SECURITY OVER PRIVACY – WHO IS TO BLAME? LOOKING BEYOND U.S. INFLUENCE FOR THE REAL DRIVERS OF EUROPEAN POLICY CHANGE

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Communication, Culture and Technology

By

Julie Celton, B.A.

Washington, DC
April 30, 2008
Special thanks to my advisors:
Abraham Newman
Michael Nelson
Linda Garcia
# Table of Contents

*Chapter One: Introduction* ................................................................. 1

*Chapter Two: Policy diffusion theories* .............................................. 11
  Coercion ......................................................................................... 11
  Economic interdependence ............................................................... 12
  Dependence .................................................................................... 14
  Change in public opinion ................................................................. 15
  Symbolic imitation ........................................................................... 16
  Emulation ....................................................................................... 17
  Response to uncertainty .................................................................. 19
  Legitimacy ....................................................................................... 20
  Bureaucratic structure ..................................................................... 21
  Learning .......................................................................................... 22
  Domestic preferences ....................................................................... 23
  Conclusion ....................................................................................... 27

*Chapter Three: Privacy and security in Europe and America* .......... 30
  Privacy in the European Union and the United States .................... 31
    European privacy legislation ....................................................... 31
    American privacy legislation ...................................................... 37
  A different approach to privacy: implication for internal security .. 45
    National security in the United States ........................................ 47
    National security in Europe ....................................................... 56
  Conclusion: shifting the European equilibrium ............................. 61
Chapter Four: Presentation of the case studies ........................................66
The Passenger Name Record Agreement ...............................................67
The Data Retention Directive .................................................................89
Conclusion .............................................................................................99

Chapter Five: PNR and data retention—empirical findings ..................101
Coercion .................................................................................................105
Domestic preferences ...........................................................................110
  Germany ...............................................................................................111
  Britain ..................................................................................................117
  France ..................................................................................................126
Economic interdependence ..................................................................132
Security dependence ............................................................................135
Bureaucratic Structure .........................................................................141
Conclusion .............................................................................................151

Chapter Six: Conclusion .......................................................................153

References ...........................................................................................166
List of figures and tables

Table 1: Policy diffusion theories.........................................................26

Table 2: U.S. Undertakings of May 2004.............................................75

Table 3: Comparison of required PNR fields of data in the 2003, 2006 and 2007
Agreements .................................................................84

Table 4: Comparing the 2004 and 2007 PNR Agreements.......................87

Table 5: U.S.-E.U. Declaration on Combating Terrorism, June 2004..........138

Figure 1: Balancing privacy and security before September 11...............102

Figure 2: Balancing privacy and security after September 11...............104
Chapter One: Introduction

“They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.” These words, spoken by Benjamin Franklin in 1759, accurately capture the nature of a modern society facing imminent threats. The terrorist attacks of September 11 have accelerated the recourse to expansive security measures to ensure citizens’ safety, while often treating civil liberties as less of a priority. By changing the social norms surrounding security and privacy, some governments seem to have forgotten the words of Franklin. Indeed, while the E.U. used to balance both civil liberties and security more evenly, lately its position has shifted ostensibly closer to security policies that seem to undermine decades-old privacy policies. Why then is the European Union becoming more security-oriented, aligning its strategy with the American model? This thesis will examine today’s dilemma, by focusing on the causes of the changes in European privacy and security policy since September 11. In particular, I will argue that using coercion from the United States as the only explanation for this policy change is not sufficient. Other factors come into play, especially the shift in general European interests towards an increase in security.
Over the last four decades, innovative information technologies have facilitated and accelerated data flow, making information available virtually anywhere in the world. This sudden accessibility to data and the easiness with which information can be exchanged triggered an intensification of privacy concerns. As control over transfers seemed harder to achieve and risks of abuse rose, many governments decided as early as the 1960s to implement privacy protection measures using different approaches and various levels of requirements.

The concept of privacy is not easy to articulate comprehensively and cannot be summarized into a single definition. For instance, it can be regarded as “the right to be left alone” as Brandeis and Warren (1890) suggest or defined as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967). Although privacy seems to be an issue affecting primarily individuals in their day to day lives, the different interpretations of this concept also strongly impacts on the political and cultural levels, influencing the setting of norms, laws and values.

