vast databases held by U.S. telecommunications companies (Eric Lichtblau, 2005). The programme was designed not only to access these mass telecommunications databases in order to identify terrorist patterns, but to exploit the fact that by both design and by accident, the United States had become the centre of global telecommunications traffic, where companies such as AT&T and Verizon held in their databases not only domestically transmitted data, but data that was sent from the United States overseas and in many cases overseas traffic that simply used U.S. infrastructure for the purposes of routing global communications.[79] As a result, the Bush administration saw it as an asset to access these databases in order to search these databases and monitor traffic – phone calls, e-mail, phone logs – in the hopes of finding evidence of terrorist identity as well as terrorist plots originating outside of the country yet could be found within U.S. telecommunications databases (Eric Lichtblau, 2005). Although the surveillance was conducted in secret and in cooperation with AT&T and Verizon, it was revealed that the NSA programme, while accessing these databases, also contained data pertaining to U.S. persons, alongside foreign nationals. However, when the programme was revealed to the public, not only was there concern or controversy that extended to the infringement on civil liberties, but questions concerning the legality of the programme in respect to Fourth Amendment protections due to the warrantless search of a U.S. person – here a U.S. corporation would be considered a 'person' even if it acted voluntarily with the government. In defence of the programme, three arguments were put forward: (i) that, as it has been argued, there was a

[78] 'Persons' within the language of FISA refers to U.S. citizens, U.S. resident aliens and U.S. incorporated businesses.

[79] The fact that international to international traffic is routed through the U.S. is the result of both how telecommunications infrastructure has developed, primarily with investments into speed and bandwidth taking place within the U.S. and via competitive pricing that has made it cost-effective and more efficient to route international traffic via U.S. telecommunications hubs.

requirement for the NSA programme to work around FISA in its collection of foreign intelligence agents because FISA, even with the amendments as part of the Patriot Act, was not nimble enough and did not reflect a changing landscape of technology and communication; FISA was not designed for super-massive databases containing communications in digital form; (ii) due to the asymmetric threat posed by Al Qaeda whereby a clear distinction cannot be made between terrorist and non-terrorist, further information or intelligence is required in identify a threat; and (iii) that the president during times of war has the inherent authority to authorise such programmes to protect national security. The further justification for this third point in respect to the NSA programme has been argued by Attorney General Alberto Gonzales, who indicated in a congressional hearing on the NSA programme that the president's wartime powers were approved by Congress as part of the 2001 'Authorization for the Use of Military Force' which contained the words, pointed out by Gonzales, that 'authorize[s] the President to use all necessary and appropriate force'; and further argued that 'we believe signals intelligence to be a fundamental incident of war' (Bazan & Elsea, 2006, p. 2). Second, it was argued in review of the FISA Court by the office of the solicitor general in respect to the amendments made by the Patriot Act of FISA[80] that although FISA was designed to direct and approve electronic surveillance conducted by domestic intelligence – therefore creating a warrant procedure for domestic surveillance activities – FISA need not necessarily have the ability to encroach on the president's constitutional power if a warrantless search was so approved[81] (Federal Reporter, 2002). This argument was based upon the 1979 case *Truong v. United States,* and its rationale departs from the AUMF since it unlike the AUMF which, while problematic is contained within a framework of war and the rules of war, *Truong* points to an inherent presidential capacity that places the president beyond oversight and beyond the law. In *Truong* a court of appeals upheld the submission of evidence obtained via a warrantless wiretap and microphone placed in the defendant's premises, indicating that such a search, as presented in the case granted by the attorney general – as the representative of the president – did not violate Fourth Amendment protections where *Truong* was charged with the information obtained, with passing intelligence information to the Republic of Vietnam (United States of America v. Truong Dinh Hung, 1979).

What is particular about the Truong ruling is that it did not outright[82] support the presidential authority and capacity to conduct warrantless searches, but provided four sets of criteria for

[80] As addressed earlier in the chapter, the amendment made to FISA by the Patriot Act changed the language under which a FISA warrant can be obtained to conduct electronic surveillance of an agent of a foreign power from a 'primary purpose' to a 'significant' purpose.

[81] This review based its rationale on a 1979 Fourth Circuit Court of Appeals case called *Truong v. United States.* Truong Dinh Hung or David Truong and one Ronald Humphrey were charged with passing classified U.S. information to the Socialist Republic of Vietnam. Once U.S. intelligence learned that Truong was passing classified material to Vietnamese representatives in Paris during the time of the 1977 U.S./Vietnam peace negotiations, Truong was placed under extensive warrantless surveillance. From May 1977 to January 1978 a wiretap was placed on Truong's home phone and a bug or hidden microphone was placed inside his residence. After gathering 268 days' worth of phone conversations and 255 days' of recorded audio from the bug, where it was ascertained that Humphrey, an employee of the U.S. Information Agency, and Truong were in fact working together to pass on classified material, both were arrested on January 31, 1978. Neither court authorization nor a warrant was obtained to conduct the surveillance.

[82] This notion of assertion is important in contradistinction to arguments presented by both Agamben and Yoo, who each argue from opposite perspectives – against the possibility of the unlimited exercise of sovereign power versus for the exercise of sovereign power – because it attempts to provide a rationale or grounding to presidential action in

such search. First, the Criteria of Flexibility: a clear distinction is made between foreign and domestic intelligence gathering, where the Fourth Circuit court argued that 'attempts to counter foreign threats to the national security require the utmost stealth, speed and accuracy' where a warrant requirement would 'add a procedural hurdle'. Second, a Foreign Policy Criteria: a link was made between the collection of foreign intelligence and the conduct of U.S. foreign policy where it was argued that the 'separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance' (United States of America v. Truong Dinh Hung, 1979); An Admissibility Criteria: here the Fourth Circuit made a clear distinction between the admissibility of evidence in the Truong case, distinguishing between evidence obtained during the warrantless period – understood by the court at an exercise in foreign surveillance/policy – and evidence obtained after the warrantless surveillance but prior to the arrest of Truong, where the DoJ obtained further evidence to support a criminal trial. This further evidence obtained after July 20, 1977, was held as non-admissible because it was gathered with the pretext of supporting a criminal trial, yet did not follow standards of probable cause determination that invoke, even for foreign nationals or agents of foreign powers, Fourth Amendment protections and therefore warrant procedure. Finally, a Primary Purpose Criteria: due to the concern for individual privacy rights, the distinction between foreign and domestic intelligence gathering, which allows for an exception of warrantless search in the case of the former, must be carefully considered and/or supported – that is, search should be limited only to agents of foreign powers and their collaborators, and where 'subtle judgment' is required 'about military and foreign affairs' – if a foreign link cannot be made, then the 'executive's needs become less compelling'[83] (United States of America v. Truong Dinh Hung, 1979). What this 1979 ruling shows, based on these four criteria, is that the rationale governing the collection of foreign intelligence, while made possible by and under the direction of the executive branch, is understood to be an expression of foreign

respect to search that does not occupy, or occupies less of a metaphysical orientation. This means that Agamben bases his arguments of sovereignty on the dichotomy articulated by Schmitt and Benjamin, in opposition to one another. For Schmitt, sovereign capacity is based on the creation of a 'state of exception' (SoE) or a space of sovereign action that prescribed by law, but is without law. This SoE, however, is viewed by Agamben, but in the first instance by Benjamin as a site of violence – there are no longer any restraints on executive action since the law has become unbounded – whereby the only way to counteract this site of sovereign violence is through the violence found in revolution. Both Schmitt and Benjamin, it can be argued, take a metaphysical position in respect to sovereign violence – where Agamben carries this forward – in the sense that there is an assumption that when sovereign power is actualized it results in the issuance of *only* pure violence – i.e., the exercise of state power where on the horizon looms the spectre of death. However, what are not considered are the other forms of social, institutional, economic or constitutional practise in which sovereign power is shaped and or constrained even in respect to the SoE. This point is argued by Rose and Rabinow in respect to the concept of 'biopower' as it applies to the life sciences, where biopower is viewed – if it can be understood from the perspective of governmentality – as an individuating and individualizing strategy even as it aims to intervene on a collective. In short, it is not a totalizing strategy. If we return to the concept of SoE, this is not to say that abuses or the arbitrary exercise of power cannot take place in a space that is not bounded by law. On the contrary, these abuses may and in fact do happen and need to be guarded against. However, sovereign action or, in this case, presidential capacity can be seen not as a metaphysical quality, but, rather, as something with a set of limits and rationales that if they must be curtailed, need to be charted and addressed as such.

[83] A supporting statement from *Truong*: 'Because the Fourth Amendment warrant requirement is a critical constitutional protection of individual privacy, this discussion should conclude by underscoring the limited nature of this foreign intelligence exception to the warrant requirement which we recognize in the instant case. The exception applies only to foreign powers, their agents, and their collaborators. Moreover, even these actors receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution. Thus, the executive can proceed without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers or their assistants. We think that the unique role of the executive in foreign affairs and the separation of powers will not permit this court to allow the executive less on the facts of this case, but we also are convinced that the Fourth Amendment will not permit us to grant the executive branch more'. 629 F. 2d 908 - United States v. Truong Dinh Hung.

policy and not in the first instance concerned with establishing procedures to support a criminal case.

This first point, of the act of intelligence collection as a tool of foreign policy as well as the ability for the president to authorise warrantless electronic surveillance, was seized upon and put forward in the 2002 FISA court review – this view was subsequently rebuked by Congress in its substantive review of the data-mining practises that took place at AT&T and Verizon. This review suggested that the president was not constitutionally bound by FISA, as *Truong* had shown, given special interests, in this case a situation of national security (Federal Reporter, 2002). What this report did contest, however, was the distinction drawn between foreign intelligence gathering activities and criminal prosecution, arguing instead that the government's foreign policy interests do not diminish when a foreign intelligence operation turns into a criminal trial; on the contrary, the criminal trial itself becomes a tool of foreign policy in respect to the capture or intervention upon an agent of a foreign power (Federal Reporter, 2002). While this argument was directed at what has already been addressed, the erection of the 'wall' between intelligence and law enforcement in respect to the sharing foreign intelligence information, it was used to inform, along with the argument concerning executive power, the rationale behind the NSA warrantless wiretapping of AT&T and Verizon.

As mentioned previously, in 2005 the uncovering of the NSA programme by the New York Times did in fact lead to a congressional backlash in respect to the encroachment of executive power on civil liberties.[84] Here the civil liberties in question were not necessarily those afforded to foreign nationals, but, rather, U.S. persons along with the corporations that assisted the NSA. A point that was contested in congressional analysis of the legal basis of the NSA programme was presidential authority as argued by Attorney General Gonzales and, more particularly, the ability of the executive branch, as argued in the 2002 OLA report, to side-step the FISA warrant process. The congressional reply to this assertion by the OLA, although not an official legal ruling, suggested that the basis sought by the OLA in *Truong* did 'not seem to be as well-grounded as tenor of letter suggests' given that *Truong* was ruled on, prior to the enactment of FISA (Bazan & Elsea, 2006). Here attorneys Bazan and Elsea argued that, while a lower court may have taken for granted the president's inherent authority, it is likely that the definition used by the NSA in their approach to electronic surveillance was the same as that used in FISA – implying that FISA should apply to FISA in this case – and that while the courts had generally accepted the role of the president to conduct domestic surveillance, nowhere have courts ruled against congressional oversight in that matter, implying that executive privilege in and of itself does not have the straightforward ability to push away oversight as part of the separation of powers (Bazan & Elsea, 2006). Furthermore, it was ruled as recently as 2010 that the activity of warrantless search by the

[84] Congressional opposition on civil libertarian grounds can also be seen to apply to a number of other domestic intelligence programs, such as the Total Information Awareness system, the Computer Assisted Passenger Pre-Screening System (CAPPSII) and the first version tabled of another passenger pre-screening system called Secure Flight.

NSA, where evidence was obtained outside of the FISA process put forward to the DoJ for prosecution, was in fact illegal (Al-Haramain Islamic Foundation et al v Bush, 2010). The basis for the ruling, by Judge Vaughn Walker of the California Northern District Court, was much like the congressional response to the OLA report, that the electronic surveillance – in this specific instance, of an Islamic charity in Oregon – required a warrant as part of FISA to be lawful – although it could be argued in the style of Bazan and Elsea that this ruling of illegality was made by a lower court and therefore cannot be considered definitive.

This example shows that while there has been an effort to establish domestic practises of non-particularised search under the directive of presidential authority, these efforts have been curtailed. First, presidential authority does not grant or allow for the practise of electronic surveillance outside of the FISA process or, in the event that presidential activity strays outside of this framework, it is heavily contested. Second, the practise of accessing mass telecommunications databases belonging to U.S. persons and corporations, even if the end goal is to identify particular terrorist patterns, is a potential infringement upon the Fourth Amendment and its protections. What this example does show, however, and this is consistent with Yoo, the 2002 OLA report and *Truong*, is that intelligence-gathering activities directed at foreign agents, even if conducted within a domestic context or at the border, are in fact not only an expression of U.S. counter-terrorist policy, but, more precisely, an expression of its foreign policy. Although the distinction in respect to the applicability of law between U.S. persons and foreign nationals is ambiguous – many constitutional protections remain valid and in place as applied to both nationals and non-nationals alike within a domestic civil and criminal law context – it does, in fact, direct this expression of foreign policy that is enacted by domestic intelligence agencies away from a purely domestic context and into the border region. This notion of an expression of foreign policy also directs sociological analysis to the space described by Agamben as no longer codified by law. This expression of foreign policy evident with intelligence-gathering efforts, then, can be seen in respect to the collection of PNR data, where unlike the NSA surveillance of AT&T and Verizon that activated internal domestic constitutional controls to bracket electronic surveillance, the ability for U.S. immigration and intelligence to collect PNR and biometrics from foreign nationals has not been hampered by any such internal or constitutional protections. Rather, the boundaries placed on search of foreign nationals, where they exist, have been shaped by external political and diplomatic pressure primarily by the European Union. As a result, this border zone that is responsible for the inflow of foreign nationals into the United States allows for a greater flexibility in respect to the actions taken to screen and search foreign national data in an effort to identity and prevent terrorism. The example of the political practises carried out by U.S. domestic and border security within this zone is the subject matter of Chapters 5, 6 and 7; however, what we are concerned with here is a further understanding of the parameters of the space or field that have resulted in the emergence of a new form of statecraft, one that is focused on the collection and analysis of identity data for the purposes of counter-terrorism.

4.4 PNR and Trans-National Data Flows

In 2001 after the 9/11 attacks, the U.S. government passed the Aviation and Transportation Security Act (ATSA 2001), creating the requirement for the DHS and within it the Customs and Border Patrol (CBP), to collect and analyse passenger and crew manifests of foreign flights entering the United States. What is described as a manifest was not limited to the name and passport information of crew and passengers travelling to the United States but also included PNR data that included commercial and personal information produced in the ticket purchase and check-in process. This addition of PNR was a significant change from obtaining Advanced Passenger Information (APIS) – passport, flight number, nationality/visa category, name – that has come to be the standard for identity verification at most international ports of entry since the 1980s (Lords, 2007). Although ATSA provided the legislative framework for the DHS to obtain PNR data from non-U.S.-based commercial airliners, it did not outline any of the procedures surrounding how the data would be captured or how it would be used in order to evaluate risk. This further definition of what constituted the PNR data-set was elaborated internationally through U.S. foreign policy and diplomacy initiatives. In 2003 the United States engaged the European Union in order to draft a temporary agreement for the exchange of PNR data between E.U.-based carriers and U.S. security services – the CBP to be passed onto the DHS and FBI. This effort was pursued under the threat of sanctions of a $1,000 per-passenger, per-flight fine, on any foreign carrier travelling to the United States after the negotiation period for the agreement had expired. The European Commission (EC), however, expressed initial reluctance to engage with U.S. demands[85] due to the potential violation of Directive 95/46/EC Article (1) and (7), which governs the transfer of 'community' data – data processed within the E.U. for commercial purposes – to a third party unless an adequate level of data protection and security are provided (Council of European Union, 2007). However, since the EC did not see a way out of the negotiations, they worked proactively to craft the PNR agreement within the general framework of European data protection and privacy legislation, ultimately with a longer-term vision of using the legislation to create their own counter-terrorism efforts.

This negotiation resulted in a 3.5-year agreement between the E.U. and U.S. on the grounds that U.S. authorities had to meet a set of conditions. First, to limit the data-retention period, or the period that data obtained on foreign nationals through the PNR transfer process would be stored from 50 years to 3.5 years – the duration of the agreement itself. Second, to limit the number of PNR fields transferred from the maximum 60 data points or predicates on the individual to 34. Third, from this list of 34 data points, to delete any items that provided information concerning an individual's race, religion, sex or medical life and prove discriminatory, therefore in compliance with another E.U. Data Protection Directive 95/46/EC, Article 8. And, finally, for the DHS/CBP to draft a set of 'undertakings' that would give assurances, although not legally binding, of fair data use and privacy protections of

[85] Liberal MPs, privacy advocates and the European Data Commissioner's office also viewed the transfer of PNR data as extra-juridical and a political affront.

European data. This negotiation also produced a set of policy intentions beyond a 3.5-year agreement period in order to allow for a review of the efficiency of the programme, to change the type of data transfer from 'pull' to 'push' and to create reciprocal data exchange – that is, for PNR data to be sent to E.U. security on flights originating within the United States. Up until the end of the 2003 agreement, the CBP was still be able to access foreign air carriers' flight reservation systems and 'pull' the data they sought from the 34 fields; that is, to manually connect to foreign air carriers' reservation systems and extract the PNR data. The agreement was finalised in May 2004 and provided the framework for trans-Atlantic data transfer to United States in order to identify and screen for possible terrorists and criminals. As of 2012, the use and collection of PNR by both U.S. and E.U. domestic security agencies have become central to counter-terrorism prevention measures.

In 2004, the processing of PNR data was written into the Intelligence Reform and Terrorism Prevention Act (IRTPA, 2004), where it was outlined that this data would be used for screening against watch lists that contained information on terrorists and criminals, and against secondary lists that contained information on stolen or fraudulent passports. This inclusion in the IRTPA was also bolstered by the 9/11 Commission, who identified PNR data as a key intelligence tool in their list of recommendations in the '9/11 Commission Report'. For the 9/11 Commission, passenger travel and the 'patterns' or predicate trail produced by the travellers entering and exiting the United States were seen as a rich source of data that could illuminate the travellers' immediate social network as well as provide insight into behaviour – the explicit use of this data will be addressed in Chapter 7. PNR was regarded as vital because a number of the 9/11 terrorists had repeatedly moved in and out of the country and were seen after the event to have been identifiable by U.S. intelligence (9/11 Commission, 2005). In 2007 testimony before the European Commission, DHS Secretary Michael Chertoff was also found repeating this claim in order to make the case for the 2007 PNR transfer agreement through the illustration:

> . . . two of the hijackers who appeared on a US watch list would have been identified when they bought their tickets. Three of the other hijackers used the same addresses as the two who we had on the watch list, so we would have been able to identify three additional hijackers. One of them, by the way was Mohammed Attah. A sixth hijacker used the same frequent flyer number as one of the other hijackers, so we would have identified him as well. Finally five other hijackers used the same phone number as Mohammed Attah, so we would have identified those five. With three simple analytic moves using this kind of data we would have identified 11 of 19 hijackers and stopped them from coming into the United States. (Chertoff, 2007, p. 4)
>
> Secretary Michael Chertoff, Department of Homeland Security

The 2004 agreement was short-lived, however. In May 2006 the European Court of Justice in Luxembourg struck it down on grounds that Directive 95/46/EC – the directive concerning data transfer to third countries – only applied to the transfer of community data for

community purposes. In this case, what was at issue was not the earlier concerns with 95/46/EC voiced by the EC to do with assurances of data protection and possible discrimination, but, rather, the categorical use of PNR data by U.S. authorities. That is, the European Court established that PNR data gathered by air carriers in the flight-registration process was commercial in nature and part of community data processing, as opposed to the collecting and processing of data for criminal justice purposes or matters of security. As a result, the court annulled the PNR transfer agreement, stating that 'the decision on adequacy – made by the EC – did not fall within the scope of the directive because it concerns processing of personal data that is excluded from the scope of the directive' (European Parliament v Council of the European Union, 2006). The court in this same decision reiterated its commitment to preventing terrorism and combating serious crime alongside their American counterparts and gave both parties 90 days to negotiate a new agreement that classed PNR data under a criminal-justice framework. This new transfer agreement between the United States and European Union was finalised in June 2007, roughly following the template of the 2004 agreement but differing in two crucial ways: it extended the retention of PNR data from 3.5 to 7 years, or the life-span of the new agreement, with an additional 8 years of retention added on to what was described as dormant data, and it reduced the number of data elements to be transferred to the U.S. CBP from 34 to 18 + 1, as a result of pressure from the EC. To contrast the 2007 agreement with the 2004 agreement, while the 2004 agreement provided a basis for the analysis of passenger information in real-time by U.S. border security, the 2007 agreement established a new basis for data retention and the use of PNR data for both real-time analysis and risk assessment, and according to a 15-year axis, both as a tool for the development of travel profiles and as a digital forensic.

From this chronology of the PNR transfer agreement debate and the issues of contention brought forward by the European Court, three points can be made that fit with the consideration of executive privilege in respect to data acquisition and non-particularised search: (i) PNR, while existing prior to 9/11 and as part of the standard airline-booking process, became viewed as a strategic asset that could potentially yield intelligence to identify of track foreign agents; (ii) unlike the analysis of the data-mining practises of AT&T and Verizon by the NSA, the collection and analysis of PNR data was deemed a permissible action by U.S. authorities because data collection was linked to foreign nationals and performed within the threshold of the border; (iii) while this practise had detractors, the collection of such data performed under the threat of monetary penalty shows that this data-collection practise is not merely an innovation, but, rather, an extension of U.S. foreign policy and political will onto an ally. The use of this data, whether PNR, passport information or biometrics, can then be seen to be the material through which an advanced liberal democracy such as the United States is able to not only assess the risk of individuals as they cross the border, but also have the ability to act on such risk decisions under the auspices of executive privilege.

4.5 Conclusion

How, then, can the field of post-9/11 border security be understood in light of the examples provided? Furthermore, how do these practises constitute a rationale of post-9/11 security in the context of legal precepts and foreign-policy determinations? It is instructive to return to the criteria established at the beginning of this text in order to evaluate: first, how intelligence gathering functions as an expression of war and/or the exercise of executive power; second, how this form of intelligence gathering can reveal the emergence of a new law-enforcement rationale in respect to non-particularised search; and third, what, if any, distinction can be made between U.S. citizens and foreign nationals regarding this form of intelligence practise which has its fullest expression at the border?

If the argument is that post-9/11 domestic intelligence operates under a set of principles unbounded by congressional oversight or legal constraint, the answer to this is both true and false. True in the sense that specific initiatives such as the NSA wiretapping case provide an example of what Agamben describes as the 'state of exception'. However, what is important to note is that despite this action taken by the executive branch and advocated by scholars such as Yoo, considerable opposition has been mounted, where executive action, outside of a separation of powers framework – if not substantiated legally, then at least supervised by Congress – has taken place. In the case of the NSA programme, this opposition has occurred in respect to both curbing executive powers and enforcing constitutional norms and protections. To answer 'false' to this question, we simply have to refer to the example of the use of the law by domestic intelligence and the DoJ as a tool against terrorism. Here law has not been done away with, but, rather, it has been amplified, allowing marginal statutes applying primarily to immigration law – therefore requiring less of an evidentiary standard to enforce, as argued by Ericsson – to become a significant counter-terrorist tool with a direct link to border practises; that is, the control of immigration and the flow of foreign nationals in and out of the country. However, despite the dual character of the application of law and executive privilege in the context of counter-terrorism, one dominant rationale emerges, consistent with the arguments of Yoo and the OLA: that intelligence gathering with the aim of either intervening on a rapidly unfolding situation is an expression of foreign policy. Intelligence gathering in this manner becomes a tool to address both a political situation – preventing a suicide bomber from boarding a plane – rather than a tool strictly codified by law.

It can also be seen from all three examples that an overall approach to domestic counter-terrorism has been to perform non-particularised search in order to enable law enforcement to pinpoint particular terrorist threats. Although the technical forms of data-mining and analysis used in the context of border security will be described in greater detail, what is evident is that while non-particularised search can be seen as the generalised form of domestic-intelligence practise, it has been directed most explicitly as a foreign policy tool towards the border region. This form of governance can be seen to be the result of

constitutional protections that prevent mass or non-particularised search of U.S. persons to take place. As a result, the form of mass search or, in the case of PNR, mass screening can be seen to find its greatest expression at the border and in the context of the immigration system where foreign nationals, despite diplomatic arrangements with home countries, do not have the same legal standing as U.S. citizens. Although this point seems to be an obvious one, it is nonetheless important since it forms the direction and field through which this new form of security, if not statecraft, can take place.

Finally, the distinction between U.S. National and Foreign National: As has been emphasised, the distinction between national and foreign national is what has enabled a new procedural field to emerge in respect to U.S. domestic intelligence and law enforcement. The procedural field allows for a more flexible data collection, sharing and analysis environment and is informed by a policy orientation of prevention. However, despite this distinction, protections still remain in place for foreign nationals such as those surrounding due process, in the event that an individual is charged with a crime. What has become apparent, however, in respect to intelligence gathering or data collection, as in the case of PNR, is that this data can be used by U.S. security for either a political or legal purpose: political, such as described in Chapter 7, concerned with the use of terror watch-lists, where individuals can be denied entry to the country, but not arrested, if they are deemed a terror risk by U.S. security. Legal, in the sense that immigration, PNR or biometric data collected can be used to open a legal case if such a case is warranted. This is the result not only of the dismantling of the ‘wall’ between domestic intelligence and law enforcement, but of the expression and application of foreign policy into this threshold space between national and non-national, domestic and foreign. This legal and policy ground introduced at the beginning of the chapter is what provides the permissions, limits and assumptions through which technological and institutional practise is carried out. This legal basis concerning search then informs the possibility of action taken by U.S. security services as well as reveals the rationales through which their behaviour is governed.

5. [LAYER 2] The Economics of Security: Visa Reform and Post-9/11 U.S. Border Security

5.1

As introduced in Chapter 1, post-9/11 U.S. border security has adopted a layered approach to counter-terrorism that has involved the securitisation of the U.S. immigration system; in particular, the system that manages approximately 30 million non-immigrant travellers entering the country each year. This layered approach, made possible by legislative changes designed to enable domestic intelligence and law enforcement to better track and monitor threats, has been oriented primarily around the screening of foreign nationals in respect to their identity predicates as they enter the U.S. immigration system. This form of screening is composed of three technological and institutional layers, each focused on the verification of individual identity and the assessment of risk for the purposes of counter-terrorism. The first institutional layer – layer 2 – involves the screening and securitisation of the non-immigrant visa process, student visa process and Visa Waiver Program (VWP). The remaining two layers, subjects of Chapters 6 and 7, focus on the analysis of fingerprint biometrics collected at the border as part of the US-VISIT programme and on the collection of PNR information. As was described in the previous chapter, each of these layers is supported by a legal framework that allows for the collection of such identity information.