In Europe, civil liberties have long been embedded in legislation, starting from the 1950 Convention of Human Rights. In 1995, privacy protections were strongly reinforced as the European Union adopted a Data Protection Directive, setting out strict
conditions for information handling and data transfer. Unlike Europe, the U.S. chose a different privacy model, based on a fragmented sectoral approach and implemented data protections safeguards when the need arose.

The issue of balancing privacy and security is not new as the European countries have had to address it at the domestic level in confronting terrorism. However, September 11 brought back the debate surrounding privacy and security with a new level of significance. The attacks on the World Trade Center—and subsequent terrorist bombings in Madrid and London—profoundly altered the world’s perception of privacy and security and significantly impacted on social norms and legislation. Countries reacted differently to the events and, taking the restriction of their privacy regulations into account, they introduced security measures with different degrees of stringency. Immediately after the attacks, the United States introduced strict security policies, such as an increase in surveillance and data sharing, which often significantly weakened privacy safeguards. On the other side of the Atlantic, the European Union adopted additional safety measures as well, but tended to favor those having a less negative impact on civil liberties. Unlike the U.S., whose privacy regulation is not comprehensive, the European Union is bound by strict data protection legislation that limits the actions of the national governments. As the United States started pressing the
Europeans for greater transatlantic cooperation and expansive security polices, the two models of privacy protection triggered conflicts and slowed down collaboration.

The methodology used to demonstrate the argument developed in this thesis is based on two hypothesis-generating case studies: the Passenger Name Record (PNR) Agreement and the Data Retention Directive. The rationale for selecting these two examples lies in the fact that both have created significant debates within the E.U. and illustrate the intricate balance between privacy and security. The data I have used in this thesis is mainly comprised of primary sources, as I examined official statements by key players, agreements between the United States and the European Union as well as national and supranational legislation. I complemented my research with articles from academic journals, European and American newspapers and books written by influential scholars and experts in the security and privacy fields.

The thesis is constructed with six chapters, as follows:

Chapter Two develops in great detail policy diffusion theories, which explain why a country adopts a policy developed abroad. This thesis will briefly present 11 theories, which constitute the common views shared by scholars: coercion, economic
interdependence, dependence, change in public opinion, symbolic imitation, emulation, response to uncertainty, legitimacy, bureaucratic structure, learning and domestic preferences.

Chapter Three goes back to the premise of this analysis, as it will present an overview of the American and European privacy regimes as well as security strategies. This study will argue that different types of data protection regulations impact national policymaking by granting governments a varying degree of ability to make security decisions. Because the E.U. has to take into consideration its strict privacy regulation, the Member States adopted security policies that were more oriented towards police and judiciary cooperation on specific cases, rather than measures requiring the wholesale collection of private personal information. On the other hand, the United States, not constrained by such strict privacy laws, chose to expand surveillance as the appropriate means to ensure national security. Analyzing balancing strategies from both the United States and the European Union has significant value, as it demonstrates the shift of European priority towards American security practices.

Chapters Four and Five are dedicated to the demonstration of my argument as I will apply my hypothesis to two case studies: the 2007 Passenger Name Record (PNR) Agreement, authorizing the transfer of travelers’ personal journey information from the
European air carriers to the American Customs and Border Protection, and the European Data Retention Directive of 2006, requiring telecommunications providers to retain information for 6 to 12 months for law enforcement purposes.

Chapter Four presents both case studies, developing the timeline of the debates and the main players trying to influence the outcome. In the case of PNR, a first agreement was adopted by the European Commission and the United States in 2004, but was annulled by the European Court of Justice in 2006. The European Parliament, initiating the lawsuit, strongly opposed the PNR Agreement as damaging civil liberties. The debate was finally closed in 2007, as the European Union and the United States agreed on the conditions of PNR transfer. Although the U.S. made several concessions, the Data Protection Authorities still remained critical of the treaty’s implication on privacy. The second case study addresses data retention and presents the European debate as to whether to introduce mandatory data storage by telecommunication providers, and under what conditions. Before 2006, the Member States had different data retention laws, which limited the judiciary and police cooperation within the Union. The need for harmonized legislation appeared in 2000 but was reinforced following the September 11 attacks and the bombings in Madrid and London. In March
2006, even the most reluctant Member States and the European Parliament agreed on a final Data Retention Directive.

Chapter Five provides the analysis of these two case studies, as I applied the five theories selected in Chapter Two to the PNR and data retention debates. Coercion represented a strong influence on the negotiation, emanating from the Unites States for PNR and, to a lesser extent, from the European Council for data retention. The analysis of this second case study bolsters the assumption that American pressure alone is not sufficient to understand the European shift in position. Indeed, the debate surrounding data retention was purely European and the preference for security over privacy reflected internal dynamics. As a result, domestic preferences also represent a particularly substantial factor of policy change. Analyzing in greater detail the interests of the U.K., France and Germany has pointed out their preferences for more security, even if it involves a trade-off with privacy. Because of their influential position within the Union, the British, French and German governments pressed for the adoption of their security preferences at the E.U. level. Another factor explaining the policy change is the economic interdependence between the E.U. and the U.S., which appeared particularly critical in the PNR case, as the U.S. used economic sanctions to coerce the European airline industry into adopting the American positions. This relationship can
also be expanded to the general level, as the E.U. and the U.S. constitute the world’s two largest economies and bilateral trading partners. These factors influenced the E.U. in adopting American policies and becoming more security-oriented. Security dependence represents the third factor applying substantially to the research question developed in this thesis. Indeed, the European Union and the Unites States realized that their collaboration was essential to ensure the security of their citizens. Finally, the fact that the European Union is becoming more security-focused can be explained in part by the lack of the Data Protection Authorities’ influence. As these defenders of civil liberties only had limited power due to an unfavorable bureaucratic structure, they were not able to counter the direction of the PNR or data retention debates.

Finally, Chapter Six presents a global overview of the empirical and theoretical findings, the limitations of this study and the policy implications. In particular, it provides suggestions for American and European policy makers as they strive to craft policies that can enhance both privacy and security.

Before getting in depth into this analysis, it is important to clarify a substantial difference in perspective. This thesis will not address the issue of balancing security vs. privacy but balancing security and privacy. Indeed, it is commonly said that increasing
privacy always leads to a reduction of civil liberties. Ed Giorgio, a security consultant working with U.S. National Intelligence Director Mike McConnell, reiterated this notion, as on January 2008, he declared, “We have a saying in this business: 'Privacy and security are a zero-sum game.'” However, EPIC Executive Director Mark Rotenberg and Jennifer Granick, the Executive Director of the Stanford Law School Center for Internet and Society, argue that both privacy and security can and should be improved in parallel. Bruce Schneier, a well known computer security expert, shares their point of view and believes that “the best ways to increase security are not at the expense of privacy and liberty.” Therefore, collecting data to enhance security would not harm privacy if the data collected is protected by appropriate safeguards. For instance, improving the protection of financial data by implementing better encryption and passwords would reduce cyberfraud and identity theft, while at the same time enhancing customers’ privacy. Another example that privacy and security are not inversely correlated is that the enforcement of more efficient safety measures could actually endanger security as well as privacy. Indeed, as more information is collected, the risk of data misuse and inappropriate handling increases. Thus, implementing strict security policies without the proper safeguards would not be effective and could

---

1 Lawrence Wright, the Spymaster; A Reporter at Large. The New Yorker. January 21, 2008
2 Electronic Privacy Information Center, http://epic.org
undermine both security and privacy. Were the number of identity thefts by terrorists to increase due to mishandling of data by federal authorities, the public support for anti-terrorism effort could also weaken. The demonstration that both security and privacy are needed can also be reflected in the fact that civil liberties advocates do not oppose the idea of increased security and recognize the need to improve the citizens’ safety. Their concerns usually lie in the conditions under which security measures are implemented, and they try to make the governments aware that preserving privacy is crucial and can be achieved in correlation with security.
Chapter Two: Policy diffusion theories

Over the last few decades, scholars have developed several theories explaining why a country adopts a policy developed by another state. This chapter will present an overview of the main policy diffusion theories and apply each of them to the adoption of American security measures by the European Union. This analysis will demonstrate that although coercion often seems to be the first explanation of the European policy change, other significant factors have to be taken into account as well. The theories presented in this chapter range from those where policy change is most forced on governments to those where the adoption of a foreign policy constitutes a free choice.