What provides continuity to these three layers is the telescoping function that they perform. That is, each layer acts as a filter through which individual identity is analysed and assessed, moving from the macro to the micro level. In the case of the present layer focused on national affiliation and the mechanisms through which the visa process is administered, it has come to be the most politicised since as noted, the student and business visa process was directly exploited by the 9/11 hijackers as they developed their plot. As a result, in the immediate aftermath of 9/11 as well as in response to subsequent attempted airplane bombings – in 2004 with Richard Reid, known as the shoe bomber, and in 2010 as described with Umar Farok Abdulmutallab, known as the underwear bomber – there have been immediate defensive actions taken against larger subsets of the foreign national population entering and residing within the United States. For instance, in the immediate aftermath of 9/11 there were calls by U.S. politicians to place a moratorium on the issuance of all student visas through the country – instead, a new programme was created to monitor and track student enrolment called SEVIS. Likewise, in the aftermath of the two attempted plane bombings as mentioned, for a brief period all nationals from countries deemed as state sponsors of terrorism were banned from flying to the U.S. with or without a valid visa to do so. Further complicating this security picture was the acknowledgement that several of the hijackers not only exploited the visa programme by posing as legitimate students or business travellers, but they were granted visas on grounds of good-standing since they were classified as ‘third country nationals’. These nationals were citizens from northern Africa and the Middle East but had gained residency permits within Europe that enabled them to benefit from accommodating diplomatic relations between the U.S. and Western Europe.

These examples raise two questions to be addressed in this chapter. First, what new modes of security have been applied to the U.S. visa programme inclusive to student and business visa categories, and how have they reshaped U.S. border security? Second, despite the political pressure to close the U.S. border to large subsets of the travelling population, at least temporarily, U.S. borders remained open after 9/11 and have, in fact become less stringent to the nations whose nationals were involved in 9/11; why is this? It will be argued in the first instance that the approach to the securitisation of the visa issuance process in respect to student visas at foreign Consular offices has been to create a new database infrastructure where each enrolled individual undergoes a process of identity verification in order to reduce identity fraud as well as matching against terrorist watch-lists. While these systems can be seen to create a new inclusive relationship in respect to those who are deemed low-risk and able to enter the United States and those that are denied visas, these networked systems are found to have delays and errors in processing that lead to inconsistent visa administration practises and renewed vulnerabilities. Second, it will be argued that the most significant driver for keeping U.S. borders open despite a threat that is 'catastrophic' and 'generational' is not an appeal to liberty, as many civil libertarian critics have proposed – where the conceptual battle post-9/11 is the dichotomy of liberty versus security – but, rather, due to economic pressures concerning trade relationships, business and tourism that require the U.S. to engage and in fact lead the global liberal economy.

5.2 The Visa Process Pre-9/11

Despite the attention given to the U.S. immigration system by congressional leaders, intelligence and law enforcement as a direct consequence of 9/11, it would be inaccurate to assume that the U.S. immigration system was wholly devoid of its own longstanding and pre-established forms of individuation, population management and control. Theorists Bigo and Guild points out that in its current form, terrorism aside, the European Union as a basic mechanism for the operation of its immigration system divides individuals into four categories: (i) those individuals who belong to member states and have the right to enter and reside within the territory of any other member state; (ii) nationals whose home countries have a privileged relationship with the E.U., such as Switzerland and Iceland that allow those nationals to enjoy equal economic rights; (iii) favoured countries that appear on a 'white' list and do not require a visa to enter the E.U. – such as non-European VWP countries; and (iv) those countries that are placed on a 'black list' and whose nationals must obtain visas before entrance is granted (Bigo & Guild, 2005, p. 239). This type of categorisation can also be seen within an American context, where since the establishment of the Visa Waiver Program in 1986, U.S. immigration divided foreign national populations into three categories: (i) Visa Waiver Program nationals or nationals from 36 nations whose citizens are able to travel to the United States for up to 90 days without first obtaining a visa; (ii) nationals who do not belong to the VWP and therefore are required to obtain a visa from a U.S. consular office in their host country prior to entrance; and (iii) those nations designated as 'state sponsors of terrorism', whose nationals face additional scrutiny and sanction when applying for a U.S.

visa. Furthermore, in respect to U.S. immigration practises, nations whose citizens must apply for visas to enter the U.S. are also subject to additional screening based on interests of U.S. foreign policy. For instance, out of the approximately 25 nations subject to 'non-terrorism-related' clearances, a list that includes countries such as Angola, Armenia, China and Pakistan, each can be seen to be coded with a set of interests and concerns that range from Treasury Department violations (Angola) to a concern over the dissemination of intellectual property and educational resources related to the development of American military technology obtained by students studying in certain programmes at U.S. universities (China), to those individuals entering the United States in order to advance domestic nuclear programmes (Pakistan) (Ford, 2002). This same form of coding also applies to those nations who within a pre-9/11 context were viewed as 'state sponsors of terrorism' or as 'countries subject to terrorism-related clearances' (Afghanistan, Cuba, Iran, Iraq, Libya, North Korea and Russia). While the political cleavages of American foreign policy over the last 30 years can be seen as apparent in this list countries on this list such as Afghanistan and Russia represent more recent political concerns. Afghanistan can be seen to be coded to identify members of the Taliban leadership, senior military leaders or even individuals conducting business on part of the Taliban; Russia is coded not only in respect to lingering Cold War sentiment, but also due to internal turmoil surrounding the Russian war in Chechnya that began in 1994. What is compelling about these examples is that they display a pre-existing policy and institutional layer that was adjusted towards U.S. foreign policy interests and concerns. The question, then, to ask is: From this pre-existing visa framework, what did the 9/11 hijackers exploit, and subsequently what has changed? How has this security layer been transformed?

As presented in Chapter 1, congressional scrutiny into the missed opportunities that led to 9/11 concerned the failures of the intelligence community to share information between domestic (FBI) and international (CIA) agencies in order 'connect the dots', as well as with the day-to-day operations and due diligence of U.S. customs and consular services. Although this material has already been addressed in general, it is important to review the specific material details pertaining to the processing and facilitation of 23 non-resident visas – student and business visas – that were given to the 19 9/11 hijackers. Much in the way that particular countries are viewed or filtered according to a pre-established set of criteria, U.S. consular services and immigration officials pre-9/11 primarily relied on guidance established in 1952, and subsequently updated in 1996, in the Immigration and Nationality Act (INA), sections 212–222[86] when reviewing visa applications (Ford, 2002) (Immigration and Nationality Act, 1996). While sections 212–222 can be seen to contain broad and multiple criteria through which a visa applicant could be denied – heath, criminality, terrorist activities,

[86] These sections are titled: 212 general classes of aliens ineligible to receive visas and ineligible for admission; waivers of inadmissibility; 213 admission of certain aliens on giving bond; 213A requirements for sponsor's affidavit of support; 214 admission of nonimmigrants; 215 travel documentation of aliens and citizens; 216 conditional, permanent resident status for certain alien spouses and sons and daughters; 216A conditional permanent resident status for certain alien entrepreneurs, spouses, and children; 217 visa waiver pilot program for certain visitors; 218 admission of temporary h-2a workers; 221 issuance of visas; 222 applications for visas.

past immigration violations and/or misrepresentation – the main application of the INA by consular officers pre-9/11 was section 214(b); failure to establish non-immigrant status – that is, consular officers when reviewing visa application or conducting interviews sought to determine foremost whether or not the person intended to stay in the United States beyond the intended duration of the visa or that he or she lacked sufficient funds to return to his or her home country.[87] For instance, during the 2000 fiscal year, approximately 2 million visa applications were refused. Out of these, 79.8% were refused as a result of 214(b) failure to establish non-immigrant status; the threat of terrorism, 212(a)(3)(B) only accounted for 99 total visa rejections; 471,523 or 24% were refused for violating INA 221(g), failure to provide appropriate documentation for visa adjudication.[88] This is a telling fact since it supports the challenge made to social science theories of disparity that have been argued are causal supports for terrorism. What is known of the 9/11 terrorists was that each came from more or less middle class backgrounds and even Osama Bin Laden came from a position of extreme privilege. This then implies that the 9/11 hijackers were able to present themselves not only with legitimate business or academic aims, but also with financial support to be able to pass through the dominant immigration filter.

Beyond this set of criteria, consular officers are also required to screen the name of each visa applicant against the Consular Lookout and Support System (CLASS) database that until 9/11 held approximately 6.1 million records, primarily consisting of individuals who had been previously denied visas.[89] Although consular officers were provided with stringent parameters for visa adjudication as well as further vetting capability in terms of CLASS name checks in order to prevent potentially threatening individuals from coming to the United States, the 'culture' of the consular visa process pre-9/11 did not take on the foreign policy concerns of the United States as their primary focus. Instead, the U.S. consular service was encouraged to expedite visa applications not only in order to facilitate travel and trade, but to promote free movement and even cultural exchange while adhering to the conditions set out by the INA. This push towards greater openness had several unintended consequences. Between 1998 and 2001, worldwide visa applications to the U.S. rose 28% from 7.7 million to 10.6 million per year, resulting in staff shortages, burn-out and longer wait times to receive a decision of visa admissibility (Ford, 2006). What is interesting to note is that the number of visa applications has continued to grow after 9/11, and in 2008, even after the creation of more stringent visa guidelines, U.S. consular offices processed some 15 million applications. As a result, it was found that U.S. consular services turned to the State Department's 'Consular Best Practises' handbook, which provided the ability for consular staff to streamline the visa process by waiving the mandatory interview required for each visa applicant if the applicant could be determined as a non-immigration risk, making it possible

[88] This is an important point, because it will be shown in the following paragraph that despite the high number of rejected visa applications due to the provision of insufficient documentation, a number of the 9/11 hijackers who obtained their visas from U.S. consulates in Saudi Arabia did not properly fill out their visa applications, nor were they required to be interviewed as part of the visa process.

[89] Apart from the 6.1 million records, primarily containing names of individuals who had been denied a U.S. visa, CLASS contained approximately 48,000 names from State Department interagency databases, as well as 7,000 names of individuals who were to be denied visas on terrorist-related grounds.

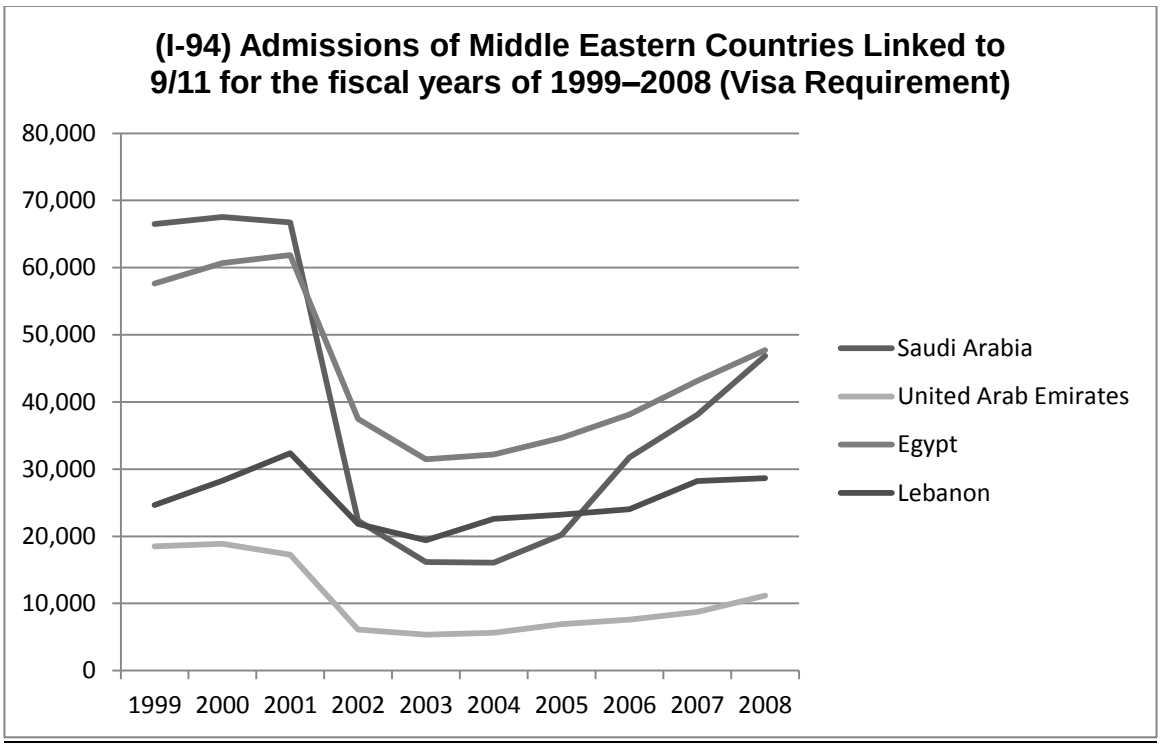
for visa applicants to use third parties such as travel agents to make applications on their behalf (Ford, 2002). This economic emphasis of the visa process also led to the creation of a referral process through which pressure was placed on consular officers to process visas of nationals who had some ties or relationship with members of Congress or other political figures. For instance, consular officers working out of Cairo received 202 congressional inquiries during 2001, each following the denial of a particular visa application (Ford, 2002). Turning to 9/11, the liberalisation of the visa process can be seen to have impacted the visa adjudication decisions in respect to the 19 hijackers. For instance, at consular posts in Saudi Arabia, where 13 of the 19 hijackers came from, and the United Arab Emirates, where a further two hijackers resided, consular officers operated under a policy of routinely waiving visa interviews based on the understanding that Saudi and Emirati nationals did not present an immigration risk. Although interviews took place if the name of an applicant appeared on the CLASS database, less than 3% of all applicants to the Riyadh embassy were required to conduct an interview and less than 1% of applications were refused. Out of the 18 visa applications applied for and granted to the 15 Saudi/UAE hijackers, none of the applications had been properly filled out. Furthermore, returning to the problem of data sharing between the State Department, intelligence and consular services, while the name of each applicant was checked against the CLASS database, CLASS did not contain vital information received by the State Department from the intelligence community in late August 2001 that could have identified two applications by 9/11 hijackers.

The U.S. security response to both these procedural and data-sharing lapses rested very much within a Foucaultian framework of securitisation or 'limiting bandwidth', where limiting bandwidth is understood as a security procedure through which unwanted events are adjusted according to an economic rationale to an acceptable set of limits (Foucault, 2007). Here consular officers wilfully accommodated the potential of the unwanted event of illegal immigration since it fit with the prevailing economic rationale of visa processing. This mode of liberalisation, alongside the general dimensions of foreign and military policy carried out by the U.S. government, which viewed the terrorist threat as originating in the remote corners of the world, led U.S. homeland security policy to focus upon and seize the visa process as a site of security intervention. This scrutiny focused not only on the fact that the consular process lacked either legislative guidelines or an institutional mandate, placing a greater security emphasis on identifying terrorist risks, but also on the specific visa categories through which the hijackers were able to enter the United States and the resulting violations, such as visa overstay. For instance, Ziad Jarrah, the hijacker who piloted United Airlines Flight 93 which crashed outside of Shanksville, Pennsylvania, entered the United States on a valid B-1/B-2 (tourist/business) visa obtained in Berlin on May 25, 2000 (Eldridge, et al., 2004). Shortly after arriving in the United States, Jarrah enrolled in the Florida Flight Training School without changing his immigrant status to 'student', violating his immigration status. To this effect, the 9/11 Commission pointed out that '[t]his failure to maintain legal immigration status provided solid legal basis to deny him entry on each of the six subsequent occasions he entered the United States. But because there was no student

tracking system in place and because neither Jarrah nor the school complied with the law's legal notification requirements, immigration inspectors could not have known of his status' (Eldridge, et al., 2004, p. 12).

The consequence of the securitisation of the visa system applied immediately following 9/11 resulted in three subsequent actions: (i) the State Department changed the policy of a flexible interview process for visa applicants to require interviews from all applicants prior to visa approval and introduced more stringent vetting techniques as well as evidentiary criteria for applicants to demonstrate the legitimacy of their applications; (ii) in 2002 the DHS created the Student and Exchange Visitor Program (SEVP) to monitor the enrolment status of all international students studying in the United States; and (iii) the DHS strengthened the identity-credentialing process as it applied to the VWP by requiring all VWP nationals to obtain tamper-resistant, machine-readable passports, initially by October 26, 2004 – a date that was subsequently extended to 2005 (DHS, 2002). Although the details and implications of each of these initiatives will be addressed over the following pages – in particular, in relation to how each initiative has worked to create new categories of individuals that can be monitored and intervened on in respect to counter-terror practises reliant upon the analysis of identity data – the securitisation of the U.S. visa and immigration system can be seen to have created a fundamental dilemma in U.S. homeland and border security. That is, a dilemma not necessarily between liberty and security, but between economy and security; or, rather, how to keep U.S. borders open as part of a broad policy towards economic liberalisation while ensuring protection of the homeland from terrorism (Eldridge, et al., 2004).

Figure 5.2.1: Visa Approvals from Countries whose Nationals Were Involved in 9/11



(Hoefer, 2009)

Figure 5.2.1 represents the number of I-94[90] admissions from 1999–2008 from the non-VWP countries – countries whose nationals are required to obtain a visa before entering the United States. What is apparent from this graph is that out of the countries whose nationals were involved in 9/11, Saudi Arabia has seen the greatest decrease in the numbers of visas issued to the U.S., from a high of approximately 68,000 to fewer than 20,000 in 2003 and 2004. This decrease can be attributed to four initiatives at U.S. consular offices in Riyadh and Jeddah: (i) the requirement for all visa applicants to present themselves to consular officers for an interview in order to determine admissibility; (ii) the requirement for all visa applications to be properly filled out; (iii) the barring of third parties from submitting visa applications on behalf of the applicant; and (iv) the bolstering of the CLASS name-check process to match names not only against an expanded watch-list – containing names from U.S. criminal and intelligence lookout databases. A fifth change in security was also applied to this process, whereby phonetic name matching was performed on each visa application against a terrorist watch-list. Additionally, this decrease in visa applications from each of these nations can also be seen as part of a broader trend post-9/11 of a decline in visa applications. For instance, while the number of visa applications declined by 16% worldwide, applications declined by 50% in the UAE immediately following 9/11 (Ford, 2002). It is unknown whether or not this decline resulted from fear of further terror attacks in the U.S. where the U.S. could be viewed as a threatening location, or perceived fears by residents of the UAE who felt that because the U.S. was attacked by an Islamist group there would be an internal bias against these residents.

5.3 The Visa Process Post-9/11

The securitisation of the U.S. immigration system in respect to visa and passport management as a result has focussed upon several changes in respect to the adjudication of visas by consular services, primarily with the introduction of additional vetting procedures and the establishment of the SEVIS. The DHS also instituted, although perhaps less importantly, new requirements for all VWP country nationals to upgrade their passports to machine-readable ePassports under the threat of sanction. These practises can be seen to establish a new set of routines and procedures that seek to persistently verify and vet individual identity – the identity of the visa holder – against a host of anti-terror databases and watch lists, and to monitor those who have been identified that have entered the country in respect to their validity and standing. The instantiation of these routines of identification can be seen as creating new kinds of subjects to be monitored and intervened on in respect to their identity predicates – in this case, the terms of their visa, the evidence presented in order to get a visa and the appearance or non-appearance of information of interest housed within U.S. counter-terror databases. It also establishes a new set of standards for travel illustrated by the introduction of such things as RFID chips placed within the passport containing unique identifiers and, due to greater interconnection of consular and intelligence databases, making individual identity more regular and traceable. As discussed in the

[90] The I-94 record is the best way to calculate admissions into the U.S. by non-nationals, since all foreign nationals – those belonging to the VWP and those not – are required to fill out an I-94 and pass it to U.S. immigration on arrival to the U.S. I-94 forms contain name, passport, nationality and residence information.

previous chapter, these procedures further coincide with the use of immigration infractions as a counter-terrorist tool. With the creation of more standardised and secure documents that can signify duration of stay and overstay, these infractions can be more easily determined and acted on. Similar to the analysis of PNR or the capture of biometrics, the general counter-terrorist practise involving the analysis of visas and passports also incorporates aspects of prevention in respect to identity predicates, based on policy motivations oriented towards the protection of the U.S. from terror. However, this move towards greater vetting and modes of prevention through new technological means of identity verification can been seen not only to create new methods of enforcement, but as a result of more detailed vetting procedures informed by the understanding of terrorism as catastrophic risk. These new vetting procedures, while enhancing the informational awareness of consular officials and U.S. immigration, are also seen as subject to lead to institutional or endogenous inefficiencies or barriers, where the technology used to fashion new security insights can also prove to be problematic.

Immediately following 9/11, the State Department changed the procedures under which visas were to be vetted abroad at U.S. consular offices and embassies in order to more greatly rely upon the intelligence resources located within the United States. Procedurally, this change of policy resulted in what was called the 30-day 'visa condor' procedure, where all new visa applications from males aged 16 to 45 were to be placed on hold for up to 30 days to be screened by the FBI and CIA (Ford, 2002). Along with the provision of the visa condor, the same male applicants were required to provide additional evidence concerning their travel and educational history, employment record and whether they had ever served in the military. This additional screening was meant not only to provide a topical assessment of a terrorist threat to determine whether or not a visa should be granted, but also to provide leads and connections pertaining to terrorist cases launched by the FBI. As a result, this vetting process created a considerable backlog as well as a procedural error in respect to visa issuance; namely, consular officers were instructed to approve any visa application in question if the 30-day period had expired without a response from the FBI. Although this loophole was eventually corrected, it did lead to a further set of security lapses reminiscent of those that were involved in 9/11 – for instance, communications on 200 visas that had been rejected were sent to U.S. consular officers after the 30-day period had expired and visas subsequently issued (Ford, 2002).

Beyond these inefficiencies, there was also an internal conflict between the State Department (the department responsible for oversight of the consular services) and the Department of Justice (the department responsible for the prosecution of criminal cases on behalf of the U.S. government) over the threshold of evidence required to deny a visa. Immediately following 9/11 the State Department, working with the FBI, increased the number of records within the Consular Lookout and Support System (CLASS) database from some 6.1 to approximately 12 million through the incorporation of terror and criminal files

from numerous federal databases.[91] Along with the addition of files, CLASS began to use loose name-matching algorithms – these algorithms will be addressed in Chapter 7 – in order to match both Arabic and Slavic names entered into the system against those contained in the database. The result of the use of the visa condor process as well as the loose name matching against CLASS, however, created a conflict between the State Department and the DoJ, who could not come to agreement over how to interpret INA 212(a)(3)(B)[92] pertaining to terrorism. For the Justice Department this inadmissibility clause on grounds of 'terrorist activities' could be triggered according to a very low threshold of evidence, for instance, with a 'possible' name match against CLASS or during the visa condor. The State Department had a differing view, however, contesting that a clear link to terrorism, rather than merely a name association, should determine inadmissibility; for instance, the problem with name matching, let alone loose name matching, is that it does not correct for names that are either misspelled or are duplicates. Although this resulted in approximately 587 visa applications that were deemed inadmissible by the DoJ being disputed by the State Department, it also reveals the emergence of a rationale of precaution that can be seen to extend beyond the visa-issuance process into most aspects of 9/11 homeland and border-security practises, which seek to verify and substantiate the identity of foreign nationals and their status to travel to and remain within the country**.** This move to precaution can be seen to have unintended consequences – here in terms of institutional efficiency – in respect to the SEVP as well as the representation of counter-terrorism practise that is unable to overcome itself, a clear contrast to the notion of sovereign decision, as put forward by Agamben, that conceptualises a direct line to the distinction between life and death. To elaborate, while the lowering of the threshold for inadmissibility results in the ability for U.S. consular services to more easily deny the issuance of a visa, it also shows a form of sovereign power, that while active does not result in the arrest of these individuals deemed too risky to enter the U.S. While it does place the individual closer to U.S. intelligence, the identification and capture of individual terror suspects is only activated after detailed evidence is gathered, rather than speculation or computer error as a result of false positives incurred as part of loose name matching.

Student Exchange and Visitor Program (SEVP)

As part of the USA PATRIOT Act 2001, the Department of Homeland Security was mandated to create a programme by January 1, 2003, to enrol and monitor the approximately one million international and foreign exchange students present in the country. This programme, called the Student Exchange and Visitor Program (SEVP) and reliant upon the SEVIS[93] student database, was a second attempt – along with the creation of an entry/exit monitoring system of foreign nationals crossing U.S. borders – to create a student monitoring system first called for in 1996 as part of the Illegal Immigration Reform

[91] Records have been incorporated into CLASS from the National Crime Information Center (NCIC) database along with the FBI's database on Violent Gang and Terrorist Organizations.
[92] The provision within the Immigration and Nationality Act pertaining to 'Terrorist Activities' as an inadmissibility offence.
[93] Student and Exchange Visitor Information System.

and Immigrant Responsibility Act. The SEVP programme worked in much the same way as the requirement U.S. consular services placed on male visa applicants: it was a way to not only verify the physical identities and account for the exact number of foreign students in U.S. educational institutions – through interviews with those students by foreign student administrators – but to verify that approximately 7,300 U.S. colleges and universities were not accepting students without proper documentation as was the case with the 9/11 hijackers (Skinner, 2005) (DHS, 2002). U.S. post-secondary educational institutions were then required not only to enrol each foreign national into this programme, but to report to the DHS on five sets of criteria within 21 days: (i) if a student had failed to maintain the status of the programme; (ii) any change in the student's legal name or residential address within the United States; (iii) in the event of early graduation; (iv) any disciplinary action taken by the school in respect to crime; and (v) a response to any other notification request made by SEVP (DHS, 2002). It is evident from this set of criteria that SEVP seeks not only to take account of student enrolment, but to chart student behaviour through their course of study and the duration of their stay in the United States. What is also evident from this criteria of assessment is that not only has the securitisation of the student visa programme placed foreign students in closer proximity to intelligence, it has turned mundane disciplinary categories, typically enforced by educational institutions, into a matter of counter-terrorism. For instance, it presents scenarios where a gifted foreign student, say from Pakistan, who graduates with honours from a leading university and does so ahead of schedule, is potentially turned into a counter-terrorism matter, since this type of behaviour deviates from normal student behaviour.[94]

In order to further examine SEVP, it must be viewed within the context of the greater enforcement efforts applied to the visa programme – that is, the enforcement efforts that go along with not only SEVP but also US-VISIT and the NSEERS programme, which are designed, like SEVP, to monitor over time the visa status of individuals who are nationals of countries on the U.S. terror list. As part of the creation of the DHS, renewed emphasis was placed on the enforcement of visa and immigration violations to be carried out by the Immigration and Customs Enforcement (ICE) and its internal research department, the Compliance Enforcement Unit (CEU). It is important to understand that while SEVP was created in a direct response to the abuses of 9/11, it rests within and on top of a larger policy and institutional framework responsible for addressing visa overstays and illegal immigration. This twinning of policy motivations not only highlights the challenge of radical Islam or contemporary terrorism, which arrives in a generic form – the terror attempts of the last decade in the United States as well as in the United Kingdom and Spain have been made by individuals who disguised themselves as citizens[95] – but also places a wider range of governmental processes under the purview of counter-terror policies and practises. This shift in policy clearly signals the shift in respect to search that was identified in Chapter 4; namely, the belief that the nature of the terrorist threat, one that is both catastrophic yet disguised or

[94] An example of the problematic of student visa analysis will be presented in Chapter 7.
[95] For instance, the four perpetrators of the July 7, 2005, London Tube bombing were naturalized British citizens. Each was Muslim; three were of Pakistani descent and one was of Jamaican descent.

hidden within given population categories – student population, population of foreign nationals entering the United States or Europe – has brought about a move from particularised search, where law enforcement and intelligence have a clear idea of who they are interested in, to non-particularised search, the vetting of a population in the hopes that mundane visa or travel information can yield unexpected results, as well as the implementation of a policy practise of prevention and precaution.