Coercion

Coercion is the imposition of policy on a state by a powerful country or international organization (Braun & Gilardi, 2005). Although coercion tends to imply the threat or use of physical force, it can also refer to more implicit methods. Alternative incentives and sanctions such as the manipulation of economic costs, as well as the monopolization of information or expertise, can be used to impose policies (Simmons, Dobbin and Garrett, 2006). The stronger country thus promotes its policy
and use a mechanism of carrot and stick to induce other nations to follow suit (Weyland, 2005).

This theory applies well to the issue addressed in this thesis. Indeed, in the past, the United States has used political and economic pressures to promote the adoption of a policy reflecting American interests, by the European Union. For instance, the U.S. has openly threatened to use economic sanctions against the European Union, in order to have its preferences adopted on air travel security. Simmons, Dobbin and Garrett (2006) argued that the powerful country has a desire to stimulate policy change abroad while the weaker country would prefer to resist. In this case, the United States wants to gain extraterritorial control to pursue its national security goals. On the other side, the European Union has norms and legislation that sometimes conflicted with the American interests. However, the Member States still adjusted to some of the U.S. demands, because the stakes of non-compliance would be too great to face, were the Americans to follow through on their threats.

**Economic interdependence**

Advocates of this theory argue that economic interdependence, including competitive and cooperative interdependence, increases probability of policy diffusion.
Two countries competing for a growth in international capital and export market shares will tend to implement similar policies. Proponents of this theory explain that a policy choice in a country impacts on the competitor as it creates externalities for this second state (Braun, Gilardi, 2006). In order to adjust and remain competitive, the second country will be forced to follow and adopt the same approach. Simmons, Dobbin and Garrett (2006) point out that this policy diffusion process will most likely occur between countries sharing the same competition networks. In the cooperative interdependence model, the two countries will increase their competitiveness by adopting common standards and thus facilitating business practices.

At first glance, one could consider that the issue approached in this thesis is not economic in nature and thus cannot be explained by the economic interdependence theory. Indeed, what both countries have to win is an improvement of national security to reduce the risk of terrorism and the primary goal of their cooperation is not oriented toward a gain of economic leverage. However, by taking a broader perspective, one would realize that the effects of globalization have made the high level of privacy protection a significant expense. European companies are forced to adjust to the market pressures to remain competitive. As the E.U. privacy legislation limits the conditions of information sharing, a foreign country could choose to work instead with American firms, which are not held by such limiting legislation. The economic interdependence
theory thus has to be taken into account in the explanation of the European shift towards more security oriented policies.

**Dependence**

This theory argues that dependence between two countries leads to harmonization. Countries sharing the same goals and values will tend to resemble each other. In that sense, policy diffusion can be most expected to occur with geographical proximity ("copy your neighbor"), or between countries sharing the same economic and cultural patterns (Leichter, 1983).

Because terrorism has become a transnational matter, there is a need for a greater cooperation between the United States and the European Union. Both actors want to ensure the safety of their citizens and prevent any other terrorism attacks. As a result, they have to adopt common instruments and enhance their cooperation to answer the security demands of the public. This theory can thus strongly apply to the issue developed in this thesis, as one could argue that the need for collaboration – a principal tool to fight terrorism – is pushing the European Union towards a more security oriented approach. The field of information sharing follows the same logic. Indeed, the dependence between European and American law enforcement and
intelligence agencies also influences the Member States to follow the policies developed in the United States. This can be demonstrated by the increase in cooperation between these agencies as Europol and the United States adopted information sharing agreements in 2001 and 2002 and the U.S. and the E.U. signed two treaties in 2003 on extradition and Mutual Legal Assistance (Archick, 2006).

**Change in public opinion**

A change in public opinion could represent another explanation of policy diffusion, pressing a government to adopt a measure developed in another state. Consequently, even if a government opposes a particular action taken abroad, the sudden public support for this policy could push the authorities to readjust their positioning.

This theory could illustrate our case study if there were any evidence that the European citizens favor security even at the detriment of privacy. However, searching for polls or surveys reflecting the public opinion on these two issues has proven unsuccessful. Nonetheless, some data presenting the Europeans’ position on the fight against terrorism are available and could be used to argue in favor of the theory discussed in this paragraph. Indeed, the EuroBarometer poll of 2007 has demonstrated
that 81% of Europeans believe that fighting terrorism should be carried out at the European level. Moreover, 80% of citizens interviewed are in favor of strengthening entry controls into the E.U. for persons coming from non-Member States (Eurobarometer Flash report, 2004). These finding demonstrate the importance given by Europeans to the security issue, their willingness to develop stricter control instruments and their desire for a common strategy to fight terrorism. Although these figures do not literally demonstrate the preference of the Europeans for security as clearly as in the United States⁴, they still could be interpreted as a demand for more security-oriented policies.

**Symbolic imitation**

The symbolic imitation (Braun, Gilardi, 2006) or normative imitation (Weyland, 2005) theory explains that a country will adopt a policy in order to seek recognition from the international community. A state may implement legislation that does not necessarily represent a domestic priority but shows that it acts in a proper and adequate way. The fact that the country may not even be ready to adopt the policy does not matter, as the main goal is to impress and get legitimacy from other states.

⁴ According to the Rasmussen Report of January 2008, 51% of Americans prioritized security over privacy, against 29% considering privacy as more important. 20% of the interviewees did not express their preference.
(Simmons, Dobbin and Garrett, 2006). In this situation, there is an informal pressure to adjust to international norms.

Over the last two decades, the European Union has gained tremendous recognition as an international actor. Moreover, it includes the most powerful European states, which also increase its influence as a global entity. For this reason, arguing that the European Union shifted its positioning because it seeks international legitimacy does not seem to apply to the privacy and security debate.

**Emulation**

Several scholars believe that this theory constitutes a strong factor of policy diffusion, basing their reasoning on the fact that repeated interactions in networks lead to the development of common norms (Braun, Gilardi, 2006). Shared socialization will entice the actors to develop similar views and a consensus on what is appropriate will then emerge. At the international level, Simmons, Dobbin and Garrett (2006) argue that “sociocultural linkages (common language, history, religion and so on) may contribute to ‘psychological proximity’ among nations.”

---

At first, one could consider that the emulation theory does not apply to our case study. Indeed, the European Union and the United States have diverging views on how to ensure national safety and fight terrorism. Even if they interact in many ways and share numerous similarities in terms of economy or culture, the authorities of both actors still maintain their opposing views. However, the extensive interactions between European and American law enforcement and intelligence agencies tend to counter this perspective. Indeed, Frank Kerber, former U.S. Mission to the European Union, argues that the cooperation between these agencies has never been more intense. For instance, he explains that contacts are increasing between both players, arguing that the E.U. and the U.S. have signed several important agreements addressing these issues during the last couple of years. Moreover, Europeans and Americans have sent agents and specialists on the other side of the Atlantic to participate in meetings or follow project developments. Kerber also emphasizes the fact that a complicated agreement such as the Extradition and Mutual Legal Assistance treaty was negotiated in only eight months, which underlines the existence of a common perception on how to deal with the issue and the strong political will from both actors to cooperate. This evidence points out the importance of the emulation theory as a viable explanation for the European shifting of positioning.
Response to uncertainty

A country can also adopt a policy developed abroad as a response to uncertainty (DiMaggio and Powell, 1983). Facing a problem never encountered domestically, a nation will turn to other countries and assess the solutions implemented abroad in a similar situation. A high degree of urgency to solve the problem (Leichter, 1983) and the failure of precedent policies (Walsh, 2006) will make policy diffusion even more likely to occur.

This theory seems relatively difficult to apply to the European Union security and privacy strategies. Indeed, one could argue that the Member States have already adopted a domestic response to terrorism. Unlike in the United States, European institutions have opted for security policies striking a balanced equilibrium between the need for safety and the respect of individuals’ privacy. Moreover, the issue of terrorism is not new to numerous Member States. The counter argument to this perspective would be to say that the European Union is adopting U.S. policies as its own approach failed to prevent two terrorism attacks in Madrid and London. However, as there is a lack of substantial evidence to demonstrate that the American security policies are effective, this perspective does not rely on sound arguments and should thus be dismissed.
Legitimacy

The legitimacy theory emphasizes the domestic perceptions of the foreign policy. Indeed, if the measure developed abroad appears legitimate, it will more likely be adopted domestically. As such, a country will be more inclined to introduce similar legislation if there is a general consideration that this policy has positive, appropriate and efficient impacts (Jensen, 2003). Besides, the more countries assimilating the policy, the more legitimate it becomes. As Braun and Gilardi (2006) explain, “the taken-for-grantedness argument posits that over time, some practices may become accepted as the normal or even the obvious thing to do in given contexts.”