Following the 9/11 terror attacks and with the understanding by the U.S. Congress that there were approximately three million illegal immigrants within the U.S. with a further projection that there would be an annual increase of 350,000 illegal immigrants entering the country each year – 35% of whom were considered 'visa overstays' – the DHS assigned ICE and the CEU to monitor and enforce the programme of SEVP, US-VISIT and NSEERS (Skinner, 2005). In respect to organisation structure, enforcement of visa overstays, visa revocations and the intervention of individuals on national security grounds is passed onto the CEU from each of the three programmes listed in the form of a 'lead'. Each lead is then vetted and investigated in order to determine its merits at the CEU, and if the CEU determines the lead to be actionable it is passed onto a further system called NAILS to be taken up by ICE agents in the field. The acting case agents are then given the responsibility to report back to the CEU every 30 days in order to communicate the outcome by indicating one of six reporting options: (i) the violator has been located and arrested; (ii) the violator has been located but found to be in compliance of immigration laws; (iii) the violator has adjusted his or her visa status and is not in compliance;[96] (iv) the violator has not been located but is presumed to have departed from the United States as verified through subsequent investigation; (v) the violator has not been located but is being addressed by another field office within ICE; and (vi) ICE has exhausted all leads and has not located the violator (Skinner, 2005). Although this organisational structure displays a narrow form of efficiency in respect to the monitoring and enforcement of immigration violations, it can also be a seen as a system that has been overwhelmed by the very leads it is supposed to take up. Therefore, we can return not only to the concept of 'predicate triage' but also to the problematic of maintaining open borders that facilitate the American economy during a time of extreme uncertainty. For instance, from 2004–05 it was reported by the DHS Inspector General that the CEU had received 301,046 leads from SEVP, US-VISIT, NSEERS and the State Department. Out of this amount, 96% of the leads proved to be invalid, with only 671 leading to apprehensions – although a marginal number of those individuals located and detained were deported from the country (Skinner, 2005).

The reason for this extreme discrepancy between the number of leads generated versus the number of apprehensions is twofold: (i) as with the visa condor process described previously, the CEU simply could not process the number of leads provided to its office in a

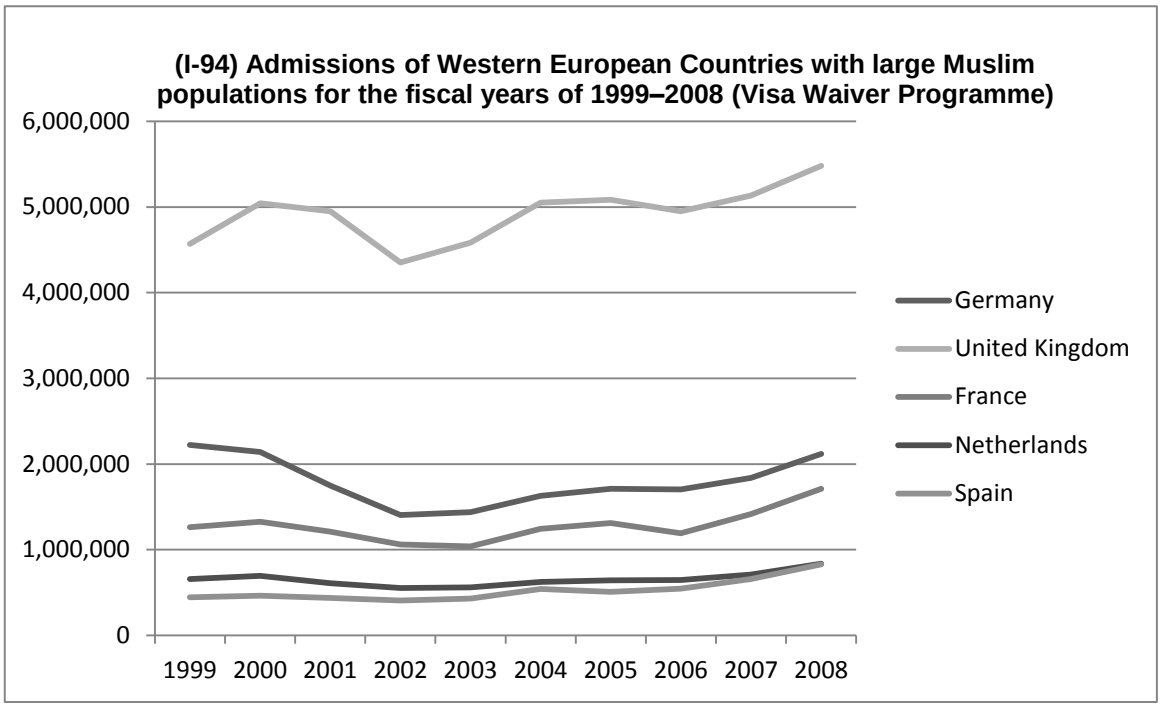
[96] Here it is common practise for visa holders, once their visas have expired, to remain in the country while they wait for a visa extension to be processed. In the case of student visas, the students are given up to 70 days to return to compliance if they violate the conditions of the SEVP. This means that despite the number of 'leads' produced for visa violations, a proportion, primarily in respect to the student visa process, are resolved prior to ICE involvement.

timely manner – here out of the approximately 300,000 leads generated over the 2004–05 period only 158,230, or 53%, had been processed; and (ii) the 138,652 leads closed by the CEU were found to be either 'in status', meaning that the violator had returned to valid visa status, or that that the visa holder was determined to have left the country since there was no address information to enable apprehension (Skinner, 2005). This is not only emblematic of a precautionary turn in respect to risk management: pre-9/11 visa overstays were simply viewed as an economic immigration problem impacting primarily those states bordering Mexico, but now each and every routine violation is elevated in importance to a potential terrorist predicate. It also shows that these systems, while seeking to obtain maximal information about immigrants within the country, break down. This rationale of governmentality, which seeks to acquire 'total information awareness', either creates too many alerts due to a precautionary selection process and therefore cannot process these alerts, or discovers that the idea of total information is somewhat of a fallacy since there is a lack of address information from approximately half of the constituents counted.

The general lack of apprehensions resulting from visa-violation referrals is not just a major issue in regard to how visa holders – who possess a high security value post-9/11 – are managed and monitored: these same delays and misidentifications also apply to those cases specifically related to national security concerns. These delays arose from two sources. First, much like normally assigned visa violations, the violations were caught within the basic processing inefficiencies of the CEU. For instance, 117 leads that were provided by NSEERS, the database used to track visa holders from countries designated as supporting or harbouring terrorists, each took an average of 33 days to move from the CEU to ICE. This can be seen as an inefficiency given the urgency through which executive directives are supposed to be carried out during a time of emergency. The second reason was that until 2004 with the passage of the National Intelligence Reform Act, visa holders who had the terms of their visas revoked while they were inside the United States on national security grounds could not be apprehended and/or deported unless a substantive immigration violation could be found (IRTPA, 2004). This problem of the inability to apprehend an individual who had his or her visa revoked on national security grounds was a constant point of contention for U.S. lawmakers over the two years following 9/11. Although it was resolvable with subsequence legislation, as discussed in Chapter 4, and the use of immigration charges for the purposes of counter-terrorism, it shows the entanglement and at times contradiction between legal norms and political prerogatives concerning the war on terror. A further consequence from the delay in processing these cases, whether designated a national security priority or not, is that the longer each file takes to process, the greater the probability that the subject of the investigation will not be found. This is due to the fact that the address information provided by foreign nationals as they enter the United States is considered to be 'perishable' in that it is either vague or incomplete, or indicates only a temporary residence for those individuals who are in the United States only temporarily. For example, the DHS Inspector General reported that one such visa violator whose file had been sent to ICE for enforcement had only provided the address of 'Hyatt' upon arriving in

San Francisco. The Inspector General notes that there are six Hyatts in the San Francisco Bay area (Skinner, 2005). This practise, then, of the generation of massive numbers of leads based on visa violations, as well as the inability for the DHS, CEU and ICE to respond in a timely manner in their investigation, suggests that this system of monitoring and enforcement is rendered inefficient due to the understanding of the generic nature of the terrorist threat. That is, in seeking to correct the past institutional lapses that plagued the immigration and consular system, not only respect to 9/11 but to the larger problem of visa overstays, the U.S. government has produced a system that does not significantly curb the visa overstay problem, nor does it react with efficiency to the ever-changing threat-horizon presented by terrorism.

Figure 5.4.1: Visa Waiver Programme Entrants from Western European Nations since 2001



(Hoefer, 2009)

Figure 5.4.1 represents the number of VWP entrants from Western European countries from 1999–2008. This graph is significant for two reasons: (i) it shows the general level of importance in respect to tourism and business traffic that VWP country nationals bring. For instance, out of approximately 15 million entrants from VWP nationals, France, Germany and the United Kingdom account for approximately 7.5 million entrants. The remaining 24 VWP countries account for the remaining 7.5 million entrants. (ii) The VWP countries of France, Germany and the United Kingdom – to a lesser extent Spain and the Netherlands – are viewed, apart from those countries subject to Terrorism Related Screening – Iran, Cuba, Pakistan, Sudan, Yemen, Russia and Afghanistan – as secondary but significant sources of extremist violence due to the large and segregated Muslim populations found in each nation. At the heart of this dilemma is that, while the U.S. is eager to curb terrorism, it is also eager to open its borders to VWP nationals who, while citizens of VWP countries, may have significant ties to countries such as those listed that have ties to terror.

5.4 The Economic Contribution of the Visa Waiver Program

Despite the deployment of numerous programmes to securitise the U.S. border and immigration system, and collect identity predicates associated with individuals crossing the border, a distinction can be made between those nationals from countries requiring visas to enter the United States and those from countries which are part of the Visa Waiver Program (VWP). The routines of individuation such as PNR analysis, biometric collection and terrorist

watch-list matching are carried out on almost all[97] entrants to the United States; however, the vetting routines carried out on visa applicants is much more rigorous than those screening techniques applied to VWP nationals. This screening differential has led to expressions of concern from members of Congress as well as from the DHS, who have argued that the VWP represents a vulnerability to the border-control process, since there is very little warning of the potential threat of an individual until he or she has arrived in the United States[98] (Meek, 2008). This security concern has also been reinforced as a result of the counter-terrorist policy that views Western Europe as a security threat, given its large population of Muslims, many of whom have active ties to countries with known terrorist activities, such as Afghanistan and Pakistan (NIC, 2007). This concern was highlighted by the 2005 London transport bombing carried out by five British Muslim men, four of whom had ties to Pakistan, as well as through the 2009 attempted bombing of Northwest Airlines Flight 253 as it descended into Detroit from Amsterdam. This attempted attack was carried out by a young Nigerian Muslim, Umar Farouk Abdulmutallab, who, like the 9/11 hijackers some eight years later, was able to board a connecting flight originating in Lagos as a VWP national since he held a British student visa – i.e., he was given travel clearance as a third country national. However, despite these security concerns and despite evidence suggesting that Islamist terrorism remains a threat to the U.S. 'homeland', the borders have remained open. Not only has the VWP been maintained and has served its original purpose of business and tourism promotion since 9/11, but as of 2008 it has been extended to six[99] further European countries, consistent with European enlargement (CEC, 2009). As a result, it will be argued, the requirements of economic openness and the maintenance of fidelity with U.S. allies and trading partners have generated pressures in a direction opposite to those of security.

What is compelling about this opposition between economy and security as it is embodied in the VWP is that it brings with it the 18th-century notion of security described by Foucault as 'limiting bandwidth' (Foucault, 2007). This notion of security is distinct yet not altogether separate from the identity-based security practises described in this thesis which seek to individuate members of the population in order to determine risk. This notion of 'limiting bandwidth', however, recalls an older logic of security that is based on the analysis and scrutiny of a population as a whole in respect to internal statistical patterns and regularities (Foucault, 2007) (Hacking, 1990). This understanding that a population has given internal patterns or laws, Foucault argues, gives rise to two modes of governmental logic: (i) that population becomes the 'final end of government' where what is to be governed are the different rates – birth, mortality, longevity, migration and so on – that constitute this given collective; and (ii) that this attention to population must be governed 'rationally' and with 'efficiency' and therefore results in the development of general economic procedures for

[97] All foreign nationals except Canadians are required to provide their fingerprint and face biometrics to U.S. border authorities as part of the US-VISIT program.
[98] This notion of vulnerability and lack of sufficient screening has also been expressed by Secretary Chertoff, who fears that terrorists could enter the U.S. via Canada.
[99] As of 2009 out of the six European countries offered to join the VWP: Czech Republic, Estonia, Hungary, Latvia, Lithuania and Slovakia, with a seventh, Greece, pending. In 2008 South Korea was also added as a VWP country.

governance. The implication of these conditions for security – or what Foucault describes as the milieu of security – is threefold: (i) that an event in question is inserted into a field of probabilities – that is, it can be made calculable and that it has a rate existing over time; (ii) that the political power applied to such an event is rationalised in respect to cost; and (iii) that instead of the establishment of 'a binary between what is acceptable and what is prohibited' an acceptable rate or 'limiting bandwidth' is established that acts as a limit or threshold on what is considered 'optimal' (Foucault, 2007). This notion of optimality or limiting bandwidth, however, does seem to be directly opposed to the definition of terrorism that U.S. counter-terrorist policy since the terrorist threat as catastrophic is, as argued by Beck unbounded – i.e., resting outside of the bandwidth described by Foucault. However, it does come to delimit, in part, how the VWP is administered in respect to large subsets of the travelling population to and from the U.S. It will be shown that where these three attributes break down, in respect to cost and the management of the event of terrorism in respect to probabilities, is taken up by a security approach that is discrete, that is based on the analysis of predicates against watch lists, etc., as opposed to a security practise that is continuous, or, rather, an acceptable limit in respect rates of visa overstays and illegal immigration. This notion of illegal immigration, primarily from South America and Eastern Europe, muddles the U.S. border-security picture where as a result and in respect to cross-border flows, despite the rhetorical and policy orientation towards counter-terror, the continuing problematic remains illegal immigration that accompanies open border practises via the VWP as well as simply by geographically possessing a 3,141-kilometer border with Mexico and a 2.475-kilometer border with Canada.

The economic rationality governing visa issuance and the VWP are illustrated by debates that took place shortly after 9/11 where congressional lawmakers considered not only placing a freeze on the acceptance of all foreign students but curtailing or even cancelling the Visa Waiver Program. In both instances, these arguments were overturned by an appeal to economic reasoning. The VWP was started in 1986 with the expressed intent of promoting business and tourism within the United States, and was made available to nationals of 26 countries who shared similar economic and political standing. The criteria to be admitted to this programme consisted primarily of general political and economic stability – for instance, Argentina was removed from the programme in 2002 as a result of its economic crisis due to fears of illegal immigration – as well as maintaining a passport rejection rate, or passport fraud rate – of less than 3%[100] (Goodman & Verne, 2006). The Attorney General may also remove a country from the VWP if an emergency situation arises that is counter to U.S. interests and prospects: the overthrow of a democratically elected government, war, a breakdown in rule of law, economic collapse or any other extraordinary event that may impact the United States. This does not mean that nationals from these countries are not

[100] What is interesting to point out is that in terms of the 2008 VWP additions, only Greece had a passport refusal rate of less than 3%. All other nations were found to have rates higher than this threshold, yet they were still admitted to the programme.

allowed to travel to the United States; it just means that they are not able to travel[101] directly, visa free. A further criterion for inclusion in the VWP is the way in which a given country is integrated within international standards concerning passport control and airport security. These requirements not only establish a base level of protocols that all countries must abide by, but they also allow for security technologies and data concerning the behaviour of international travellers to be transferrable. This notion of transferability is exemplified in the change of requirements the United States legislated through the Enhanced Border Security Act 2002 (ESBA) (Leahy, 2002). As mentioned earlier, ePassports passports are required not only to possess tamper-resistant pages but also to contain an embedded RFID chip that carries biographical data, such as passport number and name information, as well as biometric data in the form of a photograph of the passport holder's face. What is important to understand about this shift to these passports is that they do not simply create a new standardised field further separating VWP member from non-VWP member, but are also a step towards both maintaining the general integrity of the group and introducing a method of individuation**.** For instance, while the ePassport enables VWP nations to meet their required targets for the passport-rejection rate, the introduction of new tamper-resistant materials also makes it more difficult to alter a VWP passport if it is found or stolen. Second, these passports work to individuate or more closely tie the identity of the VWP national to his or her passport or identity credential. Much like US-VISIT, which obtains fingerprint biometrics of all foreign nationals at the border in order to fix their identities in respect to date, time, travel history and visa status, the ePassport creates an additional security layer through information embedded in the RFID chip that further grounds the identity of an individual who usually arrives unannounced at U.S. borders. Third, the introduction of these passports required that each individual in a VWP nation had an interview before obtaining a new passport. As a result, individuals who were issued passports that had not expired by the time the U.S. required only machine-readable passports to be used when entering the country had to re-apply for this new passport, thus presenting a further opportunity to verify the identity credentials of the individual.

This macro emphasis on rates of passport rejections as a dominant feature guiding security policy has, however, proved to be somewhat problematic for U.S. security. This is due not simply to the fact that even with the introduction of ePassports there is a chance that a visa can be tampered with or stolen. It also arises from the lack of cooperation by VWP countries, in particular, Western European countries, who typically fail to notify their American counterparts of stolen or lost passports in real time. For instance, in 2005 the DHS confiscated 298 fraudulent passports from individuals attempting to enter the United States via the VWP (Ford, 2006). What has compounded this issue is that U.S. border inspectors, despite the switch to machine-readable passports, do not have access to Interpol databases. This resistance to providing the DHS with stolen passport information, however, has not

[101] Even citizens of countries that are a security concern due to terrorist-related activities at times can enter and come to live within the United States. For instance, under the U.S. Refugee Admissions Program, since 2007 some 19,910 Iraqis have settled in the country as refugees. This represents a further way in which U.S. borders are managed that go towards admitting significant numbers of foreign nationals into the country on humanitarian grounds.

been due to the incompatibility of intelligence systems, but, rather, arises from concerns by VWP countries over the privacy of their citizens as has been evidenced in the previous chapter. This inability to thoroughly pre-screen has led to the imposition of additional screening methods to VWP nationals; namely, the creation of the Electronic System for Travel Authorization (ESTA), which requires all VWP nationals to provide their passport and flight details to the DHS for screening purposes approximately 72 hours prior to their arrival to the United States. This form of pre-screening seeks not only to provide a greater amount of information to be screened by U.S. security, blocking particular individuals from entering the country if need be, but it also provides a greater amount of time for security services to investigate and act upon potential leads.

However, despite these individuating security methods, the VWP has not only remained open, but has continued to support high numbers of tourists and travellers to the United States (as shown in Figure 5.4.1). This support of open borders, business and tourism has been maintained primarily for economic reasons, despite the fact that they run counter to the policy demands of U.S. security. For instance, in the post-9/11 period, France, Germany, the Netherlands, the United Kingdom and Spain, each with either large Muslim populations or experiencing terrorist attacks domestically, have only seen minor fluctuations in the number of travellers flying to the U.S. This is in stark contrast, at least in terms of the percentage of decline, to the reduction of visas afforded to Saudi nationals who were also regarded as close economic partners to the United States pre-9/11. We can thus see that economic factors – in terms of the contribution of the VWP to the U.S. economy – appear to be the dominant rationale for maintaining the programme. For instance, in 2000 VWP nationals accounted for over half of the total entrants into the county and for 57% of all tourists, where total tourism was $39.6 billion (Goodman & Verne, 2006). Moreover, the average VWP national spends $2,253 per visit as opposed to $1,274 spent by non-VWP nationals. As a result, the VWP not only contributes approximately $75–100 billion in direct and indirect spending to the U.S. economy, but this spending accounts for approximately one million U.S. jobs, concentrated primarily in New York, Florida, California and Hawaii (Goodman & Verne, 2006). The prospect of cancelling the VWP, then, would not only be the loss of tourist dollars spent, but also the loss of a projected 475,000 jobs, along with the corresponding tax revenues from American employees of $16 billion. A further consequence of cancelling the VWP would be the fracturing of longstanding diplomatic relationships and ties not only with economic partners, but with partners that were allies that supported the United States in the war against terror. For instance, the United Kingdom, Germany, Japan, Italy and Australia, each country with high volumes of tourist traffic to the United States, have each provided soldiers to the NATO-led military effort in Afghanistan. Furthermore, European nations have also worked with the United States to identify and freeze assets of suspected terrorists with holdings within the E.U. totalling some $100 million in 2002.

What can be seen from these economic and diplomatic arguments to keep the VWP programme open is that they amplify and give support to the 18th-century economic notion

of security as described by Foucault; one that is not simply based on monetary factors, but which works to allow for the continual succession of events, even unwanted ones, to take place. This rationale, as argued earlier, is in contrast to the security logics that have come to define U.S. homeland security and the war on terror. From an economic perspective, the fact that U.S. authorities confiscated 298 fraudulently used VWP passports is seen as an acceptable trade-off, since during the fiscal year of 2005 approximately 15 million VWP nationals entered the country. However, from the perspective of U.S. domestic security, any individual within that 298 could prove to be a terrorist threat – a plotter, a transporter of WMD, an agent of a foreign power – that could bring about catastrophe in much the same way as the 9/11 hijackers did.

5.5 Conclusion

This chapter has argued that a twofold security process has taken place in respect to the visa issuance system and VWP allowing foreign nationals to travel to the United States. On the one hand, additional practises of screening and individuation have taken place in respect to population categories that shared some resemblance with the motives and practises of the 9/11 hijackers. Here these practises have been applied to the populations of foreign students studying within the U.S. as well as those nationals from countries deemed to sponsor terrorism, or those nationals from nations who are not part of the VWP. The security routines to vet these individuals, while at times suffering from inefficiencies due to technological error or the competing interests of the multiple security agencies at work within the U.S., seek to verify individual identity and give advanced warning to U.S. domestic security agencies. On the other hand, nationals belonging to VWP countries receive far less scrutiny in respect to the thoroughness of background checks and pre-travel screening. Despite additional measures or layers of security – to be discussed in the next two chapters – these nationals only face additional scrutiny upon arrival at U.S. borders once in contact with immigration officials. This lesser degree of scrutiny, while objected to by U.S. congressional members due to the fact that VWP nations such as the U.K., France, Netherlands, Germany and Spain have large Muslim populations linked to terrorism, have maintained relative liberalism with this programme due to the economic benefit these nations bring in respect to tourist expenditures to the U.S. As a result, and returning to the broader theoretical discussion of the emergence of executive and sovereign power within the post-9/11 period, sovereignty can be seen to be increased for those individuals whose population category resembles that of the 9/11 hijackers, but curtailed or restrained in respect to those categories of tourist that contribute approximately $100 billion to the U.S. economy each year. What is also evident is that despite the move to create new methods of categorisation and vetting within the United States for foreign national groups, U.S. domestic security is inhibited by institutional inefficiencies that are attributed either to disagreements over what constitutes a threat between competing security agencies or to the proliferation of suspicious activities that in an era of preventative policing overwhelm the system.

6. [LAYER 3] Biometrics and Identity: U.S. Border Security Post-9/11

6.1.

The biometric border-security capture system called the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is the third empirical layer examined as part of this study. As it was represented in Chapter 2, Charlotte Epstein argues that US-VISIT and its collection of fingerprint and face biometrics regards foreign nationals as mobile bodies, embodying risk. While it will be shown in this chapter that this assessment is accurate, whereby US-VISIT works to collect biometrics at the border in order to be matched against terrorist watch-lists, the analysis presented in this chapter will further show that the empirical reality of the functioning and performance of this form of risk analysis is complicated by competing interests and policy directions between the FBI, DHS and in fact Department of Defense (DoD). Beyond the complications of risk assessment that result from competing policy aims as well as conflicting technological standards that in certain instances prevent the sharing of captured biometric information between agencies; US-VISIT functions not only as a security setup that assesses the risk of individual travellers, fixing their identity within space and time, but as the meeting point for domestic and international counter-terrorism practises. That is, US-VISIT does not work in isolation in the vetting and assessment of foreign nationals crossing U.S. borders; rather, it is enhanced and strengthened via the acquisition of biometric data obtained from the FBI – and their ongoing domestic terror and criminal cases – as well as from the DoD, who operate their own biometric capture programmes in Iraq and Afghanistan. As the third security layer addressed, US-VISIT can be seen to extend the geographical integrity of the U.S. border where information on entrants is gathered not only from established travel routes, but from those zones where digital infrastructure – the very infrastructure that makes this new form of border security possible – is less available.