Could the European Union thus adopt the American preferences because it seems to be the obvious response to fight terrorism? Answering this question proved to be difficult as different perspectives oppose each other. Indeed, one taking the side of the civil liberties advocates would consider that the legitimacy theory can absolutely not apply, arguing that American security policies strongly infringe on privacy and thus cannot be considered legitimate and even less as representing a common norm. On the other hand, European law enforcement and intelligence agencies would state the opposite, pointing out that the increase in intelligence sharing in the United States

---

represents a crucial tool of terrorism prevention. Another argument in favor of this perspective would be that the United States has not faced any terrorism attacks since the implementation of stricter policies, while the European Union has encountered several. The intelligence and law enforcement agencies would then argue that the American policies are legitimate and thus should be implemented in Europe.

**Bureaucratic structure**

The adoption of foreign policies is often not perceived positively by all major national players and encounters various degrees of resistance. Depending on the bureaucratic structure of a country or organization, and thus the level of influence granted to opponents of the policy, a government’s decision to adopt this foreign measure will be more or less challenged.

This theory strongly applies to our case study as the European opponents of the American security policy do not have enough power to influence the outcome of the debates. The Privacy Commissioners and the civil liberties advocacy groups are independent entities and do not benefit from a strong influence in the policy decision-making process. Even if the Privacy Commissioners have legal authority as set up by European laws, they are not always based at the core of national key institutions and
are not necessary included in major debates and decisions. They mostly give opinions and recommendations that are not always taken into account. This lack of perpetual presence within the Union’s policy-making process limits the Privacy Commissioners’ power to influence the outcome of the security debates.

**Learning**

Learning about a new policy implemented abroad constitutes another explanation of policy diffusion. Advocates of this theory argue that the acquisition of new relevant information remolds domestic beliefs, values and norms and thus influences policy change (Simmons, Dobbin and Garrett, 2006). Weyland (2005) introduced two different aspects of learning as vector of policy diffusion: rational learning and cognitive heuristics. A country using rational learning will assess various policies developed abroad and select the one demonstrating its superiority. On the other hand, cognitive heuristics, also referred to as bounded learning (Braun, Gilardi, 2006), implies that a government will adopt a policy that seems attractive and could potentially be successful. The policy’s efficiency cannot be demonstrated but the prospects are considered as highly positive and more important than the actual risk of
failure. Tyran and Sausgruber (2003) emphasize the importance of information sharing between countries as a necessary element of the learning theory of policy diffusion.

Although the European Union is aware of the constant improvements of American surveillance capabilities and information sharing tools, one could argue that the learning theory still does not explain why the E.U. is shifting its positioning towards a more security-oriented approach. Indeed, the debate is not really centered on the techniques themselves, but more on the question of using these tools or not. The United States has been developing new technologies for the last decade but the European Union still chose an approach that better balanced security objectives and respect of privacy. Following this reasoning, there is no demonstration that the new American surveillance systems introduced after the September, 11, 2001 attacks suddenly influenced the European Union into changing its policy.

**Domestic preferences**

Finally, according to this theory, a nation decides to adopt a policy promoted by another country because it reflects its own goals and values. The change is absolutely not forced, but is chosen in accordance to the national interests.
This theory applies to the European Union as internal forces drive security policymaking. Each member state has its own policy preferences, reflecting national interests, concerns and history. The European governments will thus try to influence the decision process at the Union level and press for the adoption of policies most closely matching their inclinations. For instance, the United Kingdom and France have long confronted terrorism and have already developed strong national security legislation. Moreover, both countries need to address citizens’ concerns about immigration, which encourage them to increase the surveillance of individuals. For these reasons, their domestic preferences tend to lie in stricter border controls. As the U.K. and France are among the most influential countries in the European Union, they greatly influence the European policymaking process. This example thus emphasizes the importance of national interests as factors of policy diffusion.

The following chart summarizes this chapter by presenting an overview of the policy diffusion theories. I identified the conditions necessary for each theory’s application to the thesis research question and their actual relevance in explaining the European shift of policy.
The first theory represents the situation where the foreign policy is most forced on a government, while the last presents the case where policy change is freely adopted by a country.
<table>
<thead>
<tr>
<th>Description of theory</th>
<th>Conditions for application</th>
<th>Level of application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coercion</td>
<td>Threats of force, economic incentives and sanctions by the United States</td>
<td>HIGH — the U.S. has threatened to suppress trade and technology to enforce privacy regulations.</td>
</tr>
<tr>
<td>Economic interdependence</td>
<td>Competition for market share and economic gains will either force a country to accommodate its policy with its competitors' or both sides will choose to adopt similar policies</td>
<td>HIGH — although the E.U. and the U.S. are primarily pursuing policy that is not to its economic goals, the strong implications of privacy policies to the competitiveness of European companies that influence European decision-making to reduce general privacy restrictions.</td>
</tr>
<tr>
<td>Dependence</td>
<td>Both the U.S. and the EU want to prevent terrorism and secure national safety. Existing collaboration in this matter</td>
<td>HIGH — fighting transnational terrorism requires greater transatlantic cooperation. Increasing contacts and agreements between the E.U. and the U.S. since 9/11.</td>
</tr>
<tr>
<td>Change in public opinion</td>
<td>European citizens support the American security policy over the European approach (less security oriented, but respecting more privacy)</td>
<td>MEDIUM — polls tend to show a priority given to security over privacy but public involvement demonstrates the citizens' desire for policy changes.</td>
</tr>
<tr>
<td>Symbolic imitation</td>
<td>The European Union seeks legitimacy from the international community and thus adopts the American perspective, considered as the appropriate norm.</td>
<td>NOT APPLICABLE — the EU is already a powerful international actor and does not need to gain legitimacy. Depending on views, the U.S. approach is not even perceived as appropriate.</td>
</tr>
<tr>
<td>Emulation</td>
<td>Because of the repeated contacts between European and American representatives, the E.U. and the U.S. have reached a consensus on the appropriate tools to fight terrorism and secure domestic safety</td>
<td>LOW / HIGH — the application of this theory is mitigated as the Privacy Commissioners would argue against the existence of a consensus, while the Law enforcement and surveillance agencies would state the opposite.</td>
</tr>
<tr>
<td>Response to uncertainty</td>
<td>The U.S. is adopting American policies as a response to threats of terrorism and does not know how to respond</td>
<td>LOW — counter-terrorism policies weighing both security and privacy are already adopted by the E.U. as the appropriate solution. Terrorism has also been experienced by Member States for a long time.</td>
</tr>
<tr>
<td>Legitimacy</td>
<td>The American security policy is perceived as legitimate and is thus taken for granted as the norm to adopt</td>
<td>LOW / HIGH — depending on the institutions, the U.S. security policy is perceived as strongly illegitimate by privacy commissioners or appropriate (law enforcement / intelligence agencies).</td>
</tr>
<tr>
<td>Bureaucratic structure</td>
<td>The European Privacy Commissioners and civil liberties advocacy groups have limited power on the decision-making of European national security policies</td>
<td>HIGH — because the Privacy Commissioners are not based within the European institutions but stand inside independently, their access to central debates and decision-making is limited.</td>
</tr>
<tr>
<td>Learning</td>
<td>The E.U. is adopting the American security approach, as the U.S. recently developed new tools to fight terrorism, altering the European position.</td>
<td>NOT APPLICABLE — the debate is not centered on the means to prevent terrorism but on the moral judgment of using these privacy-invasive measures or not.</td>
</tr>
<tr>
<td>Domestic preferences</td>
<td>The American security policies fit with the European Union's domestic values and goals.</td>
<td>HIGH — internal dynamics push the E.U. to become more security-oriented, as the American security policy reflects the interests of some influential Member States.</td>
</tr>
</tbody>
</table>
Conclusion