6.2. Why Biometrics

In 2004, US-VISIT was deployed at 115 U.S. airports, 14 seaports and 154 out of a 170 land-ports of entry to the United States with the expressed aim of collecting biometrics from foreign nationals for the purposes of identity verification (GOA, 2006)**.** As indicated, biometric collection by the DHS was seen to answer the problem of possible fraud or abuse of travel documents by foreign nationals by providing an auxiliary method through which U.S. security services could verify individual identity. It also envisaged a way for U.S. immigration to keep track of those individuals who had overstayed the terms of their visas by requiring biometrics to be taken not only on the way into the country, but upon exit as well. While this notion of tracking visa overstays has only been partially enabled as described in the previous chapter and due to the fact that as of 2012 a comprehensive ‘exit’ system has yet to be developed, the collection of biometrics has presented U.S. security services with a number of security gains. These gains are twofold: biometrics work to fix the identity of the individual in time and space by placing an immutable bodily record within U.S. security databases to be referred to

upon future encounters; and through the ability of U.S. security to match these biometrics against terrorist watch-lists in real-time either to apprehend suspects at the border or to be used as points of reference in counter-terror investigations. Despite these gains and before asking the further question of how US-VISIT operates as a security layer, the question of why biometrics have appeared within the context of the border needs to be asked. This question results from the specific lack of clarity as to the origins of the selection of biometric technology to be used at the border versus many other viable identity credentialing techniques. For instance, it was shown in the previous chapter that the problem of visa overstays or the violation of the terms of visa, at least in the case of 9/11, were attributed to an unmonitored student visa programme and an overly liberal visa issuance process that did not require interviews from visa applicants. It also showed that the policy rationale through which border security operated was attentive only to 'intending immigrants' or drug smugglers, not terrorism. These problems, if not completely solved, were addressed by applying a stricter set of identity verification and vetting procedures to these programmes. What definitive security gains, then, do biometrics add?

This question is provided with further definition by comparing USV and the Japanese passport-control process. Like USV, Japanese border control requires foreign nationals to provide face and fingerprint biometrics for the purposes of identity verification upon arrival to the country. Japanese passport control also places a small 'Quick Response Code' (QR Code) inside the passport of each foreign national that indicates the date they entered and the date they are due to depart – 90 days hence for VWP nationals. Upon exiting the country, however, instead of retaking biometrics from each foreign national to be matched against the original biometric obtained at entry, Japanese passport control locates and scans the QR code within the individual's passport to ensure compliance with the condition of visa and duration of stay. Comparing this process with USV, it can be seen that biometric capture serves a similar function in the U.S. as in Japan: to consistently record the identity information of the individual to be used, as well as part of counter-terrorism efforts. But what about other policy aims, such as visa-overstay? Japan has taken on the process of simply matching an attribute of the passport with the individual upon exit. In the case of USV, the policy aims have specifically forwarded the use of biometric verification for the purposes of an entry/exit programme, yet a decade after 9/11, USV has only the capability to perform entrance verification. While it is important to enquire after the causal properties of a lack of an exit programme – which primarily can be answered with the same economic reasoning offered in the previous chapter, simply that an exit procedure would negatively impact the U.S. trade economy as well as place additional burdens on DHS budgets – it is perhaps more important to ask why biometrics in order to uncover clues of institutional practise and aims. Before addressing this question, it is important to review briefly both what a biometric is and how verification function as well as touch on the history of fingerprinting in order to identify key technological attributes as well as historical rationales for the practise of fingerprinting that are consistent with those found in USV.

6.3 What is a biometric?

A biometric is a distinct behavioural or physiological characteristic of the body that can be measured and used to reliably distinguish one person from another (Mansfield, et al., 2001). There are many types of biometrics or characteristics of the body that can be measured, but many are either too difficult to evaluate efficiently – such as the retina or an individual's DNA – or are not statistically significant enough to match reliably or differentiate one body from another over time. As a result of these two factors, accessibility and statistical integrity, the two most commonly used biometrics are fingerprint scans and the iris image. The face, which is also commonplace and is described as a biometric, has been kept in many applications according to convention,[102] but it is not regarded as robust and therefore has had a limited role in automatic processing due to high false-positive rates. Biometric authentication in general has been described as performing two functions: identity verification or the verification that an individual is in fact who they claim to be or if they have been previously enrolled in a database; and watch-list screening matching an individual's identity against a database, 'where [. . .] . . . "undesired" identities are registered' (Daugman & Kabatoff, 2008, p. 82). The biometric scientist James Wayman has argued that biometric authentication, or the field of biometrics, is not forensic, but is used solely as a control technology, with the aim of including those individuals who have been enrolled in the system while keeping out those who have not, and further identifying those individuals who have been enrolled but are no longer welcome (Wayman, 2000). While this claim is not inaccurate, it has been argued that a key component of USV has been to collect fingerprint biometrics precisely to perform a forensic function, matching fingerprints gathered in a database against latent fingerprints obtained as part of a terror investigation. This will be discussed in greater detail later in the chapter.

For a biometric to be computationally robust, it must be invariant, durable, distinct and accessible to some form of reading device. It is instructive, then, to compare the attributes of the most common biometrics: the face, the fingerprints and the iris image. The face is not a good biometric in terms of robustness because of discernible changes that can be recognised approximately every five years, but it is perhaps the most universally accessible (Daugman, 2003). Fingerprints can be regarded as more robust than the face, but they, too, have issues concerning durability. Fingerprints can be damaged if exposed to chemicals, they dry out in old age and 1 in 100 people are without fingers or fingerprints altogether (Mansfield, et al., 2001). The iris, however, does not suffer from problems of durability because it is a part of a highly protected internal organ that is visible externally and, as medical evidence suggests, iris patterns do not change over the course of an individual's life (Daugman, 2003). In terms of distinctiveness, the face, while highly unique in the mind of the

individual, contains limited statistical significance; the fingerprint is both distinct and provides a pattern that can be considered significant, and, as it will be shown in the following paragraphs, is the most commonly used biometric within the context of law-enforcement and intelligence. The iris, again, is the most computationally complex of these three biometrics where this complexity is the result of an epigenetic process that begins at three months and finishes at eight months in the womb (Daugman, 2005).

Biometric authentication works by matching the desired biometric from an individual with a biometric template already enrolled in a database. As mentioned, this process is used to verify the identity of an individual or to determine whether an individual has been placed on a security watch-list. The biometric in question is obtained by using a sensing technology, typically computer vision, when analysing an image of the face, fingerprint or iris. The iris is the paradigmatic biometric for performing this task since it operates according to a failure of a test of statistical independence when comparing two iris images. According to the Daugman algorithms, the uniqueness or complexity of the iris is equivalent to a sequence of 249 (independent) coin tosses, in which each individual iris is considered to have 249 degrees of freedom[103] (Daugman, 2003). This number is significant as a principle of pattern recognition since it works to maximise between-person variability while minimising within-person variability therefore providing a high degree of certainty that two iris images are either the same or different as part of the authentication process (Daugman, 2003). Pattern recognition works by privileging difference, and it is the complexity of the iris pattern or fingerprint that provides this quality. It would be wrong to suggest that despite the high degree of complexity of the iris, or the sufficient complexity of the fingerprint, false-positives and false-negatives, do not occur within biometric systems. In fact, there are two ways that these errors can occur: (i) if the system itself is 'spoofed' – that is, where an individual makes a fraudulent claim to identity using a fake biometric;[104] and (ii) if the biometric-matching process encounters the unlikely single-case – that is, where the 1 in 1,000,000 or 1 in 100,000 chance for a false match does occur. Although there are many counter-measures to fraudulent biometrics, the false match produced through the identity-verification process does not necessarily pose a tactical problem, but a political and economic one. For instance, as it has been shown in the previous chapter, a key factor in maintaining the openness of the border to foreign nationals across the visa spectrum was primarily due to economic considerations. Similarly, biometric systems managing iris or fingerprint recognition can be made more stringent in their matching criteria, therefore reducing the number of false-positives, although this has two contractor impacts. First, while a more stringent matching criteria would reduce false-positives, this criteria would inversely increase false non-matches since any imperfection or difference in quality between two of biometric images would lead to a non-match even if the biometrics were legitimately the same. The increase in false non-matches, then, would have a negative economic impact at the border since it would require

[103] Remember that most of us have two irises that are each independent of one another and, if both are used within a security application, can provide an additional security layer.
[104] Here it can be imagined that a fake biometric would consist of something like an iris image printed onto a contact lens, or the creation of a fake fingerprint that could be achieved using a silicon imprint.

additional time spend by a border guard or other biometric administrator to obtain a correct biometric match. Conversely, if the economic concern is satisfied, where the matching criterion is made more liberal, then a political issue arises due the increase in false-positives. The notion of false-positives in respect to homeland security applications has been argued as acceptable 'collateral' damage by Posner and Vermeule, who view domestic security not only as a social good, but as a good that services the majority – it will be shown in the next chapter that despite this appeal to the 'greater good' false-positives have significant negative impacts for individuals (Vermeule & Posner, 2007). While false-positives in respect to biometrics have not become overtly problematic for the DHS since 2004, the ability to meet counter-terrorism security goals – ones that are grounded in the notion that terrorism is catastrophic and generational – is placed in question due to not the ability to match discrete fingerprints, but to match newly acquired biometrics against the widest data set possible. In order to further understand how this process of matching across databases works, as well as to answer the question of why biometrics, a brief history of biometrics along with backgrounds of the three databases that converge upon USV is required.

Figure 6.3.1 Legend for Biometric Performance Figures (Fingerprint, Iris Image, Face)

Biometrics verification rates				
	FMR: False Match Rate	**FNMR**: False Non-Match Rate	**FAR**: Failure to Acquire Rate	**VSR**: Verification Success Rate
Fingerprint	1 in 100,000	1 in 100	1 in 100	81%
Iris Image	1 in 1,000,000	1 < 100	1 in 50	96%
Face	1 in 1000	1 in 10	0	69%

(U.K. Home Office, 2004)

6.4.1 A Brief History of Biometrics

The historians Sengoopta and Cole have separately traced the origin of fingerprint technology to the economic expansion of the East India Company and the British Raj, with the first application taking place in the aftermath of the Sepoy disturbances of 1857. Fingerprinting as a technique was 'invented' by William Herschel, a colonial administrator of the Hooghly district of Bengal, who described that the outcome of the disturbances, which were caused by rumours that British soldiers lubricated their rifle cartridges with beef and pork fat, had led to prolonged violence and civil dysfunction (Sengoopta, 2003). Fingerprinting was used to intervene into this perceived chaos, providing a fixed and stable point on which to anchor claims of identity. Herschel also found that a large number of local inhabitants were collecting pensions by impersonating deceased pensioners, because there was a very low threshold for what constituted proof of identity when applying for and

receiving a pension, and, as has been often cited, British soldiers were unable to tell the difference in appearance from one native to the next (Cole, 2001).[105] Fingerprinting, then, was inserted into the British colonial context, primarily as an administrative tool, where the British colonial power attempted to act as the arbiter of legal disputes and, when the situation arose, even for criminal identification. This notion of the ability to distinguish between seemingly indistinguishable peoples or to obtain a stable basis of identity is the first quality of biometrics and its historical use that can be seen to be imported into USV as well into U.S. military operations in Iraq and Afghanistan.

While the discourse of the criminal recidivist and the hereditary criminal were already an active part of legal debates within Western Europe during the mid-1800s (Matsuda, 1996), when applied to the Indian colonial context this discourse took on new meaning. With a mixture of amateur British ethnography, which viewed India's caste system according to hierarchical racial types, and the theory of the hereditary criminal, a new theory was 'concocted' where many lower castes were not simply regarded as racially inferior but born criminal, as 'criminal tribes' (Cole, 2001, p. 68). In actuality, these tribes were simply lower-caste and nomadic peoples, and not expressly linked to criminal activity. However, these theories worked together with British suspicion that equated nomadism with criminality and resulted in the passing of the 1871 Criminal Tribes Act, which called for their 'registration, surveillance and control' (Cole, 2001, p. 68). This bill, 'made possible to proclaim an entire social groups criminal, on the basis of their ostensibly inherent criminality', and 'hundreds of communities were brought under the Criminal Tribes Act' in which fingerprinting played a central role (Cole, 2001, p. 67). How fingerprinting within the context of USV has departed from an application against a specific group or population is that fingerprinting or biometric acquisition has been applied to all foreign nationals as opposed to a specific ethnic or religious group. While biometrics can be seen to control a nomadic population – namely, the daily group of travellers that pass through U.S. borders each day – U.S. counter-terrorism has sought to depart from racial profiling despite the fact that the 9/11 hijackers were of Middle Eastern and North African origins and possessed Islamic beliefs.

The second example of fingerprinting foreigners, which will help support this first argument, is the use of fingerprinting for that very purpose on Chinese migrants to the United States during the Gold Rush and railway expansion era of 1840–1890. Within the American context, Cole notes that, while the institutional capacity of the American criminal justice system was too weak to take on fingerprinting during these early periods of migration, another agency, U.S. Customs, did take active interest. As with the British colonialism, the need for identification in the United States did not concern criminality so much as it did the control of a mobile population of racial 'others"' (Cole, 2001, p. 120). By 1880, Cole notes, 100,000 Chinese had entered the United States, where approximately 75,000 settled in California. While Chinese labourers tended to work in different industries than white Americans and for

[105] One of the largest applications in the world for iris recognition administered by NEC technologies is currently in use in India for the very purposes of fraud prevention in regard to the distribution of food stamps and subsidies.

even lower rates of pay, they became a convenient scapegoat during the depression of the late 1870s. Anti-Chinese sentiment resulted in U.S. Customs placing all new Chinese migrants under closer administrative scrutiny, but as in the British colonial example, U.S. Customs officials had difficulty distinguishing between the Chinese and complained about 'the great similarity . . . in the colour of their hair, eyes, and skin' (Cole, 2001, p. 123). It wasn't until 1883 that the fingerprint was used, with this time a thumbprint being obtained. The institutional language around this use Cole recounts was described by Detective Henry Morse, a U.S. Customs official, as 'certain and cheap' and 'better than a photograph – men's faces change, but the creases of the skin, never' (Cole, 2001, p. 132). In 1885 U.S. Customs attempted to impose an exit, re-entry system, taking the thumbprint of all Chinese migrants who planned to leave the country with the intention of returning. On August 1, 1885, it was established by U.S. Customs that out of 35,235 certificates issued; only 14,726 were collected from returning Chinese at U.S. Customs. There was reason for alarm that some 20,509 certificates were outstanding. While the debate raged within the Pacific Branch of U.S. Customs over how best to track and monitor the entry and exit of the large migrant Chinese population – simultaneously a valuable source of labour for California's industry and the object of derision by white Americans – U.S. Congress, in 1888, under nativist pressure, simply cancelled the certificate system and banned the entry of Chinese altogether. This ban lasted for a further 10 years, during which time all Chinese residing within the United States were forced to re-register with authorities but without the aid of fingerprinting. Mobility and the threat of a 'racial' other can be seen to typify the historical use of biometrics for population management. What these examples show is that biometrics not only act as a control technology such as defined by Wayman, or as a way to match fingerprints or irises against a suspect watch list, but also in respect to policy biometrics have been deployed with a specific purpose. Within the historical context, this purpose can be seen as the need to distinguish between individuals within contexts that lacked appropriate identity infrastructures. The second purpose has been to manage specific populations where biometrics allows not only for identity verification, but a form of accounting and monitoring. Within the context of USV, all three processes are at work: a highly mobile population is identified according to statistically significant identifiers – not just a passport which invites an opportunity for fraud; that mobile population – in this case foreign nationals – is monitored and tracked; and finally, and this is the technological innovation or departure of biometrics attached to the database from its predecessor, is the ability to match collected biometrics against various watch lists. However, the use of biometrics still seems to be somewhat misplaced. Again, the question can be asked: Why biometrics and not just more advanced passport design? The answer can be found in the more recent history of biometric practise pre-9/11 of both the FBI and INS or U.S. border security.

6.4.2 IAFIS/IDENT

In order to answer the question, 'Why biometrics?' as part of USV, beyond the historical and scientific presentation of the attributes of biometrics, it is necessary to look at the past

institutional practises of the FBI and the INS in the decade leading to 9/11, a decade that saw the development of two separate automated fingerprint systems by each institution. In 1989 U.S. Congress provided funding for the INS to develop an automated biometric identification system called IDENT based on the understanding that not only were more than 1.5 million illegal aliens apprehended at the U.S. Southern border each year, many of these aliens held either past border-crossing violations or criminal histories (USDOJ/OIG, 2000). The rationale for IDENT was further supported by a statement by Congress in their attempt to 'to address the so-called revolving door phenomenon of illegal entry by aliens . . . to clearly define the problems of recidivism as well as to immediately identify those criminal aliens who should remain in custody of the INS' (USDOJ/OIG, 2000, p. 6). The INS then required an efficient way to determine which aliens should be detained within the United States and prosecuted against, or released back across the Mexican border. As in the historical example of colonial India, U.S. border control was also confronted with the inability to track accurately the identities of the individuals detained since aliens typically travelled without identifying documentation and provided false names when apprehended. Approximately one year later, in 1990 the FBI was also granted funds to update their paper-based fingerprinting system that had been in existence since the 1920s to a digital system similar to that developed by the INS. This system was called the Integrated Automated Fingerprint Identification System (IAFIS). However, unlike the described INS system, aimed at quickly collecting and scanning biometrics at border stations, IAFIS played a central role in the FBI's domestic criminal investigations where the database itself carried over 47 million 'flat file' 10 fingerprint records – or fingerprint records of individuals taken as part of the procedure for arrest (Inspector General, 2004). In 1991 the INS and FBI met in order to discuss points of collaboration with the joint recognition that it would be useful for both the INS and the FBI to share biometric information in order to match against the broader, more detailed FBI database and to provide INS officials with additional data in order to determine the criminal history of aliens in custody. While this notion of collaboration was viewed as beneficial, the INS chose not to integrate IDENT with IAFIS on the grounds that the FBI could not provide the INS with either the computer power or the administrative speed to process the amount of fingerprints collected at the border. The INS also objected to the demand by the FBI that IDENT collect all 10 fingerprints so that it could better match up with IAFIS. What is interesting to note is that this cleavage or distinction between 10 and two fingerprints lasted until 2008, when the DHS was finally able to deploy a technology that enabled the collection of 10 fingerprints according to the precepts of efficiency and economy required at the border (Inspector General, 2004). For instance, until 2008 and advances in biometric and matching technology, the FBI could not meet the stated goal of a 2-minute 10-fingerprint match against IAFIS. Here, much like as it was described in the previous chapter regarding institutional inefficiencies impeding counter-terrorism, are endogenous factors curtailing the collaboration of two security agencies.

Despite the lack of integration with IAFIS, the INS set a goal with IDENT to enrol all apprehended aliens in order to be matched against their own internal lookout and recidivist

databases. The process functioned as follows: an apprehended alien would provide their right and left index finger to be scanned; also, a photograph would be taken that contained accompanying biographical information entered by the border-control agent. The fingerprints would then be matched against x > 400,000 records of aliens who had been previously deported by the INS or had a criminal record; and matched against x > 1,000,000 alien records who had been previously apprehended and enrolled in IDENT (USDOJ/OIG, 2000, p. 8). With the first match taking place against the 'lookout' database, border officials would be presented with a list of possible identities the biometric could be attributed. The official then would further match the original identity against the recidivist database in order to determine a consistent identity. This process typically would take less than three minutes. If an alien was found to have a criminal record, the arresting border official would contact the Western Identification Network Automated Fingerprint Identification Center (WIN/AFIS), which held a comprehensive list of warrants on alien trespassers. Once a field agent passed on the biometric information to WIN/AFIS, WIN/AFIS would confirm a 'lookout match' and directly phone the field office conveying the nature of the warrant, providing the contact details for local law enforcement. With this information, the border patrol agent handling the case would contact local law enforcement, which was responsible for issuing the warrant and ask if they wanted to pay for transport of the alien to their local jurisdiction for prosecution. If local law enforcement did not want to pay for this transport cost, U.S. border patrol would return the alien across the Mexican border. In following with this form of border enforcement, which was limited or curtailed due to internal economic pressures, an audit of IDENT by the Attorney General in a 1998 report found that the system itself was underused. For instance, it was found that the INS was enrolling less than two thirds of the aliens apprehended at the U.S. Southern border, and that only 41% of aliens deported in FY 1996 were entered into the system. Furthermore, out of this 41% only 24% of the records contained photos and there were no sufficient standards placed on the quality of images entered (Inspector General, 2004).

The lack of an integrated IDENT/IAFIS database, economic constraints preventing the enforcement of warrants against aliens at the border, and the inability of INS border guards to enter biometric information consistently and accurately into the IDENT database – apart from revealing a programme that was mismanaged – led to two major incidents that carried through into the debates concerning immigrant tracking and the use of biometrics within the post-9/11 period. These cases are known as Resendez and Batres – only the Resendez case will be discussed here. In 1999 a warrant was issued for the arrest of Rafael Resendez-Ramirez (Resendez) for the murder of Dr. Claudia Benton in her home near Houston in December of 1998. In May of 1999 Resendez was connected to three other murders in Kentucky, where he subsequently became known as the 'railway killer' since he was believed to travel around the U.S. by freight train, killing his victims in and around railway lines. At this time he was also placed on the FBI's 'Ten Most Wanted Fugitives' list (USDOJ/OIG, 2000). Despite the four warrants for murder, Resendez had an extensive criminal history within the U.S. dating back to 1977, ranging from the destruction of private

property to grand theft auto and trespassing.[106] What is surprising, and perhaps further evidence of the lack of resources available to the U.S. border control and law enforcement, is that while Resendez did receive several 'significant' sentences for crimes committed, he 'typically did not serve a full sentence before being released from prison and voluntarily deported to Mexico' (USDOJ/OIG, 2000, p. 11). In the aftermath of the Houston murder, local police contacted the INS with a request to place an alert within IDENT that could be flagged if and when Resendez was next apprehended crossing the border. Early in the next year, Houston police again contacted the INS to obtain Resendez's identity file and seek further information regarding Resendez's behavioural patterns. After reviewing the file, Houston police noticed that the original request of placing a lookout on IDENT against Resendez was not carried out, even after he had appeared on the FBI's most wanted list. In March 1999 a third query was made to the INS by Texas law enforcement regarding Resendez that accompanied a request to place a lookout on IDENT, and for a third time this request was not followed up with. In April 1999, DNA evidence linked Resendez to a further two murders in Texas. In June 1999 Resendez was apprehended by Border Patrol and was enrolled in the IDENT database. After screening Resendez against the lookout watch-list, which, as it has been conveyed, did not contain any information concerning outstanding warrants in connection to seven murders, the Border Patrol agent processing Resendez was presented with five possible matches of 'prior apprehensions' – a prior apprehension would be enough to trigger an arrest for illegal entry into the U.S. At this time the agent dismissed these possible matches – here it could be understood that the agent did not believe that the five possible matches were in fact Resendez – and therefore allowed Resendez to voluntarily leave the U.S. for Mexico. When the FBI formed a special task force to track down Resendez on June 8, 1999, they found that not only had Resendez been within INS custody and voluntarily released just seven days prior, he had also been in INS custody seven times in 1998 (USDOJ/OIG, 2000). On July 13, Resendez turned himself in to U.S. law enforcement near El Paso, Texas.

In an audit of the Resendez case, the Office of the Inspector General (OIG) found three major faults with the practises of the INS and their use of IDENT. First, apart from the inability for INS officials to place a 'lookout' against Resendez in the database, it was found that the staff members to whom the requests were made did not have adequate training in how to process such requests; second, lookouts were placed on a 'day forward' basis, meaning that since the decision was made not to join IDENT with IAFIS, IDENT did not possess any data or criminal history pertaining to apprehended aliens from 1989 forward – as it was noted, Resendez had a criminal record stretching back to 1977 that was held in the IAFIS; last, beyond the lack of connection to the FBI IAFIS database, IDENT was also not connected to any other criminal databases either held by the INS itself or by other branches of law enforcement and domestic intelligence (USDOJ/OIG, 2000, p. 30). The notion of

[106] The past criminal record of Resendez is as follows: 1977: Mississippi destroying private property; 1980 Florida burglary, aggravated assault, grand theft auto; 1986 Texas false representation of U.S. citizenship; 1989 Missouri falsely rep to be a U.S. citizen; convicted felon with a firearm, re-entry after deportation; 1992 New Mexico for burglary; 1993 Texas evading request; 1995 California for trespassing; 1996 Kentucky trespassing.

interlinking criminal, terrorist and immigration databases, then, can be seen as the fundamental transformation of post-9/11 border security.

What this example reveals is that not only does it function as a 'single case' event, which illustrated the utility of biometrics at the border, but that it shows that there were already active programmes oriented towards the collection of biometrics pre-9/11 that had encountered and struggled with the challenges that the 9/11 hijackers posed. Furthermore, the Resendez case – a similar case of an illegal alien travelling from the Southern border to commit murder within the U.S. while being tagged but not recognised as a threat within IDENT – was submitted as evidence by the FBI when queried by Congress in the immediate aftermath of 9/11. Instead of highlighting the securitisation of the visa system by adding additional screening procedures for consular officers, the establishment of a student visa monitoring system or the development of name-matching systems to use PNR data, biometrics were first forwarded as the solution to the problematic of variable identity and the ability of foreign nationals to enter and exit the country unfettered. From a perspective of social science, it can be argued, then, that the answer to 'Why biometrics?' has less to do about the 9/11 hijackers as such – since it has been shown that the problem of 9/11 was due to a lack of data sharing between domestic and international intelligence as well as overly liberal visa-issuance methods – is, rather, based on the transposition of the programmes already in place at the southern border and made all the more urgent and frightening due to incidents such as Resendez. What is ironic about this transposition is not simply that the U.S. government was willing to extend a border security programme and rationale that was already riddled with errors due to funding and training shortfalls, but that the extension was applied to border points – air travel corridors – that were already heavily regulated and had pre-established mechanisms for verifying identity and monitoring individual behaviour. For instance, it is common understanding that a foreign national would not be able to board a plane from a foreign destination, let alone enter the United States, without a valid passport. In the case of the Southern border $x > 1.5$ million individuals were found each year to cross the border without identification, which raises an appeal to the valid historical and scientific utility of biometrics. In the case of the use of biometrics as part of USV, again, their use is found to be part of institutional cleavages transposed onto air, sea and land borders; beyond their specific application to the Southern border. What has remained consistent, then, is not only the application of such techniques and technologies to foreign nationals, but that the key security gain is attained through the linking of the multiple criminal and immigration databases held by the FBI and U.S. law enforcement with this new border security infrastructure. What has also remained empirically consistent – as was shown in the last chapter – are: (i) technical errors in linking and matching biometrics across multiple U.S. security agencies, since each agency, while serving the same goal of counter-terrorism and anti-crime, works under different operational logics;[107] and (ii) that the aims of USV to

[107] This distinction of operational logics has already been made in respect to the initial decision by the INS not to join IDENT with IAFIS due to the difference in the needs of its agents and their duties versus those of the FBI. The INS needed a quick response to determine whether or not an alien needed to be deported; the FBI required a longer

monitor both the entry and the exit of foreign nationals and visa holders who travel to the U.S., much like the efforts of IDENT in the 1990s, has been curtailed due to economic limitations. What is taking place, however, which fits with a new set of security gains made possible by watch-list matching and the interconnection with databases across U.S. law enforcement, is a new mode of individuation and analysis that works as part of a layered form of security.

6.4.3 IDENT/IAFIS Post-9/11: Integration into U.S. VISIT

In 2002 the Enhanced Border Security and Visa Entry Reform Act (EBSVERA, 2002) was passed, which amended provisions stipulated in the U.S.A. PATRIOT Act, to require the development of a multipurpose, multiagency database in order to verify the identity of 'persons who apply for a United States visa' (USDOJ/OIG, 2000, p. 3). In order to facilitate the development of this system that resulted in USV, the DHS proposed the IDENT act as the 'backbone' for the project because the INS – renamed the DHS – was already in possession of a biometric database and its infrastructure (DHS, 2003). The DHS stated that IDENT currently had 14,000 support staff to accompany 2,200 workstations throughout the U.S. and abroad. IDENT also contained biometric files on x > 12 million individuals and since 2000–01 had integrated all FBI IAFIS 'wants and warrants' on a biweekly basis, resulting in 6,547 confirmed hits along the Southern border during FY 2001 (DHS, 2003, p. 3). The DHS further argued that during 2001 IDENT had processed 3 million records, resulting in 26,238 'lookout' hits and the identification of 463,247 recidivist aliens – a dramatic change in the abilities of IDENT from just one year before. What the DHS also proposed as a carryover from the past operational logic of IDENT was that USV should maintain the use of two-fingerprint scans, which in their view had a 99% accuracy rate on a population of 12 million records, as opposed to moving to the full 10-fingerprint scan. It should be noted that even with an accuracy rate of 99% the number of false-positives would be 1%, or in the case of IDENT, possible matches would be approximately 120,000 identities that border patrol would need to manually sort through to determine admissibility. The number of false-positives was made even greater by the projection that USV would encounter 25 million travellers during the first year of use, or be exposed to approximately 250,000 false-positives, or 684 per day. This appeal to the pre-established requirement of two-fingerprint collection by IDENT versus 10 fingerprints required by the FBI fell onto the common theme of speed – where speed is used synonymously with economy. The DHS argued anew that two-fingerprint scanning, where systems were already in place at most air and sea ports that collected fingerprints, returned lookout responses within 10 seconds; 10-fingerprint scanning and matching against FBI databases was found to take between two and 10 minutes (DHS, 2003). A second argument put forward by the DHS concerned cultural sensitivities of North American Free Trade (NAFTA) partners, Canada and Mexico. Here both Canada and Mexico objected to 10-fingerprint scanning because each government felt that it was evocative of criminality –

response time in order to determine if the fingerprints collected from the alien fit within a larger ongoing criminal case.

this is despite the fact that 1.5 million aliens are apprehended at the Southern border each year and fingerprinted. What is slightly puzzling about this argument is that precisely due to NAFTA and the imperative to keep trade routes open at both the Northern and Southern borders, Canadians and Mexicans were exempted from USV altogether – Canada and the United States carry out the largest amount of bilateral trade in the world, with exports and imports totalling approximately $499.3 billion (Fergusson, 2006). What these arguments reveal are not only the stated policy aims of USV to: (i) enhance national security; (ii) improve the integrity of the immigration process; (iii) facilitate legitimate trade and travel; and (vi) adhere to all relevant privacy regulations a policies; but, more specifically, the trade-offs made at the empirical level between the exercise of sovereignty and the needs of economy. The intervention of economic constraints and the appeal to economic imperatives, then, can be seen to have two impacts on the development of USV, which ultimately challenges or troubles the notion of the exercise of absolute sovereignty at the border. First, the lack of integration with IAFIS during the early stages of USV led to inconsistencies in matching biometrics obtained at the border against criminal and terrorist watch-lists held by the FBI; and, second, as it has been mentioned, USV has not been able to develop an exit system to monitor visa holders and visa overstays. Despite the projection, USV in 2003 processed 43 million individuals out of a total of 425 million border crossings to the U.S. from VWP countries; or approximately 118,000 individuals per day (Inspector General, 2004) (GAO, 2007). However, during this period, which coincided with the first year of the Iraq war as well as the continuation of counter-terrorist operations within Afghanistan, VWP nationals were only screened against a terrorist watch-list provided to the DHS from the FBI that was updated once a month. This application of security appears to be at odds with what Islamic terrorism and especially during the first number of year's post-9/11, where an attack was believed to be imminent and catastrophic.

The second example in which security aims have been curtailed is in respect to the development of exit identity verification capabilities at U.S. 'points of entry' or POEs. While USV revealed that in 2004 its biometric matching systems had achieved 4,100 hits at air and sea ports of entry and 1,300 at land ports of entry, leading to 293 arrests, meeting the important requirement of watch-list matching – even if incomplete – at the border, the DHS could not realise a way to consistently monitor the length foreign nationals were staying in the country. This was due to the inability to develop an adequate exit system, where it was discovered that in order to do so, the replication of processes to verify identity upon entry would need to be replicated. Although the DHS attempted pilots at 12 airports and 2 seaports in 2004, it was at the land POEs that DHS ran into problems due to geographical constraints. For instance in the Thousand Island POE at Alexandria Bay, New York, the border crossing is situated in what is described as a 'geographical bowl' surrounded by rocks that prevent the expansion of additional vehicle lanes for fingerprint processing (GAO, 2007, p. 15). In 2007 the DHS determined that development of such exit systems was not possible not only due to the costs required by the U.S. government, but again as a result of the costs negatively impacting bilateral trade at the border.

6.5 Defence Biometrics

Thus far USV and the use of biometrics has been addressed in respect to its theoretical and empirical properties, showing that while biometrics provide a new mode of security at the border – namely, watch-list matching – the application of biometrics as a specific counter-terrorism technique is revealed as somewhat fraught whether due to economic, technological or policy constraints. What the previous sections have also shown is the understanding of border security that is primarily domestic, or concerned with the encounters of border agents at airports and border patrol along the Southern border, with foreign nationals, aliens as they pass through the threshold of the border onto U.S. soil. This tracking and mode of individuation has been described as supported by two databases, the FBI's IAFIS and IDENT used by the INS and then the DHS. A third biometric database that has come to prominence post-9/11 impacts the functioning of USV and adds to the consideration of the impact of U.S. border security. This third database is called the Automated Biometric Identification System (ABIS), administered by the Department of Defence (DoD), which has since 2004 gained prominence within the U.S. theatres of war in Iraq and Afghanistan.

The use of biometrics to support U.S. military efforts can be traced to the NATO intervention in Kosovo in 1998–99 as a population-management tool where the U.S. military had disciplinary problems with local nationals who would 'cause trouble' at one U.S. military base, only to find another and cause further problems (Kieffer & Trissell, 2010, p. 2). However, the use of biometrics took on new purpose after 9/11 in both Iraq and Afghanistan, where biometric screening – in this case both fingerprint and iris – came to be used to fix the identities of undocumented Iraqis and Afghanis that U.S. military personnel encountered as well as provide an indication of whether to "detain or release" (GAO, 2011). In 2004 the DoD formalised this biometric programme, administered by the Biometrics Identity Management Agency (BIMA) in order to create a central repository of locally collected biometrics – biometrics obtained from standardised screening and latent fingerprints found as part of military and counter-terrorist operations. An example of the use of biometric collection on the surface has the same qualities as the historical examples presented earlier, as well as those examples of fingerprinting at the Southern border – here the object is to distinguish and record the identities of those individuals who are viewed as not possessing an identity. In the case of ABIS, biometric collection is found to be more closely tied with active counter-terrorism and military efforts. For example, a use case can is as follows: biometrics were collected from a local employee who is working as a contractor for a U.S. firm in Iraq and has access to U.S. military bases. In order to gain entry to the base, the individual must present a biometrically enabled badge that is verified by matching the image of a biometric held on a computer chip on the badge with his index finger upon arrival to work. Several months later, the U.S. army raids a suspected terrorist safe house where they discover a hidden room containing bomb-making equipment. The military forensic team inspects the laboratory and

discovers latent fingerprints that through ABIS are discovered to be those of the contractor. He is arrested upon arrival to work the next day (Kieffer & Trissell, 2010).

While this example of the use of biometrics in the theatre of war indicates a security gain for U.S. military within their local vicinity, ABIS was also meant to export or extend the border into those front-line regions that were in fact the source of Islamic terrorism, where the U.S. was engaged. In order to do so, ABIS was mandated to communicate with both AFIS as well as IDENT with the rationale that: 'American citizens will not tolerate a situation in which the Department of Homeland Security, after taking biometric data, would grant entry into the United States of a person that the DoD can identify as an enemy based on his or her biometric file' (BTF, 2007, p. 5). However, empirically while this institutional directive would again appear to provide security gains, whereby new boundaries to be erected in the remote regions of the world could block specific individuals from entering the country, the methods of database integration read in a similar fashion to the initial coordination between IAFIS and IDENT. By 2007 ABIS contained approximately 1.5 million biometric records collected in Iraq and Afghanistan – in 2011 this number had increased to 4.8 million (BTF, 2007) (GAO, 2011). Despite this consistent and expansive use of biometric collection, it was found that U.S. military personnel were not provided with training for biometric acquisition and at times were provided with non-standardised equipment that led to the entry of some 630,000 biometric records that could not be searched against IDENT or IAFIS. Furthermore, due to the remote nature of America's wars, as well as the general complexity of the biometric collection and transmission process, the DoD and the Biometric Task Force opted to create their own database that they could internally administer. This separation of databases led not only to problems resulting in data sharing and data matching against U.S. counter-terrorist infrastructure; it has turned a process of data matching into one that is laborious and incomplete. For instance, the DoD manually provides the DHS each week with records of individuals on DoD watch lists; however, given the asymmetric and imminent threat of Islamic terrorism, it would seem that this works against overall U.S. homeland security efforts. The second problem that the DoD has encountered in establishing their own database is that it does not have the same matching capacity as either the FBI or DHS. As a result, the DoD can only run a maximum of 8,000 matches per day, compared to 200,000 by the FBI or 160,000 by the DHS (GAO, 2011). While this number perhaps seems adequate given the smaller scale of interaction between the U.S. military and those individuals who populate the biometric databases – contractors, insurgents, locally trained military and law-enforcement personnel – it does hamper U.S. security abroad if the U.S. military wants to: (i) conduct forensic work within the database that requires a large number of operations to be performed; and (ii) if U.S. military seeks to monitor the daily risk levels – i.e., whether or not a contractor, such as in the example provided, at some point in the future becomes linked to terrorism – of the local population that interacts with servicemen and -women.

6.6 Conclusion

Empirically, USV functions in a way that is consistent with those assertions made by Epstein in Chapter 3. USV works to match criminal and terrorist fingerprints against all foreign nationals at the border and, by virtue of doing so, considers this travelling population a population that contains a certain amount of risk (Epstein, 2008). While this description is appealing, given the data and examples presented in this chapter, a question further becomes, How, from the perspective of governmentality, is risk understood? For Epstein, although 'risk' and 'risky subjects' are identified as the end goal of a new security logic of the border that appears to be synonymous with the politics of the executive decision this term or the process remains uninterrogated. For example, if the theory of 'layering' as it has been presented throughout this thesis can be relied upon, not all forms of risk assessment take place at the same location. As it was shown in the previous chapter and consistent with Bigo's notion of the 'always already' of immigration procedures pre-9/11, specific populations or subsets of the general foreign national population travelling to the U.S. were accounted for with the creation of SEVIS as well as through the application of more stringent vetting procedures as part of the U.S. visa process. Seen in this context, USV then displays the characteristics that Epstein presents, yet the risk assessment process as part of border security for what are understood as more risky population categories primarily eixists elsewhere.

Yet USV still plays a role in homeland security, though again we need to look beyond USV in order to understand what that work is. The data conveyed in this chapter has shown that security gains provided by USV are not only a function of accountancy – accounting for the identities of individuals travelling to the U.S. – but also using the biometrics as an intelligence resource to be topically matched against domestic and international terrorist watch-lists as well as used as part of ongoing counter-terrorism procedures. But again, this notion of watch-list matching, like the notion of risk, needs to be broken down. Watch-list matching in respect to U.S. border security has existed since the 1990s, where it was shown then, as it exists at present, this process is not a seamless as it is described to be. Incompatible institutional prerogatives as well as different technological standards compete and disrupt specific policy aims. In the case of the border, the overarching security understanding that contemporary terrorism is catastrophic, generational and asymmetric – that evokes the right of the executive to take whatever means necessary in order to provide security during a time of emergency – is defeated or obfuscated by: intermittent uploading of watch lists from the FBI to the DHS, where the FBI is the active party fielding and pursuing terrorist tracking and prosecution; intermittent uploading of watch-lists by the DoD to the DHS, where the DoD is in the front line in confronting Islamists in Iraq, Afghanistan and elsewhere who have the potential to travel to the U.S.; and competing prerogatives by the DHS and FBI in respect to how fingerprints are collected and which database they are matched against – IDENT versus IAFIS – in order to respect border efficiencies and trade economy. As a result, USV is less of a declarative space – a space of risk assessment and name matching as such – and more of a space that contains a governmentality of a competing set of operations that, seeking to

identify recidivist criminals, terrorists and immigration violators, struggles at times to account for who these criminals, terrorists and violators are.

7. [LAYER 4] Subject to Predicate: Data-Mining, Terrorist Watch-Lists and Prevention/Precaution within Post-9/11 Border Security

7.1

As I have argued throughout this thesis, since 9/11 U.S. domestic security has adopted a layered approach to security based on the analysis of identity information that maximises the opportunities afforded to U.S. border security, domestic intelligence and the U.S. military to intervene upon terrorist threats. Furthermore, this layered approach to security moves from the macro to the micro in its mode of analysis, moving from a focus on the individual in relation to a national population (passport and visa analysis), a group (biometric matching of all foreign nationals), and the individual (analysis of individual biometrics as well as biographic elements against watch lists). This strategic aim not only seeks to geographically distribute these identity-oriented counter-terrorist practises – whether it is at the border, within a domestic context or located within the U.S. theatre of war – it also seeks through the joining of technical systems to provide the same threat information to all agencies involved in such threat detection. This process is far from seamless, as has been shown in Chapters 5 and 6, but it does work to pool intelligence information that was previously guarded either by U.S. domestic (FBI) or international (CIA) intelligence, providing greater powers of surveillance, scrutiny and ultimately intervention within the context of U.S. immigration. This pooling of data has not only taken place in respect to biometric information, with the legacy systems of IAFIS and IDENT, but also with the creation of terrorist watch-lists based upon the pooling and analysis of biographic information that accompanies the visa and travel process. This information consists of both the biographical elements belonging to an individual while he or she applies for a visa as well as those details, potentially more revealing, which belong to airline passenger manifests called Passenger Name Record (PNR) data and Advanced Passenger Information (API). This information consists not of a passport or visa number, but contextual information that can provide U.S. security within insights into the behaviour of the individual such as seating preference, the name of travelling companions, method of payment, frequent flyer number used and even what type of meal is selected. The analysis of this information then moves beyond binary matching (1 x 1 or 1 x N) found in the case of biometric analysis, to a mode of analysis based not only on binary matching, but data-mining in order to match/discover behavioural patterns that could determine criminality or terrorist intent. Thus, data-mining and watch-list matching can be seen to make up the third security layer that seeks to analyse the individual according to the combination of multiple biographical or numeric data elements associated with that individual which provide evidence of behaviour as well as about the social network the individual belongs.

Therefore data-mining and watch-list matching are incorporated into a governmental rationality that aims to identify: (i) individuals with outstanding criminal warrants or who are connected in some way to an ongoing terrorist investigation; (ii) individuals who have been deemed connected to terrorism but are not part of a terror investigation; and (iii) individuals who are suspected of being connected to terrorism. This rationale then works to either capture or ban those individuals who appear on terrorist watch-lists or those individuals who

are determined at the border to possess the potential risk of terrorism as part of a secondary interview process. It can be recalled that pre-9/11 the secondary interview process was used for those individuals who appeared as 'intending immigrants'. The secondary interview process now primarily looks for intention of terrorism. This governmental rationality is not only based upon forensic, preventative and precautionary principles, but works to create new kinds of subjects at the border associated with these three categories: a subject related to past harm, potential risk and definite risk. A fourth kind of subject can also be seen to emerge, where this subject is attributed to a false-positive or error within the technical system that attributes risk to an individual. However, in order for this rationale to be realised, U.S. security services have employed data-mining technology in both a practical and analytic manner. It is practical in the sense that data-mining technology, and, in particular, the technique known as identity resolution, allows U.S. security to firmly establish the identity of an individual linked to a past harm in a way that is deductive and closely linked to standard investigative practises that attempt to follow an evidence trail, even if digitally. The change that has accompanied the move from particularised to non-particularised search as described in Chapter 4 is a move from deductive reasoning to analytic or prospective interpretation such as is the case with watch-list and pattern matching. Here, an abstraction of empirical evidence takes place in order to inform a counter-terror decision. This abstraction, while it allows U.S. security to perform a prospective assessment of risk, brings with it a high rate of false-positives, due to the digital technology involved in data-sharing and data-analysis practises. This analytic form of practise also creates subjects that are incommensurable or incompatible with rule of law since, unlike individuals who are arrested at the border due to firm evidence connecting the individual to terrorism, the information supplied to terrorism watch-lists as well as the decision-making process of the border guard who decides an individual is too risky to enter the country, are not held to the same evidentiary standards. Therefore, an individual can be banned from the U.S. based on suspicion or circumstantial evidence rather than fact. It will be shown empirically in this chapter that this applies not only to what is called 'loose name matching' in respect to terrorist watch-lists but also to the nomination process for watch lists themselves.

7.2 Data-Mining as a New Mode of Statecraft

As introduced in Chapter 1 and described in respect to the legal prerogatives that inform U.S. counter-terrorist policy in Chapter 4, data collection, sharing and analysis have taken on a central role in how post-9/11 U.S. homeland security is conducted. Data sharing involved in watch-list matching allows U.S. consular service officials to determine if an individual may be granted a visa to enter the United States; data sharing and collection is involved in matching latent fingerprints found at locations of terror attacks against those fingerprints of foreign nationals entering the United States; and further data analysis is applied to PNR data in an effort to identify specific or suspicious patterns of interest. The definition and technical attributes of data-mining functions will be addressed later in this chapter. However, first it is important to consider how this movement towards data collection and analysis contributes a

new form of government rationality. In The Taming of Chance, Hacking argues that for the first time the modern state comes to know itself through the practises of enumeration, tabulation and the analytic practise of statistics (Hacking, 1990). The birth of statistics not only allowed nation-states to 'classify and tabulate their subjects anew, but it was made possible as a result of the 'avalanche of printed numbers' associated with the proliferation of printing technology (Hacking, 1990, p. 10). For Hacking, the ability to enumerate individuals and things within a given national domain and the further analysis of this data mathematically had two consequences. First, the nation-state was able to identify law-like regularities within the a given population – for instance, early French census efforts focused on mortality rates, birth rates, suicide rates and general levels of health. Second, this form of enumeration, categorisation and development of new knowledge based on categorical placement creates new forms of subjects termed as the 'making up of people'. Therefore, these new forms of classification allowed the development of new methods of monitoring and intervention applied to given socioeconomic groups – for instance, groups with high infant mortality, disease or rates of suicide could be addressed with policies and technologies if need be that were specific to the specific social problem (Hacking, 1990, p. 17). Hacking argues that this practise first intersects with statecraft in 18th-century Prussia, where King Wilhelm Friedrich, under the advisement of the philosopher and mathematician Gottfried Leibniz, was urged to enumerate the state, its population and holdings, so that it could know its 'power' (Hacking, 1990, p. 17). From 1730 onwards, initiatives began to be directed towards the purpose of enumerating and categorising the Prussian population – leading to a taxonomy of nine categories for Prussian citizens, 20 for categories for Prussian workers for the purposes of taxation – to the application of governmental techniques aimed at changing particular 'rates' within the society; for instance, Hacking argues that after the Seven Years' War (1757–63) Prussia was concerned with under-population, importantly, due to the fact that one third of the male population had been killed in the war, leaving Prussian territory vacant and unprotected. According to this argument, the birth of statistics, based on the availability of printed numbers brought with it: (i) an enumerative function; (ii) a function oriented around categorisation and the creation of new kinds of subjects that can be intervened upon; and (iii) a predictive function where law-like regularities provide clues about future behaviour.

When this argument is mapped into the environment of post-9/11 border security, several similarities and divergences can be found. First, while the birth of statistics is realised as the result of the 'avalanche' of printed numbers, post-9/11 border security, and homeland security in general, is based on the collection and analysis of a proliferation of digital information that has allowed for new forms of enumeration for the purposes of counter-terrorism. This digital information as argued in Chapter 1 also became a newfound asset for U.S. security services as it moved to apply techniques of data analysis that had long been standard procedures within data-rich sectors of private industry. Second, this analysis and use of digital information allows for new modes of categorisation to take place, although this form of categorisation is based less on the establishment of consistent categories using measurable statistical rates than on new categories of individual that achieve specific

thresholds or risk. This analysis is applied to identity predicates that work through a process of individuation and social network affiliation. Although prospective methods of analysis are employed, such as the technique called pattern matching – the placement of an already-known pattern of behavioural risk on a data set to determine if such patterns can be located – these prospective techniques only act as a starting point for further investigation. This practise departs from the statistical methods described by Hacking and taken up in the bulk of social science literature on how risk-based governmental practises are carried out. This is because there is no emphasis within post-9/11 security practises upon 'law-like regularities'. Instead of employing a risk-based governmental approach that obtains knowledge of risks that befall individuals in respect to a collective – well documented in the work of Ewald and Castel, amongst others – which attempts to 'master time and discipline the future' (Castel, 1991) (Ewald, 1991) – post-9/11 domestic and border security assesses risks associated with the individual and their associated identity predicates and operates according to a precautionary rationale in the face of a catastrophic threat. Clearly, there is an attempt by U.S. homeland security to colonise the future as such, but, as was shown in Chapter 3, the methodology chapter, traditional frequency-based approaches to provide a baseline to distinguish useful intervention from ineffectual intervention cannot be established since terrorist events are understood as both catastrophic and infrequent. Thus a new rationale for this particular form of threat is required. This shift to data-mining technologies then allows for the analysis of the individual to take place in relation to the population to which he or she belongs. This is a movement away from calculative or rationalised risks associated primarily with actuarial modes of reasoning towards notions of prevention and precaution based upon discrete watch-list matching or according to notions of suspicion determined by immigration officials at the border, of which biometric analysis and data-mining play a central role.

7.3 Data-Mining within Post-9/11 U.S. Border Security: Technical Attributes

Within the context of post-9/11 border security, the analysis of air traveller data is taken up in three different ways, each yielding a set of different security outcomes. First, PNR and Advanced Passenger Information (API) collected on foreign nationals is used to establish the identity of the individual travelling to the U.S. where these identity predicates are matched against predicates of interest developed by ongoing intelligence operations. Second, PNR and API information is analysed for patterns of interest that may identify an individual to be a potential risk, and therefore warrant additional screening by U.S. security services – for instance, if an individual was a national from a country with a risk of terror exhibited a pattern associated with 9/11 terror attacks, such as paying for a one-way ticket to the U.S. with cash. Finally, both national and non-national traveller information is matched against a series of watch-lists that scan for both terrorist affiliations – these lists are called 'no-fly' and 'selectee' lists – as well as instances of criminality where a warrant for arrest has been passed onto U.S. immigration and border patrol. However, before addressing how each process creates a new modality of security along with corresponding subjectivities and implications, it is

important to consider how the technical process operates, and to examine its perceived benefits and drawbacks.

Data-Mining: Entity Resolution, Pattern Recognition, Watch-List Matching

As described in Chapter 2, Taipale, states that data-mining technology as a tool for intelligence or law enforcement is essentially a 'sense-making' tool that allows for new knowledge and information to be obtained from data sets too large to be searched through or analysed by hand (Taipale, 2003). Data-mining within the context of counter-terrorism has been seen as a technological or digital method in order to 'connect-the-dots' by identifying patterns of interest amongst data sets within the possession of not only U.S. intelligence, but U.S. immigration and, in particular, commercial airlines. What is particular about data-mining technologies is that, unlike statistical analysis, they allow for the analysis of the individual in respect to the individual to take place, rather than an analysis of the individual in respect to an aggregate population. This does not mean that data-mining does not allow for any prospective inferences to be made. Rather, these inferences are based on the analysis of data as it pertains to counter-terrorist efforts and a general precautionary orientation to terrorist risk as opposed to a, in this case, strict mathematical determination. As a result, an alternate mode of understanding the threat of terrorism has been taken up in order to chart and map identity, and to draw localised inferences from this data. The data-mining methods used as part of counter-terrorism and border security practises can be seen to be: (i) subject-oriented – where an individual's predicates are charted as part of a wider investigation; and (ii) pattern-based – where a set of pre-existing templates are applied to a data set, such as templates that would provide clues as to terrorist behaviour (Taipale, 2003). While there are security gains from the use of each method of analysis, these techniques suffer the problem of false-positives that are amplified when data-mining techniques come to be used in a manner that is evidentiary as opposed to simply investigatory, such as in the case of watch-list matching.

7.2.2 Entity Resolution/Link Analysis

> And let me give you some idea about what the results of this have been. Using this kind of automated process of analyzing information that the law permits, in fact, mandates, that we collect – Congress mandates that we collect this information – using our ability to analyze this information we have been able to identify and to deny entry to over 500,000 people coming into the United States in fiscal year 2005 who shouldn't be coming in here – whether it's because of terrorism links, or because they've got criminal histories, or because they're smuggling people in.
>
> Let me give you one example. We had an instance where someone came in and would buy a ticket for themselves and a number of minors, and they'd enter the U.S. and then they would leave and only buy a ticket for themselves. Then they

> came in again with a ticket for themselves and minors and they left again with only a ticket for themselves. Well, this kind of process tells the border inspector, the next time that person comes in, you'd better pull them into secondary and maybe look a little bit more closely. And as a consequence of doing that, we were able to uncover a smuggling ring, a human smuggling ring, bringing children into the country. That is exactly what the public has a right to expect; it's exactly what Congress wanted us to do; and it's a critical illustration of how information, wisely used and sensitively evaluated, can produce positive results for security without compromising anybody's civil liberties or privacy. (Chertoff, 2006, p. 10)
>
> Secretary Michael Chertoff, Department of Homeland Security

As seen in the above example, one of the methods used in the context of post-9/11 border security is that of entity resolution that is designed to assemble multiple predicates pertaining to a single identity matched against a pattern or template that in this case is considered to be suspicious. In the example, the risk pattern or template in place is not necessarily looking for child smuggling, but for suspicious behaviour associated with the type of ticket purchased, as well as the companions associated with the subject in question. Read in relation to 9/11, it is notable that several of the 9/11 hijackers had purchased one-way tickets on the day of the hijacking; seat placement was an important element that allowed the 9/11 hijackers who were also pilots easy access to the airplane cockpit in order to take over the functioning of the plane. Here it can be seen that a new risk category or risky subject has emerged based on the purchase and travel habits of an individual passing through the border. A second example of pattern-based analysis at the border can be seen in assessment of data collected from I-94 immigration cards that all travellers must fill in and provide to U.S. customs upon arrival to the country. The I-94 form provides a relatively rich set of data because it contains fields pertaining to family name, date of birth, country of citizenship, passport number, gender, airline flight number and country of boarding. While a single I-94 record may seem benign or even trivial, the analysis of some 85 million I-94 records obtained by U.S. customs officials each year allows for multiple patterns – such as frequency of flight or passport number used by a single individual – to be revealed. In 2005 the DHS carried out such a data-mining exercise on a large subset of I-94 records where individuals were ranked and cross-referenced in respect to frequency of flight and passport number used. What is perhaps unsurprising is that each of the names ranked in the 'top ten' were non-existent names that were given a high score due to bad or improper data. However, the 11th name on the list did contain intelligence value and pointed out for U.S. security an individual who had used 54 different passport numbers on 240 flights over the course of one year (Westphal, 2009). What must be further recognised is that even in the identification of this 11th 'real' individual, it was found that the number of different passport numbers also suffered from extreme variability – due primarily to errors in the data-entry process post-I-94 collection; however, this variability was not enough to prevent investigators from looking

closer at this identity. In an effort to isolate the valid passport numbers from the false passport numbers, each flight out of the 240 flights taken by this individual was mapped on a timeline where four different numbers emerged. On further investigation, the address to which two of the numbers corresponded was located in Orange County, California, and belonged – as it was first assumed by investigators – to an individual working for a courier company who had changed his passport midway through the work year. It was further found that the two remaining passport numbers belonged to Mexican nationals, who not only were using the same passport number of the courier, but used the same work address (Westphal, 2009). What is significant and perhaps also contradictory about these examples active within U.S. border security is that: (i) they allow for the identification of hidden or unknown patterns that would not be made available without the use of pattern-recognition algorithms; and (ii) despite this ability to gain resolution of an identity, the process is riddled with errors in the form of dirty data and false-positives.

7.3.1 Watch-List Name Matching

The second mode of analysis of traveller data taking place in the context of post-9/11 border security is subject-oriented analysis or binary watch-list matching. The most prevalent and high-profile method of watch-list matching employed by U.S. security has been what is known as the terrorist watch-list, where all air travellers entering, exiting and travelling within the United States have their name data matched against three lists: (i) the terrorist 'no-fly' list, a list containing as of 2008 approximately 2,000 names of individuals who are barred from boarding an airplane with a U.S. destination; (ii) the 'automated selectee' list, a list containing approximately 14,000 names of those individuals who are placed under additional scrutiny while crossing the border due to the perception by U.S. intelligence of ties to terrorism; and (iii) approximately six other U.S. governmental watch-lists containing names of individuals who have committed criminal offences, immigration violations or other such misdemeanours. In total, these three lists contain approximately 500,000 names (Elias, 2005). However, it has been the no-fly and selectee lists that have proved to be controversial. Naïve name matching against a watch-list would seem to be a straightforward process in respect to identifying an individual of interest. In the case of standard criminal or immigration violations, this is the case: names of individuals who have committed criminal offences are uploaded to one of a number of watch-lists that have name data taken from API gathered from air carriers. If a 'hit' occurs, U.S. law enforcement is notified and the individual is apprehended at the border. However, the decision by the Bush administration to make use of no-fly and selectee watch-lists has proven to be significantly more complicated. The complication results from three factors: (i) that terrorists such as those involved in 9/11 actively utilise aliases while crossing borders or interfacing with governmental officials; (ii) that names added to the watch-list, primarily Arabic, suffer from problems of transliteration as they are translated from Arabic, Farsi or Persian into English – as an example, Westphal has shown that 'Mohammed' can have approximately 300 different spellings in English when translated (Westphal, 2009, p. 52); and (iii.) that post-9/11 counter-terrorism is a security

practise that is oriented towards the uncovering of plots attributed to an enemy that employs asymmetrical warfare – that is, terrorists for most intents and purposes look and behave like the average tourist or business traveller.

In order to address these problems, U.S. security has employed what are known as loose-name matching, or phonetic name algorithms in order to match names collected from traveller data against the no-fly and selectee watch-lists. However, instead of performing a binary match against these lists – one name, one value – these algorithms work to match names obtained from traveller data with 'like' names found on each list (Rosenzweig & Jonas, 2005). If we return to the example provided in the previous paragraph concerning the name Mohammed, the fact that phonetic name-matching algorithms have been employed seems logical at first glance. Terrorists use aliases; 'Mohammed' can be spelled in many different ways and therefore should be matched against names such as Mohamed or Muhammad; it is important to find close approximations to an individual's name as it appears in an air carrier's departure record bound for the United States. The problem, however, is that this practise of loose name matching has resulted in an extremely high number of false-positives, with problematic consequences such as denying individuals without any connection to terrorism from boarding planes, or even at times leading to false arrest. While the rash of false-positives as part of the watch-list programme can be attributed to the use of the phonetic matching algorithms, much like in the previous example, false-positives can also be seen to arise from dirty or bad data – data that is improperly sourced or contains errors – that has been incorporated into the no-fly and selectee watch-lists in the effort by U.S. domestic intelligence to quickly develop a counter-terrorist strategy. However, before describing the construction and empirical sites where the no-fly and selectee lists are used, it is important to recognise, as with the previous example, the new modes of subjectivity created by this process – much like the creation of new categories or subjects of analysis through the implementation of SEVIS or the addition of biometric analysis to VWP nationals. Like the process of entity resolution that locates suspicious patterns through the analysis of I-94 records, the watch-list process creates three categories of subjects: (i) those individuals who are wanted for criminal convictions or other such violations that have occurred in the past, where the individual is positively identified and apprehended at the border; (ii) those individuals who appear on the selectee list and are understood to have the potential to commit, in this case, an act of terror; and (iii) those individuals who are on the no-fly list who are barred from boarding a flight with a U.S. destination and are understood to with certainty pose a grave and serious threat to U.S. national security. The watch-list process therefore accounts for those individuals who have committed crimes in the past, those individuals who have the potential of committing terrorist attacks in the future, and those individuals, placed on the no-fly list, who are viewed as certain to commit terrorist attacks in the future – yet ironically, as it has been mentioned, cannot be arrested.

7.4 Pre-screening and Counter-terrorism: CAPS, TSDB, Secure Flight, PNR/APIS

Although passenger pre-screening did not become formalised until 2004 under the Intelligence Reform and Terror Prevention Act (IRTPA), passenger screening has existed in some capacity, at least minimally, within a domestic context since the early 1990s. Surprisingly, throughout the 1990s and until 9/11, this list contained fewer than 20 names.[108] Although this number is strikingly low, it must be pointed out that the FBI used and relied upon as many as 12 different watch-lists serving multiple purposes, but these lists were never coordinated into a single passenger scanning programme (See Figure 7.6.1).[109] In 1995–96 the Computer Assisted Aviation Pre-screening System (CAPS) was created in partnership between the Federal Aviation Authority (FAA) and Northwest Airlines, using a limited set of PNR data in order to determine the potential risk of individuals based on their travel itinerary. CAPS, however, was developed to identify passengers who may be seen as carrying bombs onto airplanes, here using PNR and API as a counter-terrorist tool, however, not as focused as in the post-9/11 period. For instance, nine of the nineteen 9/11 hijackers were selected by CAPS for additional screening, but since no bomb-making equipment was found, they were not prevented from boarding their intended aircraft (Elias, 2005). In the immediate aftermath of 9/11, the Transportation Security Authority (TSA), a newly created domestic security organisation housed within the DHS, began to develop CAPPSII, which was designed to validate and verify the identity of each passenger travelling on a domestic flight against both their PNR data and data collected from commercial databases specialising in background checks, such as ChoicePoint and LexisNexis.[110] Based on this information, CAPPSII would have worked to provide a coherent identity profile of a traveller to a security official that could then be used to assign a risk score – in this case, scores were color-coded with cardinality: yellow, orange, red – where those in the red category would be prevented from flying. In developing CAPPSII, the TSA argued that it would reduce the number of individuals 'flagged' under CAPS from 15% to 5%, due to the ability to draw from additional data sources (Elias, 2005). However, this notion, not only of collecting additional travel data on American citizens travelling domestically but also of accessing or mining commercial third-party data warehouse vendors, was viewed by Congress as again a potential violation of Fourth Amendment rights against unwarranted search and seizure. This congressional limitation placed on certain forms of data collection is, then, consistent with the argument put forward in Chapter 4; namely, that non-particularised search even during times of emergency is limited and bound by a set of constitutional protections that is displaced from a national to a foreign national population.

The strategy of passenger pre-screening reliant on traveller data persisted as mandated by the 9/11 Commission recommendations and IRPTA. As a result, two concurrent programmes were developed by U.S. domestic security; first, Secure Flight, a programme designed to collect data on domestic travellers; and second, the API/PNR programme responsible for the

[108] A further point to make about both the no-fly list and CAPS is that they were and remain designated to be administered by commercial airlines. That is, commercial airlines would receive the no-fly list and CAPS information and interface with law enforcement or customs depending on the information they received.
[109] However, the failure that was cited by the 9/11 Commission was not that the FBI had not performed due diligence in creating these multiple watch-lists, but, rather, that they were not coordinated and matched against traveller data.
[110] ChoicePoint and LexisNexis are commercial services that perform background and credit checks on individuals and corporations. They are industry leaders as a result of their collection of vast publically assessable data pools.

collection of data from foreign travellers entering the United States from international destinations – this programme has undergone several revisions due to privacy concerns expressed, for instance, by the European Commission in respect to the transfer of data collected for commercial purposes by European air carriers to U.S. domestic security.[111] However, there is a significant difference between these two programmes; that is to say, in the screening of U.S. citizens versus foreign nationals. While Secure Flight uses API, printed on the ticket stub of domestic travellers, it only requires three data fields with an optional fourth – name, data of birth, gender and redress number[112] if present – the API/PNR programme requires international commercial air carriers travelling, for instance, from the E.U. to provide up to 34 fields of data, apart from the API information also printed on the passenger's ticket. Although each programme matches the names gathered against the terrorist watch-lists – no-fly and selectee lists – a more significant amount of data is gathered from foreign nationals, allowing for the potential of more detailed analysis and risk assessment to take place. Moreover, foreign nationals who belong to any of the 36 Visa Waiver Passport countries must submit this flight information 72 hours prior to departure to the United States so that they can be properly vetted and given clearance for entry.[113] The data collected on foreign nationals, then, acts not only in similar fashion to that data collected on U.S. citizens – as a predicate to be matched against a watch-list – but as an added source of intelligence to be analysed, and stored for reference in the event of a future terror attack. However, as stated earlier in this chapter, data-mining technologies do not only bring with them the ability to identify patterns and actionable information from vast data sets, but also come with false-positives. To give a further sense of the scale of the pre-screening process and the problems that even a false-positive rate of 0.001% can bring, DHS Secretary Janet Napolitano's testimony to Congress shortly after the Christmas Day terror attack of 2009 is instructive:

> To provide a sense of the scale of our operations, every day, U.S. Customs and Border Protection (CBP) processes 1.2 million travellers seeking to enter the United States by land, air or sea; the Transportation Security Administration (TSA) screens 1.8 million travellers at domestic airports; and DHS receives advanced passenger information from carriers operating in 245 international airports that are the last point of departure for flights to the United States, accounting for about 1,600 to 1,800 flights per day. Ensuring that DHS employees and all relevant federal officials are armed with intelligence and information is critical to the success of these efforts.[114] (Napolitano, 2010, p. 2)

[111] The politics and controversy surrounding the transfer of PNR data from European air carriers to the Department of Homeland Security has been described in greater detail in Chapter 4 concerning the legal and policy field under which U.S. data-collection practises, for the purpose of counter-terrorism, operate.

[112] Redress number is given to those individuals who feel that they have been wrongfully added to the terror watch-list yet cannot obtain assurance that their name has been removed, even if they have been deemed a non-threat. Individuals are then given a redress number in order to avoid additional screening if in fact Secure Flight flags them on future travel.

[113] This pre-clearance process is conducted under the ESTA program (Electronic System for Travel Authorization).

[114] What is significant about this testimony is that it reveals not only the scale of the undertakings addressed by U.S. domestic and border security, but that as a result of the volume: (1.) an automated solution to passenger pre-screening is required; and (ii.) as a result of the implementation of such a solution, there are bound to be false-positives. In this case even using algorithms that have a low false-positive rate, due to the millions of people

To perform basic arithmetic using name-matching algorithms with a false-positive rate of 0.001% would result in 1,200 false-positives flagged for the CBP, and 1,800 false-positives flagged for the TSA on domestic flights each day. Even more problematic, if these numbers are placed in the context of a national defence strategy oriented towards preventing infrequent but potentially catastrophic terror attacks, is that these false-positives would overwhelm the resources of the system, as was shown in Chapter 5 in respect to the new threat matrix applied to visa-overstays. Before the problem of false-positives is addressed in detail, it is important to consider how the terror watch-lists are constructed in order to understand further how risk is understood within the context of the border.

7.5 Terrorist Watch-List Database Construction

One of the first anti-terror measures to be put in place in the United States after 9/11 was the terrorist no-fly list that was used to bar high-risk individuals from air travel both to and within the country. This list was subsequently expanded into two lists: the no-fly list and the selectee list, containing individuals who required additional inspection at the border or were of particular intelligence interest to the DHS/CBP. With the consolidation of the lists, as well as the import of names from European intelligence and law-enforcement, this was significantly expanded in 2005, containing approximately 455,002 unique identities (OIG, 2005, p. xii). This consolidation and partition, however, was not an entirely seamless process. Significant problems were identified in a 2005 DoJ audit of the initial consolidation stage, and further problems persisted in how the no-fly/selectee lists were used to match travellers' names against each list. At the database level of the TSC, the DoJ found numerous errors in both how the transfer of watch-list names took place and how these names came to be coded in terms of their threat level. At the level of the algorithm, and the process used to match air travellers against the no-fly/selectee list, this was also regarded as flawed, although ultimately tolerable by the Government Accounting Office despite the fact that the algorithms used to match travellers consistently produced high rates of false-positives. This acceptance of false-positives signifies not only a turn towards precaution, but, importantly, the evidence of a government rationale that accepts collateral damage in respect to terror prevention; that is, the sacrificing of individual rights or protections in order to provide the greater good of security as consistent with Posner and Vermeule. First, it is important to consider the dynamics of the database environment that go into the production of the watch list.

travelling through U.S. air space each day, thousands of false-positives can be expected, and indeed have occurred.

In 2005 the U.S. Department of Justice performed an internal audit of the TSC consolidated watch-list, evaluating that data quality inside of the prototype watch-list database TSDB 1A, used from March 2004 to April 2005 and the final working database TSDB 1B in January 2005 both in terms of data quality and name-matching performance (OIG, 2005). Since there was pressure on the TSC to quickly establish a consolidated terrorist watch-list, coupled with a finite budget and finite expertise – the TSC development team was hampered by a lack of computer programmers with adequate security clearance – TSDB 1A was a somewhat limited prototype. For instance, TSDB 1A was only networked in an outward direction, that is, TSDB 1A could send its watch list to the TSA or in turn be used for name matching by law enforcement and immigration through the United States; it was not, however, able to receive new names and new data from the FBI or any other intelligence agency. The only way to put new data onto TSDB 1A was to manually load a disk that would rewrite the entire system. This presented a problem for the DoJ since the constant rewriting of the entire system prevented the viewing of the data on the database within its historical context. Second, the name-matching system responsible for matching names against the watch-list used a software application that performed searches according to phonetic code by: surname, first initial of given name, along with the date, month and year, plus or minus one year, of an individual's date of birth.[115] This name-matching software also recognised nicknames associated with corresponding proper names as well; for example, a match on the surname of 'Knight' would produce several additional spellings such as 'Night' or 'Nite' (OIG, 2005). However, the DoJ found that while this matching algorithm worked well for individuals with common names within the United States, performance results dropped dramatically when matching names of individuals from Europe or the Middle East, precisely the names that the TSC were aiming to screen against. This problem due to the phonetic, or 'loose phonetic' matching performed on the database, which resulted in a number of possible results based on phonetic similarity, will be discussed further on, specifically in relation to the TSA's use of the TSC watch-list.

Table 7.5.1
Sample Rendering of the TSDB 1A Phonetic Matching Algorithm

Surname	First Initial	Pseudonym	Date of Birth
		Night	11/11/55
Knight	**F.**	**Nite**	**11/11/56**
		Nighte	11/11/57

What can be seen from this table is that while a precautionary principle allows for U.S. security to cast a wider net and attempt to pick up on any fraudulent representations of personhood – or simply data errors – held within the database, this algorithm also creates a proliferation of leads. Here the individual F. Knight, 11/11/56 as a single match or point of investigation turns into a combinatory problem whereby F. Knight 11/11/56 results in eight additional matches to clear. While this appears to be a straightforward solution for computer science, when compounded with a large dataset as well as finite counter-terrorism resources, this security approach breaks down.

TSDB 1B was developed in January 2005 with the intent to run alongside TSDB 1A until each database contained the same number of watch-list files. TSDB 1B, however, was

[115] This algorithm is represented in the table above.

designed as an intergovernmental networked database that could have files directly sent to it from the FBI, U.S. Consular offices, Interpol, the U.S. intelligence community, and state and local law enforcement. Unlike TSDB 1A, which functioned as a repository for name and date-of-birth information, 1B was built using the architecture from the FBI's TIPOFF system, which enabled multi-linguistic name searches to take place, making phonetic name matching slightly more precise, and added additional fields for threat coding. Unlike with TSDB 1A, records were sent to 1B electronically from the FBI and National Counter Terrorism Center (NCTC) with 'handling codes' or additional information pertinent to law enforcement when encountering an individual on the list. While the DoJ found fault with the crudeness of the both the database setup and matching system of 1A, the main problem was the quality of files after the transfer from the FBI/NCTC to 1B (OIG, 2005). Within FBI/NCTC, the threat level of an individual rests on a scale of 1–4 – 1 maximum threat, 4 least threatening but of interest – known as a 'handling code'. While reviewing 1B in 2005, with a database population of 109,849, the DoJ found that only 193 were given label 1, 125 given 2; while 22% of the population was code 3 and 75%, the vast majority, was code 4 'requiring the lowest level of enforcement' (OIG, 2005). Out of this population, the DoJ found 377 files without codes for handling assigned and files that were of unknown origin – they belonged neither to the FBI or NCTC databases that the TSC list was compiled from. When asked by the DoJ why the database contained so many files of such a low threat level, the TSC responded by saying that in their intelligence practises they erred on the side of caution – or, in the case of this thesis, precaution. That is, even though the vast majority of files on the watch-list were marked as significantly low-risk, they were still considered to be valuable enough targets in terms of intelligence gathering either on their own or in terms of their derived social networks.

7.5.2 TSC Terrorist Watch-List Nomination Process

The second procedure where the terrorist watch-list has been constructed is through a nomination process administered by the FBI. Since 2005 this nomination process has resulted in the addition of 3,415 names from 2005–07 divided amongst the no-fly and selectee lists. In 2008 the Office of the Inspector General (OIG) conducted an audit of this process to determine not only the standards involved in the nomination process but also if this process contributed to the inaccuracies found within the terrorist watch-list in general. What the OIG found was that, while the FBI worked in a timely fashion to submit new names to what is called the Terrorist Review and Examination Unit (TREX), of all those individuals that who were involved in ongoing terrorist investigations, the nomination process was found to have three problem areas. First, while FBI agents were quick to send new names to TREX, TREX officials responsible for reviewing the nomination packages found many of the packages to be incomplete or missing vital data. Second, under Homeland Security Presidential Directive 6,[116] the FBI was made responsible as a nominating agency to vet and

116 Homeland Security Presidential Directive/Hspd-6 - Subject: Integration and Use of Screening Information To protect against terrorism it is the policy of the United States to (1) develop, integrate, and maintain thorough,

verify all data sent to TREX on an ongoing basis in order to correct any errors that had crept in. This type of follow-up, however, was found to happen rarely, if ever. The OIG found that FBI agents themselves were unaware that there were requirements placed on data accuracy. Third, although the FBI was responsible for processing and submitting all new nominations to TREX, agents from TREX indicated that the senior FBI agents were not the only source of terrorist nomination submissions. Here the OIG found that not only was there a discrepancy taking place within the FBI itself, where frequently field agents would directly submit a nomination to TREX as opposed to first clearing this nomination with case agents; but other agencies involved in counter-terror practises – such as the ATF, BOP, DEA, USMS and USNCB – were also submitting their own nominations applications. Although it is difficult to quantify or measure just what percentage of false-positives – or false-negatives, for that matter – have occurred as a result of these procedures, it is evident that the nomination process as consistent with the faults attached to the data-collection and -mining process suffers not only from the problem of dirty data, but from old or faulty data as well. This audit also presents the question in respect to the standards and rigors of the watch-list process itself. While a valid assumption can be made that only those individuals who are truly involved in terrorist undertakings should be added to the list, this assumption is challenged by these findings in two ways. First, given that fact that FBI case agents have been circumvented not only by complementary government agencies but by their own subordinates, it raises questions about requirements necessary for watch-list nomination – different agencies could have different criteria in terms of degree for constitutes a terrorist threat. Second, the problem of dirty data reveals a watch-list process that is both untimely and haphazard, thus not only potentially creating undue false-positives but negatively impacting security actions when necessary.

The construction process of the terrorist watch-list where it is partitioned into the no-fly, selectee and criminal watch-lists can be seen to operate, according to a diagram of accountancy or enumeration, risk assessment and precaution. This argument concerning precaution can be understood more clearly if the no-fly list itself is analysed further. For instance, while the no-fly list bars individuals found on the list from boarding a plane with a U.S. destination, U.S. airport security services as of 2008 have been denied the power to arrest an individual who has been given a no-fly status if that individual is found at a U.S. airport or international airport – hence the watch list itself cannot be used in an evidentiary capacity to result in arrest (Schneier, 2005). The security expert Bruce Schneier points to this paradox whereby those individuals who have their names on the no-fly list ‘are so dangerous that they cannot board a plane to the U.S. yet so innocent that they cannot be arrested, even under the provisions of the PATRIOT Act’ (Schneier, 2005, p. 2). This, then, raises a further question concerning the ‘true’ risk or threat level of an individual placed on this list. It would

accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

be fair to assume that if an individual were placed on the no-fly list, they would not only pose a threat to human life, but as a result would warrant a response by U.S. security to detain and arrest. However, this is not always the case. Furthermore, given this situation, one might expect that the FBI would not want to place their highest-priority targets on this list, because high-priority terror suspects require evidence consistent with rule-of-law standards to be brought to justice. It appears on the surface that not only would an intervention form the no-fly list have the potential to interfere with this process since the name of an important target would have to be made known not only to the NCTC and TREX, but the watch-list itself would be sent to individual air carriers so that they could perform frontline screening. But while this logic of enumeration, prevention and precaution is at work in respect to passenger pre-screening, poor data quality and faulty algorithms have turned what could be viewed as a security asset into a security liability. This liability impacts not only individual travellers via the problem of the false-positive – where this problem is further compounded due to the fact that watch-list identification is an automated process where security officials at airports lack any way of discovering source attributions. It also impacts them in the form of false-negatives, where individuals who could be viewed as legitimate threats do not appear as such due to data errors as part of the nomination and watch-list construction process. What has amplified these two liabilities is not simply the fact that U.S. intelligence and domestic security have turned to data-mining tools, whether entity resolution or watch-list matching, as a way to track the identity of travellers entering the United States and assess risk. The liabilities come from the use of these tools as evidentiary instead of investigative.

7.6 Cases: Positives/False-Positives/False-Negatives

While it has been argued that a false-positive rate of event 0.001% within airport screening methods would contribute to unacceptably high false-positives, this does not represent a full picture in respect to the lived reality of misidentification. There have many high-profile cases of misidentifications since 2004 – for instance, the late Senator Edward Kennedy along with Representatives John Lewis and Don Young were stopped on numerous occasions as a result of matches with the no-fly list,[117] However, what is more compelling is to examine a lesser-known example from 2005 resulting in the U.S. court case known as *Ibrahim v. DHS.* On January 5, 2005, Rahinah Ibrahim, then a postgraduate student in the department of engineering at Stanford University, was identified by the no-fly list upon check-in for a flight leaving San Francisco International Airport (SFO) for Kuala Lumpur. Instead of pulling her aside for additional screening, the check-in clerk, who was notified of the watch-list match on her computer, verified the name matched the one printed on the ticket and subsequently called the airport-based San Francisco police (SFPD). When the police arrived, Ibrahim's name was again checked to see that it matched the one printed on the list and then verified by the officer in attendance, who phoned the Terrorist Screening Center in Washington, D.C., for further instructions. Here the police officer was told again that Ibrahim was on the

[117] In the case of Senator Kennedy, the same name 'Edward Kennedy' was taken from a British intelligence database that had bulked names from suspect Irish republican terrorists. With loose matching algorithms as well as a lack of contextual information regarding the individual, this example displays the problem with the security method.

list, that she was not under any circumstances to be allowed to board her flight and that she should be arrested, detained and questioned by the FBI. On the basis of this direction, Ibrahim was placed in handcuffs in the middle of the airport terminal and in front of her 14-year-old daughter, who was to accompany her on the flight. All the while, a companion, who had accompanied Ibrahim to the airport in order to provide assistance to Ibrahim, who suffered from medical complications due recent topical surgery, had asked both the flight attendant and police officers to provide Ibrahim with a wheelchair, as she was physically distressed (McManis 2006). Instead, Ibrahim was led to a holding cell at SFO where she waited for two hours in severe physical discomfort, only to have a staff paramedic provide her with medicine she required. Soon after, Ibrahim was released, but she was given no indication about how her name made it on the watch list, only that it had subsequently been removed. Ibrahim flew out of SFO to Kuala Lumpur the next day, only to find that her name remained on the list. As a result, she experienced enhanced searches prior to boarding her flight and later at a stopover in Hawaii. As a result of this experience, Ibrahim sued the DHS, the SFPD and the flight attendant who identified her name as matching one found on the watch list as well as a host of parties involved. While the SFPD admitted wrongdoing, providing Ibrahim with $225,000 in compensation, the DHS made it virtually impossible for her to mount a legal challenge against the government. What is important to note, however, that is while Ibrahim was in fact arrested and briefly detained for appearing on the watch-list, during her trial the DHS withheld evidence from the courts on grounds of national security that would have confirmed that Ibrahim was in fact on the list. This example shows not only the interaction between the analysis of predicates along with a precautionary security policy, but the lack of reasonable channels in which justice can be achieved due to, on one side, algorithmic error – appearing on the watch list while not appearing on the watch list – and one of the other national-security provisions that make it virtually impossible to mount a challenge against those agencies responsible for wrongdoing.

The second example is that of the Christmas Day 2009 attacker, Umar Farouk Abdulmutallab, who attempted to detonate explosives attached to his person on board Northwest Airlines 254 from Amsterdam as it approached Detroit, Michigan. What is interesting about Abdulmutallab, though, is that he was known to U.S. intelligence and in fact was listed in the 400,000-member TSDB that indicated possible extremist links (Napolitano, 2010). However, Abdulmutallab, who flew from Lagos, Nigeria, via Amsterdam to Detroit, passed through metal detectors at both locations, without alerting authorities that he was carrying concealed explosives. Although Abdulmutallab was not on the no-fly or selectee list, his inclusion on the larger suspect list did prompt an alert with the Customs and Border Protection in Detroit, who in fact intended to further interview him on arrival. It just happened that this interview never took place. Abdulmutallab, after attempting to detonate explosives while flight 254 was preparing to land in Detroit, was restrained by nearby air passengers, and then detained by authorities until landing. Much like with the 9/11 terror attacks, this attempted attack was viewed as a missed opportunity, or in the words of President Obama, as a ‘screw-up’ for allowing Abdulmutallab to board the flight to the United States while

containing terrorist predicates (Economist, 2010). Furthermore, it was found that Abdulmutallab's father, a wealthy and influential Nigerian businessperson and the former chairman of First National Bank of Nigeria, had informed U.S. authorities shortly before the plot transpired that his son had become radicalised in between his studies at University College London and subsequent trips to Egypt. This information, despite its origin from a credible source, was never turned into actionable intelligence. What this example shows is that data-mining tools, while seeking to fix individual identity and to assess that identity in respect to risk, can suffer not only from false-positives, but false-negatives as well.. Furthermore, due to the clandestine nature of jihadist or Islamist terror practises, where individuals blend in with civilian populations and in many instances are civilians themselves who have become radicalised, the watch-list and name-matching tools are rendered moot.

What is needed, and this is precisely what the Christmas attack called for, is greater attention paid to local intelligence from reliable sources, rather than placing an overreliance on a brittle and somewhat dysfunctional algorithmic system. This point has been highlighted by the computer security expert George Danezis in respect not only to algorithmic failure but to the fact that there are multiple ways to work around established security systems: 'These techniques (of data-mining), applied to the security domain are elusive, because they have not been designed with an intelligent adversary in mind. It is one thing to develop algorithms that try to detect rotten apples from good ones (for examples), but the rotten apples are not going to purposefully try to disguise themselves as good ones' (Danezis, 2008, p. 4).

7.7 Conclusion

This chapter reveals the explicit precautionary nature of U.S. homeland security, concentrated along the air routes travelling to and within the country. On the one hand, the argument concerning the layered function of security is supported with the use of data-analysis technologies whereby U.S. security services are able to obtain and analyse biographic, numeric and textual features pertaining to the individual crossing the border. This new mode of security analysis therefore allows a discrete form of matching of this data against terrorist watch-lists in order for U.S. security to establish thresholds of risk, and it provides further analytic insight through the practise of pattern matching against those patterns known or believed to be used by terrorists or criminals. This microscopic approach to the analysis of the individual then works to adjudicate the individual via his or her data elements in order to determine a relationship to a criminal or terrorist event, rather than cast overt suspicion on those larger population categories based strictly upon nationality, religion or ethnicity that may be believed to hold a relationship to terror. On the other hand, what is different in the procedure of watch-list matching is that while it is again primarily directed at foreign nationals, the executive decision as to whether or deny or allow entry into the country is based on weaker evidentiary standards, and in some cases technological error. The upholding of these lower standards can then be understood as a truly precautionary mechanism and can be supported by the definition of precaution provided by Ewald in

Chapter 2; that is, when there is scientific uncertainty concerning a catastrophic event, the decision on how to respond to such an event is turned into a political decision.

Figure 7.7.1 Terrorist Watch-Lists Used by the U.S. Security Services

TERRORIST-RELATED WATCH-LISTS IDENTIFIED BY THE GOVERNMENT ACCOUNTABILITY OFFICE IN APRIL 2003		
	Description	**Agency**
1	TIPOFF System	Department of State (DoS)
2	Violent Gang and Terrorist Organisations File (VGTOF)	FBI
3	Interagency Border Inspection System (IBIS)	Department of Homeland Security (DHS)
4	National Automated Immigration Lookout System (NAILS)	DHS
5	Consular Lookout and Support System (CLASS)	DoS
6	No-Fly List	DHS
7	Selectee List	DHS
8	Integrated Automated Fingerprint Identification System (IAFIS)	FBI
9	Automated Biometrics Identification System (IDENT)	DHS
10	Warrant Information Network	U.S. Marshals Service
11	Top Ten Fugitives	Department of Defense, U.S. Air Force
12	Interpol Terrorism Watch List	Department of Justice (DoJ)

Source: GAO Report Number GAO-03-322

DATABASES USED BY THE NATIONAL TERRORISM CENTER (NTC) TO SCREEN PASSENGER NAME RECORD (PNR) DATA	
1	Advanced Passenger Information System (APIS),
2	Non-Immigrant Information System (NIIS),
3	Suspect and Violator Indices (SAVI),
4	Border Crossing Information System (BCIS),
5	Department of State visa databases,
6	TECS seizure data, and
7	Terrorist watch-lists; subsets of the U.S. government's Terrorist Screening Database.

Source: CRS Report 7-5700

8. Conclusion

This thesis has sought to interrogate the new forms of governance that have been implemented under the title of 'homeland security' at the U.S. border, specifically associated with changes in surveillance of the air travel corridors to and within the U.S. as well as with the visa and immigration system. Empirically, this thesis, while aiming to address the overarching concepts of expanded sovereignty and the adoption of risk rationales post-9/11 by the U.S. executive, has also, and perhaps surprisingly, shown that the micro-practises of U.S. security – such as their construction of databases or the process through which individuals are vetted according to risk parameters, at times work against rather the towards stated policy goals. It is also notable that despite the dramatic expansion of executive power as part of the war on terror in the international area – policies of rendition, indefinite detention, the removal of habeas corpus, or the designation of 'enemy combatant' placed outside of the framework of the Geneva Conventions (Goldsmith, 2012) – that the executive over-reach has been tempered within the border zone. This is not to say that there has not been an expansion of executive power or the display of a 'state of exception' as described by Agamben, but this application of executive power at least within the context of this study has been displaced away from U.S. citizens – who maintain a covenant with the executive – and onto the foreign traveller, student or visa holder. Given this general definition of the new mode of security operative at the U.S. border post-9/11, it is instructive to return to the three questions presented in the opening chapter. While these three questions were implied within the argumentative structure of each of the empirical chapters in this text – Chapters 5, 6 and 7 – it is worthwhile to revisit each.

(1) What relationship does this new mode of security or governmentality have with the theory of the 'state of exception' and the re-emergence of sovereign power post-9/11?

As hinted at in the previous paragraph, the new mode of security governance witnessed at the U.S. border as part of the homeland security paradigm is one that contains the expression of sovereign expansion as part of domestic counter-terrorism practise. This expansion is made possible through legislative, institutional and technological innovations. These innovations can be seen as: *Legal*, the weakening of FISA with the passing of the U.S.A. Patriot act in order to allow for 'sufficient' cause in the issuance of the FISA warrant, the passing of the AUMF that gives blanket war powers to the presidency, as well as the requirement for all VWP nationals and foreign air carriers to provide identity information to U.S. security prior to departure to the U.S. *Institutional*, whereby the perceived problems of 'the wall' and the lack of intelligence sharing between security agencies led to both the consolidation of 27 domestic emergency response and immigration agencies into the DHS, in order to create synergies as well as establish a new field of intelligence pooling and sharing, as well as the movement of the FBI into collaborative role with the DHS in respect to vetting name and biometric information against data stored within FBI databases. *Technological*, here with the introduction of biometric and data-mining technology to vet and

assess individuals against watch lists and risk profiles, as well as to collect and aggregate such information to aid in current and future terrorist investigations.

These practises have also been carried out despite a high rate of false-positives or, as it has been described in the previous chapter, with the accommodation of collateral damage. How, then, is sovereign power assessed in respect to the precepts established by Agamben, namely, where there sovereign or executive has the right or authority to 'declare the exception' and step outside of legal boundaries established in normal times – and therefore act in such a way that presents the possibility of sovereign violence? Beyond the granting of additional powers to domestic intelligence and border security agencies, it has been argued that the most prevalent form of exceptionism has taken place in respect to both the collection of identity predicates from foreign nationals and the subsequent vetting procedures applied once such data is collected. This is displayed not only with the quality of the 'ban' (Bigo, 2010) of certain individuals entering the United States through the creation of no-fly lists, but also the procedures through which individuals are physically identified as threats, as in the case of *Ibrahim*. What is notable here is that not only has a practise of detention and expulsion been created – one asks why was not Ibrahim arrested and charged with a crime – but also the distribution of sovereignty beyond border security, or law enforcement and bestowed upon airline employees. Although there is a clear expansion of sovereign power at the border, it has been shown that pure sovereign power or the unfettered expansion of the executive has been curtailed by endogenous factors – constitutional protections, competition between various domestic intelligence branches, the proliferation of dirty data throughout security databases, and the establishment of different standards for the collection and sharing of data – and exogenous factors – pressure from the European Commission, or economic pressure from VWP nations in order to help maintain the U.S. economy. The governmentality of the post-9/11 U.S. border security, if it can be understood that governmentality stands for the 'rationales' of governance, is one that performs according to three competing set of interests. The first is expansion and flexibility – much as the Schmittian discourse suggests concerned unbounded executive power. The second is curtailment, where this expansive sovereign power is both internally and externally constrained where there is a successive interplay between expansion and the tests of curtailment brought forward by legal or political challenges. Finally, the third attribute of this form of governmentality is one of self-defeat. That is, the empirical practises associated with the use of networked and identity-based technologies, while allowing for new and expansive police powers, also create new layers of complexity and ultimately problems that deviate from counter-terrorism goals as such.

However, beyond these three attributes which place U.S. homeland security practises squarely within a paradigm of governmentality, it does signal a new form of security that is attempting to grapple with two competing rationalities concerning the event. These competing rationalities propose on the one hand the management of the event, much like crime or mortality at a regular and predictable rate that is common quality of industrialised

society. As a result, it was shown in Chapter 5 concerning the economics of border security, that post-9/11 border-security measures have been attentive to the demands of economic efficiency within the border zone in order to allow for steady rates of flow, even with the understanding that there will be a minimum level of delinquency. Counter to this rationale that can be described as a 'limiting bandwidth' is the rationale proposed primarily by Beck and Ewald, where the threat of terrorism is understood as a discrete catastrophic risk. The event itself rests within the long-tail of the probability distribution. As a result, the new form of governmentality at the border, not only possesses the three qualities mentioned above, it also rests within dis-equilibrium in respect to the difference in methods of governance required to approach each type of event. Within U.S. border security, both strategies are taken up: those strategies to monitor and manage the threat that can be placed within a limiting frequency or set of bounds; and those strategies that are ultimately precautionary in nature that seek to be in state of readiness – such as PNR or biometric analysis – in order to deflect the extremely unlikely event of a catastrophic terrorist attack. It can be seen, however, that these two rationales are in competition with one another and lead to the application of at times the wrong method for the wrong type of event – such as in the case of *Ibrahim* (incorrectly understood as catastrophic) and *Abdulmutallab* (incorrectly understood to rest within a limiting bandwidth – i.e., as a normal securitised air traveller).

(2) How have biometric, data-mining and database technologies impacted and shaped this new form of security? What new modes of security and population management do these technologies make possible? What are their limitations?

As it has been described primarily in Chapters 6 and 7, the primary impact that biometric and data-mining technology has had on security governance post-9/11 as part of the strategy of homeland security, has been to fix individual identity – and thereby create a basis for tracking and monitoring that identity over time – and to perform secondary and tertiary processes with this identity information in order to aid current and future counter-terrorism operations. Beyond the creation of identity profiles that can be added to and made more robust over the lifetime of an individual, granted that they frequently fly to the United States – or to Europe, for that matter – the secondary and tertiary processes are the key conceptual and technological difference from previous forms of identity-based surveillance. That is, with the integration of suspect databases, law enforcement are not only able to match this identity information against a larger population, they can continue to match this information against such a database over time and as the population changes. Combined with a digital networked infrastructure that can be projected globally, this security practise is able to extend the field of governance in respect to the management of such threats – whether this extension is throughout the 36 nations that make up the VWP or within the ever-shifting U.S. theatre of war.

However, these new security practises and security assets – identity information – passed on to U.S. homeland security agencies, as displayed in Chapter 7, come with inherent risks. These risks are the most severe in respect to false-positives. While false-positives can be

seen as an acceptable consequence for the executive to bear, both in terms of increased expenditures in staffing and technology to clear such errors as well as litigation costs from those individuals who were wrongfully accused, it also has an ethical or human expense that is overlooked. This ethical element is characterized precisely in the use of biometric and data-mining analysis as evidentiary rather than investigative tools. That is, since each is bound with a set of algorithmic and database processes that results in a binary declaration on entrance to the United States or whether or not an individual should be questioned and detained, the individual who happens to be caught within this circumstance confronts a system that lacks transparency, fairness and recourse. The question as to why one individual versus another has ended up on the watch list not made public, nor is there full disclosure of what is held on the data-file of the individual and whether it is, for instance, inaccurate. In a recent conversation with a colleague, Matthew Bishop of the Economist,[118] it was expressed that Bishop's brother was planning on travelling to the U.S. from the U.K. to spend a month-long holiday but was barred from entry into the country (Bishop, 2011). The reason for the ban on travel was due to an element on his personal file that indicated that he had been arrested, but not charged, at a student protest in Britain some 19 years ago. This element of dirty or de-contextualised data that is sealed from public scrutiny and recourse will only become exacerbated as governments come to collect more and more data.

(3) How effective is U.S. homeland and border security in respect to its stated aims of counter-terrorism?

This final question is perhaps the most difficult to answer since it elicits a response based upon measurement, something that it was argued in Chapter 3 was very difficult to do. While there are certain metrics that can be attained for terror-related actions in the courts – for instance, according to research conducted by NYU's Center for Law and Security (CLS), over the decade following 9/11 approximately 300 terrorist prosecutions were carried out, where one third of these prosecutions took place during the first two years of the Obama administration (Greenberg, 2011, p. 3). There is a lack of evidence regarding how many suspected terrorists have been kept from travelling to the U.S. by US-VISIT and the analysis of PNR. Despite this lack of concrete evidence, the CLS has further maintained that the six[119] most serious terrorism attempts on the U.S. since 9/11 had relationships to Pakistan and Yemen, and that three of the six had a connection with U.S.-born Al Qaeda operative Anwar-al-Awlaki, who was killed by a U.S. drone attack in Western Yemen in 2011 (Greenberg, 2011, p. 3). What this suggests is that despite the argument by the U.S. Department of State that the core of Al Qaeda is 'weakening' there still exists the logistical capability and ideological pull to concoct terrorist plots and schemes from terrorist safe

[118] Matthew Bishop, Managing Editor for the America's. The Economist.
[119] Faisal Shahzad – Times Square Bomber; Najibullah Zazi – intended to plant explosives in the NYC subway; Umar Farouk Abdulmutallab – Christmas Day bomber; David Coleman Headley – American-born operative with Lashkar-e-Taiba, who conspired in 2008 Mumbai attack, arrested for a plot against a Danish newspaper; Major Nidal Hasan – Fort Hood shooter who killed 13 soldiers; Carlos Bledsoe – Muslim convert who wounded one soldier and killed another at a recruiting station.

havens as well as to encourage Muslim Americans already in the country to carry out acts of violence (Benjamin, 2011, p. 1). How then can this question be answered?

Clearly a threat remains, however; this question perhaps can be addressed from another angle in order to provide insight into present and future governance at the border. The overhaul of security infrastructure at the U.S. border has involved the full-scale overhaul of the visa, immigration and travel system into the United States where multiple security layers have been employed. Here four dominant security layers have been identified, although an even wider analysis of homeland security could also include additional layers towards the prevention of money laundering, bio- and nuclear terrorism, and actions to prevent terrorist financing. While this overhaul is understood to place emphasis on the analysis of foreign nationals, it fails to satisfy security concerns regarding either home-grown security – radicalisation of U.S. citizens themselves – or simple border crossing into the United States from Mexico or Canada. As a result, from the perspective of this research it is reasonable to anticipate that beyond the political battle for increased control of citizen data by foreign blocs such as the European Union as in the case of PNR, in the event of another terrorist attack within the United States, U.S. security would be motivated to perform increased surveillance of U.S. citizens. Nonetheless, post-9/11 border security has become not only the new standing paradigm for U.S. security practises but the model that other member states of the VWP – Great Britain, Japan, the European Union – who have come to employ similar methods at their own frontiers, each to determine who can pass through as a friend, or who is barred as an enemy.

❖ ❖ ❖

Works Cited

United States of America v. Truong Dinh Hung (1979).

12.2, J., 1992. *KJV Pew Bible.* King James Version ed. s.l.: Holman Bible Publishers.

9/11 Commission, 2005. *Law Enforcement, Counterterrorism and Intelligence Collection in the United States Prior to 9/11,* Washington, D.C.

9/11 Commission, 2004. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States,* Washington, D.C.: Government Printing Office.

9/11 Commission, 2004. *9/11 Commission Report,* Washington, D.C.: Government Printing Office.

9/11 Commission, 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States – Executive Summary,* Washington, D.C.: The National Commission on Terrorist Attacks Upon the United States.

Agamben, G., 1998. *Homo Sacer: Sovereign Power and Bare Life.* Stanford: Stanford University Press.

Agamben, G., 2005. No to Biometrics. *Le Monde diplomatique*, 6 December.

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

Agamben, G., 2006. *The State of Emergency,* Paris: Centre Roland Barthes.

Al-Haramain Islamic Foundation et al v Bush (2010).

Alvarez, L., 2010. Meet Mikey, 8: U.S. Has Him on Watch List. *The New York Times*.

Anderson, B., 1983. *Imagined Communities: Reflections on the Origin and Spread of Nationalism.* London: Verso.

Aradau, C. & Munster, R. v., 2007. 'Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future'. *European Journal of International Relations,* 13(1), p. 27.

Ashcroft, J., 2003. *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection,* Washington, D.C.

Bazan, E. & Elsea, J., 2006. *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Inforamtion,* Washington, D.C.: CRS.

Beck, U., 2003. 'The Silence of Words: On Terror and War'. *Security Dialogue,* 34(3), p. 13.

Beck, U., 2006. 'Living in the World Risk Society'. *Economy and Society,* 35(3), p. 18.

Beck, U., 2009. 'Critical Theory of World Risk Society: A Cosmopolitain Vision'. *Constellations,* 16(1), p. 20.

Benjamin, D., 2011. *Al-Qa'ida and Its Affiliates.* [Online]
Available at: http://www.state.gov/j/ct/rls/rm/2011/161895.htm

Bigo, D., 2010. The Ban and the Exception: Discussing the 'state of exception'. In: *Policing Insecurity Today: Defense and Internal Security.* s.l.: Palgrave MacMillan.

Bigo, D. & Guild, E., 2005. *Controlling Frontiers: Free Movement into and within Europe.* Aldershot: England.

Bigo, D. & Guild, E., 2005. Policing at a Distance: Schengen Visa Policies. In: *Controlling Frontiers: Free Movement into and within Europe.* Aldershot: Ashgate.

Binmore, K., 2007. *Playing for Real: A Text on Game Theory.* Oxford: Oxford University Press.

Bishop, M., 2011. *My brother needs non-immigrant visa for family holiday Aug 1st. Interview date you offer is after vacation. What can we do?.* [Online]
Available at: http://199.16.156.11/mattbish/status/224866297744343041

Bobbitt, P., 2009. *Terror and Consent: The Wars of the Twenty-First Century.* New York: Anchor Books.

Boede, L. Risk and the War on Terror. In: *Risk and the War on Terror.*

Bremmer, I., 2012. *Top Risks of 2012,* New York: The Eurasia Group.

BTF, 2007. *Biometrics Task Force – Annual Report FY07,* Washington, D.C. : Department of Defence.

Burchell, G., 1991. Peculiar Interests: Civil Society and Governing 'the system of natural liberty'. In: C. G. P. M. Graham Burchell, ed. *Foucault Effect: Studies in Governmentality, with Two Lectures by and an Interview with Michel Foucault.* 1 ed. Chicago: The University of Chicago Press, p. 318.

Buzan, B., Wæver, O. & Wilde, J. d., 1998. *Security: a new framework for analysis.* Boulder (Colorado): Lynne Rienner Publishers.

Canguilhem, G., 2003. The death of man, or exhaustion of the cogito? In: G. Gutting, ed. *Cambridge Companion to Foucault.* 2 ed. Cambridge, U.K.: Cambridge University Press.

Castel, R., 1991. From dangerousness to risk. In: *The Foucault Effect: Studies in Governmentality.* London: Havester Wheatsheaf.

CEC, 2009. *Fifth Report from the Commission to the Council and the European Parliament: on certain third countries' maintenance of visa requirements.* Brussels: European Commission.

Chertoff, M., 2005. *Remarks for Secretary Michael Chertoff U.S. Department of Homeland Security George Washington University Homeland Security Policy Institute.* Washington, D.C.: Department of Homeland Security.

Chertoff, M., 2006. *Remarks by Homeland Security Secretary Michael Chertoff on Protecting the Homeland: Meeting Challenges and Looking Forward.* Washington, D.C.: Department of Homeland Security.

Chertoff, M., 2006. *Secretary of Homeland Security Michael Chertoff: Secure Borders and Open Doors in the Information Age,* Washington, D.C.: U.S. White House.

Chertoff, M., 2006. *Testimony of Secretary Michael Chertoff,* Washington, D.C.: Department of Homeland Security.

Chertoff, M., 2007. *Remarks by Homeland Security Secretary Michael Chertoff at the Christian Science Monitor Breakfast.* [Online]
Available at: www.dhs.gov
[Accessed 2011].

Chertoff, M., 2007. *Secretary Chertoff's Remarks to European Parliament.* Washington, D.C., Brussels, Department of Homeland Security.

Chertoff, M., 2008. *Remarks by Homeland Security Secretary Michael Chertoff at Harvard University.* Cambridge (Massachusetts): Department of Homeland Security.

Chertoff, M., 2008. *Remarks by Homeland Security Secretary Michael Chertoff at Harvard University.* Cambridge (Massachusetts): Department of Homeland Security.

Clausewitz, C. v., 1984. *On War.* Indexed Edition ed. Princeton, NJ: Princeton University Press.

Cole, S., 2001. *Suspect Identities: A History of Fingerprining and Criminal Identification.* Cambridge, Mass.: Harvard University Press.

Cole, S., 2001. *Suspected Identities: a history of fingerprinting and criminal identification.* Cambridge, Massachusetts: Harvard University Press.

Congress, 2001. *Authorization for Use of Military Force,* Washington, D.C.

Council of European Union, 2007. *Processing and transfer of passenger name record data by air carriers to the United States Department of Homeland Security – 'PNR',* Brussels: Council of the European Union.

Danezis, G., 2008. *Interview with George Danezis* [Interview] 2008.

Daston, L., 1988. *Classical probability in the Enlightenment.* Princeton, N.J.: Princeton University Press.

Daugman, J., 2003. The Importance of Being Random: Statistical Principles of Iris Recognition. *Pattern Recognition,* Volume 36, p. 13.

Daugman, J., 2005. *Recognizing Persons by Their Irises,* Cambridge, U.K.: University of Cambridge.

Daugman, J., 2006. *Biometrics and Uniqueness.* London, Biometrics 2007:London.

Daugman, J. & Kabatoff, M., 2008. Pattern Recognition – Biometrics, Identity and the State: An Interview with John Daugman. *Biosocities,* Volume 1, p. 3.

Deleuze, G., 1988. *Foucault.* Minneapolis: University of Minnesota Press.

DHS, 2002. *The Student and Exchange Visitor Information System (SEVIS) Privacy Impact Assessment,* Washington, D.C.: Department of Homeland Security.

DHS, 2003. *Position Paper: IDENT Implementation for U.S. Visit. Why Use IDENT Versus Developing and New Solution?,* Washington, D.C.: Department of Homeland Security.

DHS, 2008. *Brief Documentary History of the Department of Homeland Security 2001–2008,* Washington, D.C.: Department of Homeland Security.

Dodd, V., 2011. *Asian people 42 times more likely to be held under terror law.* [Online]
Available at: http://www.guardian.co.uk/uk/2011/may/23/counter-terror-stop-search-minorities

Economist, 2010. *Another war president, after all: After the Christmas 'screw-up', new priorities in the White House.* [Online]
Available at:

http://www.economist.com/node/15213339?zid=312&ah=da4ed4425e74339883d473adf5773841

Economist, T., 2010. Stop stop and search: Another reverse for Labour's tough laws. *The Economist,* p. 1.

Eldridge, T. R. et al., 2004. *9/11 and Terrorist Travel: Staff Report of the National Comission on Terrorist Attacks Upon the United States,* Washington, D.C.: NCT.

Elias, B., 2005. *Homeland Security: Air Passenger Prescreening and Counterterrorism,* Washington, D.C.: Congressional Research Service.

Enders, W. & Sandler, T., 2006. *The Political Economy of Terrorism.* Cambridge: Cambridge University Press.

ENFORCE/IDENT PMO, 2003. *Position Paper, IDENT Implementation for U.S. VISIT, Why Use IDENT Versus Developing a New Solution?,* Washington, D.C.: Department of Homeland Security.

EPIC, 2008. *Foreign Intelligence Surveillance Act Orders 1979–2007,* Washington, D.C.: Electronic Privacy Information Center.

Epstein, C., 2008. Embodying risk: Using biometrics to protect the borders. In: Louise Amoore, ed. *Risk and the War on Terror.* London: Routledge.

Eric Lichtblau, 2005. Spy Agency Mined Vast Data Trove, Officials Report. *The New York Times*.

Ericson, R., 2008. The state of preemption: Managing terrorism risk through counter-law. In: M. d. G. Louise Amoore, ed. *Risk and the War on Terror.* London: Routledge.

Ericson, R. V., 2008. The State of Preemption: Managing Terrorism Risk through Counter Law. In: Louise Amoore, ed. *Risk and the War on Terror.* New York: Routledge.

Ervin, C., 2003. *Department of Justice, Office of the Inspector General Issues Report on the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of September 11,* Washington, D.C.

European Parliament v Council of the European Union (2006).

Ewald, F., 1991. Insurance and Risk. In: *The Foucault Effect: Studies in Governmentality.* London: Harvester Wheatsheaf.

Ewald, F., 2002. 'The return of Descartes' malicious demon: an outline of a philosophy of precaution'. In: T. B. a. J. Simon, ed. *In Embracing Risk.* Chicago: University of Chicago Press.

FBI, 2002. *Joint Inquiry into the Events of September 11, 2011,* Washington, D.C.: Federal Bureau of Investigation.

FBI, 2005. *Fact Sheet: Justice Department Counter-Terrorism Efforts since 9/11,* Washington, D.C.: Federal Bureau of Investigation.

FBI, 2011. *Integrated Automated Fingerprint Identification System (IAFIS),* Washington, D.C.: The FBI Federal Bureau of Investigation.

Federal Reporter, 2002. *United States Foreign Intelligence Surveillance Court Review,* Washington, D.C.: Foreign Intelligence Surveillance Court.

Feinstein, D., 2001. *Using Technology to Keep Terrorists Outside of the United States,* Washington, D.C.: United States Senate.

Fergusson, I. F., 2006. *United States-Canada Trade and Economic Relationship: Prospects and Challenges,* Washington, D.C.: U.S. Congress.

Ford, J. T., 2002. *Border Security: Visa Processes Should be Strengthened as an Anti-terrorim Tool,* Washington, D.C.: GAO.

Ford, J. T., 2006. *Border Security: Strong Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program,* Washington, D.C.: GAO.

Foucault, M., 1972. *The Archeology of Knowledge.* New York: Pantheon Books.

Foucault, M., 1973 (2003). *The Birth of the Clinic: An Archeology of Medical Peception.* London: Taylor & Francis Group.

Foucault, M., 1984. Nietzsche, Genealogy, History. In: P. Rabinow, ed. *The Foucault Reader.* London, New York: The Penguin Group, pp. 76–100.

Foucault, M., 1997. Polemics, Politics and Problematizations. In: P. Rabinow, ed. *Ethics: Essential Works of Foucault.* New York: The New Press.

Foucault, M., 2007. *Security, Territory, Population: Lectures at the College de France 1977–1978.* New York: Picador.

GAO, 2002. *Homeland Security: INS Cannot Locate Many Aliens because it Lacks Reliable Address Information,* Washington, D.C.: U.S. Government Accountability Office.

GAO, 2007. *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain,* Washington, D.C.: GAO.

GAO, 2007. *Homeland Security: US-VISIT Has not fully met expectations and longstanding program management challenges need to be addressed,* Washington, D.C.: United States Government Accountability Office.

GAO, 2011. *Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies,* Washington, D.C.: Government Accountability Office.

Gearty, C., 2010. *Escaping Hobbes: Liberty and Security for Our Democractic (Not Anti-Terrorist) Age.* London: LSE.

GOA, 2006. *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to be Implemented,* Washington, D.C.: Government Accountability Office.

Goede, L. A. a. M. d., 2008. Risk and the War on Terror. In: L. A. a. M. d. Goede, ed. *Risk and the War on Terror.* London: Routledge, p. 286.

Goldsmith, J., 2012. *Power and Constraint: The Accountable Presidency after 9/11.* New York: W.W. Norton & Company.

Goodman, C. & Verne, T. L., 2006. *Implications of Eliminating the Visa Waiver Program,* Washington, D.C.: GAO.

Greenberg, K., 2011. *Terrorism Trial Report Card: September 11, 2001 – September 11, 2011,* New York: New York University: The Center for Law and Security.

Grewe, B., 2004. *The Legal Barriers on Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations,* Washington, D.C.: The Commission on Terrorist Attacks Upon the United States.

GTD, 2011. [Online]
Available at: http://www.start.umd.edu

Hacking, I., 1990. A Tradition of Natural Kinds. *Philosophical Studies,* 61(18).

Hacking, I., 1990. *The Taming of Chance.* Cambridge: Cambridge University Press.

Hacking, I., 1999. *The Social Construction of What.* 2 ed. Cambridge, Mass.: Harvard University Press.

Hacking, I., 2005. The looping effects of human kinds. In: *Historical Ontology.* Cambridge, Mass.: Harvard University Press, p. 288.

HANSARD, 2007. *Evidence heard on the UK Borders Bill – March 2,* London, UK: HANSARD.

Hart, G. & Rudman, W., 2001. *Road Map for National Security: Imperative for Change – The Phase III Report of the U.S. Commission on National Security,* Washington, D.C.: The United States Commission on National Security for the 21st Century.

Heng, Y.-K. & McDonagh, K., 2009. *Risk, Global Governance and Security: The Other War on Terror.* London: Routledge.

Hite, R., 2007. *HOMELAND SECURITY: US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to be Addressed,* Washington, D.C.: GAO.

Hite, R. C., 2006. *Visitor and Immigrant Status program Operating but Management Improvements are Still Needed,* Washington, D.C.: Subcommittee on Homeland Security: Committee on Appropriations.

Hoefer, M., 2009. *2008 Yearbook of Immigration Statistics: Office of Immigration Statistics,* Washington, D.C.

Homeland Security Act (2002).

Ibrahim v. Department of Homeland Security (2006).

III, H. T., 2006. *Privacy Impact Assessment for the Interim Data Sharing Model (iDSM) for the Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability Project,* Washington, D.C.: Department of Homeland Security.

Immigration and Nationality Act (1996).

Inspector General, 2004. *Follow-up Review of the Status of IDENT / IAFIS Integration,* Washington D.C.: U.S. Department of Justice.

IRTPA, 2004. *Intelligence Reform and Terrorism Prevention Act,* Washington, D.C.: Public Law 108–458.

John W. TERRY, Petitioner, v. STATE OF OHIO (1968).

Johnson, L. K., 2008. Establishment of modern intelligence accountability. In: R. A. Miller, ed. *U.S. National Security, Intelligence and Democracy: From the Church Committee to the War on Terror.* London: Routledge.

Jonas, J., 2007. *Identity Analytics: An Interview with Jeff Jonas* [Interview] (1 April 2007).

Justice, D. o., 2008. *Fact Sheet: Justice Department Counter-Terrorism Efforts since 9/11,* Washington, D.C.

Kabatoff, M., 2005. *Biometrics and the UK's Identity Cards Legislation,* London: Institute of Public Policy Research.

Keating, D. D. P. a. M., 2008. *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective.* Cambridge, U.K.: Cambridge University Press.

Kieffer, J. & Trissell, K., 2010. *DoD Biometrics – Lifting the Veil of Insurgent Identity,* Washington, D.C.: ARMT AL&T.

Landes, W., 1978. An Economic Study of U.S. Aircraft Hijacking. *Journal of Law and Economics,* 21(1), p. 33.

Leahy, P., 2002. *The Enhanced Border Security and Visa Entry Reform Act,* Washington, D.C.: U.S. Government Printing Office.

Lipton, E., 2009. *U.S. Intensifies Air Screening for Fliers From 14 Nations.* [Online] Available at: http://www.nytimes.com/2010/01/04/us/04webtsa.html?_r=1&scp=4&sq=2009%20december,%20passenger%20screening,%20iran,%20yemen%20somalia&st=cse

Lords, H. o., 2007. *The EU/US Passenger Name Record (PNR) Agreement: Report with Evidence,* London: The Stationary Office Limited .

Lyon, D., 2002. Everyday Surveillance: Personal data and social classifications. *Information Communication & Society,* 5(2), p. 17.

Lyon, D., 2002. Everyday Surveillance: Personal data and social classifications. *Information, Communication and Society,* 5(2), p. 17.

Mansfield, T., Kelly, G., Chandler, D. & Kane, J., 2001. *Biometric Product Testing Final Report,* Middlesex, UK: CESG/BWG Biometric Test Programme.

Marx, G. T., 2001. Identity and Anonymity: Some Conceptual Distinctions and Issues for Research. In: J. Caplan & J. Torpey, eds. *Documenting Individual Identity.* Princeton, N.J.: Princeton University Press.

Matsuda, M. K., 1996. *The Memory of the Modern.* Oxford: Oxford University Press.

Meek, J. G., 2008. Michael Chertoff's deepest fears: Terrorists entering U.S. from Canada. *New York Daily News*.

Napolitano, J., 2010. *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack,* Washintgon, D.C.: Department of Homeland Security.

Napolitano, J., 2011. *Remarks by Secretary Janet Napolitano at Jackson Institute, Yale University,* New Haven: Department of Homeland Security.

NIC, 2007. *The Terrorist Threat to the Homeland,* Washington, D.C.: NIC.

Nissenbaum, H., 2001. How Computer Systems Embody Values. *Computer,* p. 3.

NSHS, 2007. *"National Strategy for Homeland Security',* Washington, D.C.: Department of Homeland Security.

OAD, 2010. *New Oxford American Dictionary.* 3 ed. New York: Oxford University Press.

OIG, 2005. *Review of the Terrorist Screening Center,* Washington, D.C.: Office of the Inspector General.

Posner, R. A., 2006. *The Reorganization of U.S. Intelligence Systems after One Year,* Washington, D.C.: American Enterprise Institute for Policy Research.

Project, L. I., 2006. *Response to written submission by John Daugman,* London: House of Commons.

Przeworski, A., 2000. *Democracy and Development: political institutions and material well-being in the world 1950-90.* Cambridge, U.K.: Cambridge University Press.

Rehnquist, W. H., 2000. *All the Laws but One: Civil Liberties in Wartime.* New York: Vintage Books.

Ridge, T., 2005. *Remarks for Secretary Tom Ridge, U.S. Department of Homeland Security.* London: London School of Economics.

Rose, N., 2000. Government and Control. *The British Journal of Criminology,* 40(2), pp. 321–339.

Rose, N. & Miller, P., 1991. Political power beyond the state: problematics of government. *British Journal of Sociology,* p. 33.

Rose, N., O'Malley, P. & Valverde, M., 2009. *Governmentality.* 94 ed.

Rose, N. & Rabinow, P., 2003. *Thoughts on the Concept of Biopower Today.*

Rosenzweig, P. & Jonas, J., 2005. *Correcting False Positives: Redress and the Watch List Conundrum,* Washington, D.C.: The Heritage Foundation.

Rumsfeld, D., 2002. *Memorandum for Chairman of the Joint Chiefs of Staff,* Washington, D.C.: Department of Defense.

Schmitt, C., 1996. *The Concept of the Political.* Chicago: University of Chicago Press.

Schmitt, C., 2004. *Legality and Legitimacy.* Chapel Hill: Duke University Press.

Schmitt, C., 2006. *Political Theology: Four Chapters on the Concept of Sovereignty.* 1 ed. Chicago: University of Chicago Press.

Schneier, B., 2005. *Secure Flight News.* [Online]
Available at: http://www.schneier.com/

Schneier, B., 2008. *Schneier on security.* Indianapolis(Indiana): Wiley Publishers.

Sengoopta, C., 2003. *Imprint of the Raj: How Fingerprinting was Born in Colonial India.* London: MacMillan.

Sengoopta, C., 2004. *Imprint of the Raj: How fingerprinting was born in colonial India.* London: Pan Macmillan.

Shane, S., 2011. *As Regimes Fall in Arab World, Al Qaeda Sees History Fly By.* [Online]
Available at: http://www.nytimes.com/2011/02/28/world/middleeast/28qaeda.html

Shapiro, I., Smith, R. M. & Masoud, T. E., 2004. *Problems and Methods in the study of politics.* Cambridge, U.K.: Cambridge University Press.

SITNHR, 2004. *Visa Waiver Program and the Screening of Potential Terrorist,* Washington, D.C.: U.S. Government Printing Office.

Skinner, Q., 2002. *Visions of Politics: Volume 3, Hobbes and Civil Science.* 2 ed. Cambridge: Cambridge University Press.

Skinner, R. L., 2005. *Review of the Immigration and Custom's Enforcement's Compliance Enforcement Unit,* Washington, D.C.: Department of Homeland Security.

STTGI, 2002. *The Role of Technology in Preventing the Entry of Terrorists into the United States,* Washington, D.C.: U.S. Government Printing Office.

Taipale, K., 2003. Data-Mining and Domestic Security: Connecting the Dots to Make Sense of Data. *The Columbia Science and Technology Law Review,* 5(83).

Taipale, K., 2006. Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance. *NYU Bulletin on Law and Security,* 7(6).

Thorp, A., 2007. *The UK Borders Bill – Research Paper,* London, UK: House of Commons Library.

Transportation, U. D. o., 2001. *Hijacking Data World Wide – 1970–2000,* Washington, D.C.: Federal Aviation Administration.

UK Home Office, 2004. *Identity Cards Bill Regulatory Impact Assessment,* London, UK: UK Home Office.

USA Patriot Act (2001) 107th Congress, 1st Session, H.R. 3162.

USDOJ/OIG, 2000. *The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of Its IDENT Automated Fingerprint System,* Washington, D.C.: Office of the Inspector General.

USDT, 2001. *Hijackings Worldwide: 1970–2000,* Washington, D.C.: Federal Aviation Administration.

Vermeule, A. & Posner, E., 2007. *Terror in the Balance: Security, Liberty and the Courts.* Oxfored: Oxford University Press.

Wayman, J., Jain, A., Maio, D. & Maltoni, D., 2005. *Biometric Systems Technology, Design and Performance Evaluation.* London: Springer-Verlag.

Wayman, J. L., 2000. A Definition of Biometrics. In: *National Biometric Test Center: Collected Works 1997–2000.* San Jose: San Jose State University.

Wayman, J. L., 2000. Fundamentals of Biometric Authentication Technologies. In: *National Biometric Test Center Collected Works.* San Jose: San Jose State University.

Wayman, J. L., 2000. Generalized Biometric Identification System Model. In: *National Bioetric Test Center Collected World 1997–2000.* San Jose: San Jose State University.

Wayman, J. L., 2007. *Biometrics and Security* [Interview] (13 March 2007).

Weich, R., 2010. *Applications for Electronic Surveillance Made During Calendar Year 2009,* Washington D.C.: U.S. Department of Justice.

Westphal, C., 2009. *Data-mining for Intelligence, Fraud and Criminal Detection: Advanced Analytics and Information Sharing Technologies.* Boca Raton: CRC Press, Taylor and Francis Group.

Yoo, J., 2006. *War by Other Means: An Insider's Account of the War on Terror.* New York: Atlantic Monthly Press.

Yoo, J. & Sulmasy, G., 2007. Counterintuitive: Intelligence Operations and International Law. *Michigan Journal of International Law,* p. 28.

Zeckhauser, R. & Zaluar, A., 2002. *The World of Trans-National Threats,* Cambridge, Mass.: Harvard University.

Zittrain, J., 2006. Searches and Seizures in a Networked World. *Harvard Law Review Forum,* 119(83), p. 13.

List of Acronyms (Alphabetical)

API	Advanced Passenger Information
APIS	Advanced Passenger Information System
CEU	Compliance Enforcement Unit
CAPS	Computer Assisted Aviation Pre-screening System
CBP	Customs and Border Control
CLASS	Consular Lookout and Support System
DHS	Department of Homeland Security
DoJ	Department of Justice
ePassport	Electronically enabled, machine readable passport
ESBA	Enhanced Border Security Act 2002
ESTA	Electronic System for Travel Authorization
FAA	Federal Aviation Authority
FBI	Federal Bureau of Investigation
FISC	Foreign Intelligence Surveillance Court
FISA	Foreign Intelligence Surveillance Act (1978) Amended 2004
FTTTF	Foreign Terrorist Tracking Task Force
HS	Homeland Security
ICAO	International Civil Aviation Organization
ICE	Immigration and Customs Enforcement
INA	Immigration and Nationality Act
INS	Immigration and Naturalization Service
IRTPA	Intelligence Reform and Terror Prevention Act
JTTF	Joint Terrorism Task Force
NAILS	National Automated Integrated Lookout System
NSA	National Security Agency
NCTC	National Counter Terrorism Center
OAED	Oxford American English Dictionary
OIC	Office of the Inspector General
OIPR	Office of Intelligence Policy Review
OLC	Office of Legal Council
PoW	Prisoner of War
PNR	Passenger Name Record
SEVIS	Student and Exchange Visitor Information System
TECS	Treasury Enforcement Communications System
TREX	Terrorist Review and Examination Unit
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
USA PATRIOT ACT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VWP	Visa Waiver Program
WoT	War on Terror
IAFIS	Automated Fingerprint Identification System
IDENT	Automated Biometric Identification System

Appendix 1

3.2.3 Research Design: Origins, Selections and Obstacles

While a problem-based approach is taken in this research project, it is important to understand how not only the research question but also research sites were identified and structured with coherence. The research question had its origins in the master's thesis work that I carried out at the University of California San Diego.[120] In 2003, I became interested in the visual representations of state surveillance practises, primarily associated with airports, and with this interest, I began to research U.S. congressional documents related to post-9/11 U.S. homeland-security practises. Here I fortuitously stumbled upon a 2002 congressional document titled 'The Role of Technology in Preventing the Entry of Terrorists into the United States' authored by the U.S. Congressional Subcommittee on Technology, which contained the meeting minutes from the October 12, 2001, meeting by the Subcommittee on Technology, Terrorism and Government Information (STTGI, 2002). What was surprising and remarkable about this document was that it outlined three important problematics to become associated with the overall U.S. approach to homeland security: (i.) that the 9/11 terror attacks were not simply an assault from a determined foe bent on causing destruction to the United States but that Al Qaeda took advantage of vulnerabilities within the U.S. visa and immigration system in order to carry out a successful attack; (ii.) that there was a lack of coordination and information sharing within the law-enforcement, intelligence community and visa and immigration system that could have led to the disruption of the attacks; and (iii.) not only was new policy and legislation required to prevent these types of terror attacks from taking place in the future, identity-based technologies – in the case of this document, biometrics – were viewed as a solution to this problem. Beyond the identification of key conclusions about 9/11 and assumptions about what the solution would be, this document acted as a blueprint that U.S. homeland security would follow, culminating in US-VISIT within two years of its publication. What was of further interest and potentially grounds the use of the biometrics at the border was their ability to both verify identity and, importantly, track recidivist criminals within a border situation applied most notably along the U.S./Mexico border (STTGI, 2002). This document did not simply represent a profound shift within U.S. security policy – from one that allowed the individual to enter the United States by passing a single threshold to one that performs greater analysis and tracking of the individual at the border – but it outlined a transformative potential that engaged policy, technology and institutional practises that would materially transform how the United States operated its borders, primarily in respect to trans-Atlantic air travel.

The research question that comes out of the problematic articulated in the congressional document was not fully realised until 2006. Prior to 2005 I had moved from Southern California to London and become involved in the debates concerning the proposed U.K. Identity Cards programme, where legislation was passed by the U.K.'s Labour Government that called for the creation of a national identity database to store an identity record of every

[120] This thesis work was presented in the summer of 2004 in a solo exhibition at Monitor Gallery, Rome.

British national and visitor. This involvement culminated in the writing of a white paper on the potential implications of such a scheme for the Institute of Public Police Research (IPPR), a New Labour–funded think tank (Kabatoff, 2005). The debate surrounding this bill concerned not only the creation of a national identity card for the U.K. – something that was used during World Wars I and II – but that such a scheme would run counter to a notion of British liberalism – the 'free Englishman' and so forth – that was developed in the 19th century to distinguish industrialising Britain from their nearest rival, industrialising Germany. The identity cards scheme was also touted to have an application beyond the validation of identity as such. It was proposed that such a scheme would primarily combat identity theft, perceived as rampant in the U.K., and have related positive effects for the administration of immigration, as well as aid in the fight against terrorism – for instance, if a terrorist entered the U.K. on a temporary visa, he or she could easily be located through consultation of the database. What is important to understand about the political debate surrounding the creation of the identity cards scheme was that political opposition was created not so much in respect to its supposed benefits – that the U.K. would be a 'safer' place with less identity theft – but, rather, due to the fact that the register would be centralised and monolithic, evoking references to an Orwellian 'big brother' society and in respect to the cost of the technology, its surrounding infrastructure and the fact that it would be the single guarantor of what was understood as a valid identity. The main political opposition instigated primarily by the 'No2ID'[121] campaign and the London School of Economics 'Identity Project' reflected these two issues. No2ID campaigned against the scheme, grounding their political opposition under the slogan of 'stop the database state'; while the LSE 'Identity Project' grounded their argument in identifying inconsistency within governmental budget projections in respect to the cost of the scheme not only for the U.K. Treasury, but those costs that would be passed onto the individual. Furthermore, in oral evidence given to the House of Lords as well as the U.K. Parliament in the lead-up to crafting the act, again the main focus of enquiry was not the purpose of the cards, but, rather, how the use of biometric technology could guarantee that the government was able to fix the identity of the individual in time and space and moreover to create an immutable fraud-proof, theft-proof record on the individual. Members of the computer security community saw these claims as far-fetched.[122]

Two important factors, however, became apparent during this period that compelled me to move away from a study of the identity cards per se towards the active site of U.S. post-9/11 border security: (i.) that while the political debate concerning the creation of the identity cards scheme was compelling, it emerged that even though the Identity Cards Act was to be passed by parliament, there were no clear deadlines nor the political will to confirm when the identity cards scheme would be implemented as a fully functional programme – in fact, the

[121] Information on this campaign can be found at http://www.no2idnet.

[122] The main opposition from the science community concerned centralization. This opposition forwarded by individuals such as Ross Anderson (Cambridge University) and Casper Bowden (Microsoft) argued that security risks were created with a centralized database since it provided one source of theft. What was proposed was a distributed system, where individuals stored their personal biometrics in an encrypted chip in a smart card. The individual then only needed to present his or her fingerprint biometric along with the card in order to perform identity verification, rather than query a central database.

programme itself was struck down by the Conservative government soon after they took power in 2010; and (ii.) that it became evident that biometrics and other identity-based technologies, such as data-mining technologies, had already been actively taken up by law enforcement, customs and immigration in both the United States and United Kingdom and could not only be suitable as research objects, but connected to earlier investigations begun in 2003. The first empirical site identified was US-VISIT and the surrounding host of programmes such as the collection of PNR and the transition to ePassports; the second was a pilot project announced by the U.K. government called Project Semaphore that appeared to mimic the data-mining practises for border-security management taken up by the U.S. government. As such, Semaphore was designed to track the movements and map the social networks of individuals flying in and out of the United Kingdom. These two empirical objects then became the basis of the initial research investigation I took up in 2005 to 2006 when I began at the LSE.

When I submitted this research proposal to the LSE Sociology Aims & Methods Committee, it was met with much interest and satisfaction, but it produced a question: Given that the research objects of interest technically fell within the domain of national security where intelligence practises are non-transparent, how would empirically sufficient data be obtained? In light of this obstacle, I felt confident that substantial access could be achieved with the U.K. government's scientific division – responsible for setting up the security installations involving biometrics and data-mining – as a result of the scientific contacts I had made during my work with the IPPR. In respect to obtaining data on U.S. homeland security matters, data access was not seen as a problem due to the greater openness and transparency in respect to the United States' general culture of accountancy and public accountability that provides for a degree of public oversight in the form of congressional committees and so forth. In an effort to obtain access to empirical data concerning project Semaphore, I wrote a request to the U.K. Home Office, addressed in particular to Marek Rejman-Greene, the head of the U.K. Centre for Biometric Expertise. As a result, I was given permission to engage on a one-to-one level with Greene and his staff, and they agreed to answer any technical questions concerning the functioning or functionality of biometric technology. However, my further request concerning how Semaphore operated, and in particular how it assigned risk scores and identified potential threats travelling to and from the U.K., was denied. Due to the national-security concerns surrounding Semaphore as well as the lack of empirical sites – institutional processes involving technical objects – within the United Kingdom, I turned my attention solely to the U.S. practises of homeland and border security. Here I found that there was an incredible store of open-source data on U.S. homeland security, biometrics, data-mining and data sharing that came not only from government, but from the scientific community and private sector. As a result, I began to perform my own 'data-mining' effort into this archive that contained legal documents, policy papers, testimony before U.S. congressional committees, and, importantly, the scientific literature concerning the use of biometric and data-mining technology. I was also able to expand this research strategy by identifying further relevant research sites that came under

the heading of U.S. homeland and border security. These included US-VISIT, the analysis of Passenger Name Record (PNR) information, changes made within the Visa Waiver Program and the legal and policy framework responsible for the governance of law-enforcement and intelligence efforts at the border.

One strategy that I did seek out while engaging in research was to perform expert interviews in respect to the political motivations and technological underpinnings of U.S. border security, along with intensive archival research. I did this for two primary reasons. First, in the case of the interview with Michael Chertoff conducted in September 2009, to identify the 'statements' or 'discursive formations' that represent the motivations and aims involved in the construction of U.S. homeland security policy; second, as a way to gain insight into the scientific and logical functioning of biometric and data-mining technology used within the border-security environment. This requirement to understand the scientific basis of this technology resulted from a further two factors. In 2005 to 2006, as part of the U.K. identity cards debate, the LSE Identity Project group released an early version of their assessment of the identity cards project that contained inaccuracies concerning the performance of a sophisticated biometric recognition technique known as iris recognition (Project, 2006). At the time, there also seemed to be a general lack of knowledge or awareness of how biometric technology, when used not only to perform identity verification but to match those biometrics against a database of suspect fingerprints or, in the case of iris recognition, iris codes, in fact worked. I felt that there was a gap in the literature concerning this technology, which emphasised politics rather than institutional process. In order to understand how these new security institutions were taking shape, it seemed quite important to consider how these digital technologies would perform in respect to screening millions of travellers each day passing through U.S. borders. The data gathered both through open-source policy papers, congressional, legal and technical documents and the expert interviews attempted to serve two purposes: (i.) to identify the 'statements' or discursive formations that can be charted throughout the data set in order to form regularities and ultimately provide a basis for understanding the political rationale within each case or data site; and (ii.) to account for the functioning of digital technologies and institutional orientations that determine the empirical reality and performance of the border security setup.