This chapter aimed at providing a theoretical framework necessary to answer the dilemma addressed in my thesis. Even if most of the hypotheses discussed above apply to my research question as to why the European Union is adopting policies reflecting American preferences, some appear to be more relevant than others. Coercion is often immediately pointed at, for it is relatively simple to demonstrate and it constitutes a powerful vector of policy diffusion. However, this chapter has showed that coercion theory alone does not offer an all-encompassing view but only represents a fraction of the reasons why the European Union is shifting its policy. The other applicable factors developed above have an important role to play, for they constitute complex but relevant dynamics of change. Particularly complementing the coercion argument, the domestic preferences, economic interdependence, bureaucratic structure and dependence theories seem to best address the topic discussed in this thesis. These additional theories can be summarized as representing new European interests. Indeed, the Member States influence decisions at the national (domestic preferences), as well as supranational (economic interdependence, bureaucratic structure and dependence) levels.
Although policy diffusion theories bring significant insight to explain the shift in European security strategy, this theoretical approach still has its limits. First, it is difficult to differentiate one theory from another, as they are often intricately related. For this reason, the shift emerging in Europe cannot be explained by a specific theory, but more by the combination of several hypotheses. Second, taking into account every angle on the issue and getting a comprehensive overview of the policy change dynamics constitutes a very difficult task. Indeed, many reports, articles and documents addressing the debate around European privacy and security often only offer a single broad perspective, blending the various voices into a common position. For instance, journalists and analysts will use general formulations such as “the European Union criticizes…” or “the E.U. says…,” without indicating which player is included in such a broad concept. By setting this agenda, the media offer a biased report, mostly presenting the strongest views and granting less importance to diverging opinions. Finally, some sources are simply not available to the public as they discuss sensitive security topics. Gathering the point of view of every player to present a complete landscape of perspectives thus constitutes a particularly challenging task.

This chapter has only offered an overview of hypotheses answering the thesis’ research question and does not represent a comprehensive analysis of the issue.
Because carrying out such a study does not fit the scope of this project, I will focus my research on two case studies (the Passenger Name Record and data retention agreements), developed in Chapters Four and Five of this thesis. However, before getting to the empirical analysis, I will analyze in greater detail the European and American privacy and security legislation. The next chapter will thus present the background of my thesis topic and introduce the shift in European positioning.
Chapter Three: Privacy and security in Europe and America

The attacks of September 11 have highlighted the weakness of European and American internal security, emphasizing the necessity for greater transatlantic cooperation as a response to transnational terrorism. However, as the United States and the European Union set the foundations to improve their collaboration, profound differences surfaced in the ways Americans and Europeans value privacy and security. Indeed, both actors do not share the same perception of privacy and their legislation is based on substantially differing frameworks. While European countries have adopted comprehensive regulatory tools since the Convention of Human Rights in 1950, the American system is fragmented into sectoral pieces of legislation and relies deeply on self-regulation.

This difference in perspective hindered cooperation, since both Europe and America hold unequal expectations of each other as well as contrasting perceptions of the appropriate instruments to deal with terrorism and ensure internal security. Since the United States is not constrained by comprehensive privacy legislation, it tends to prioritize the security of the citizens and the territory, sometimes at the expense of civil liberties. On the other hand, the European Union reacted less dramatically to the
attacks on the World Trade Center and favored a more cautious approach, granting civil liberties a greater importance in the balance with security.

In this chapter, I will analyze how the United States and the European Union approach civil liberties and security. I will first present the privacy regulations in the European Union and the United States. Secondly, I will address the security policies implemented by both actors in reaction to the September 11 attacks. This chapter will demonstrate that the United States tends to tilt the scale in favor of security over privacy, while the European Union seems, at first glance, to maintain a fairer balance.

Privacy in the European Union and the United States

European privacy legislation

Since the early stages of the European Union, privacy has been enshrined in legislative frameworks. This concept was first incorporated in the 1950s, when the Council of Europe signed the Convention on Human Rights. Article 8 of the agreement, dedicated to the “Right to respect for private and family life,” mentions that every individual has “the right to respect for his private and family life, his home and
his correspondence” without any “interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

Although all the member states of the European Union are also signatories of the Convention on Human Rights, the European Court of Justice declared in 1996 that the treaties establishing the European Community did not empower it to accede to this Convention. After several years of work, the European Parliament and European Commission finally signed in 2000 the Charter of Fundamental Rights of the European Union. This treaty did not have a binding power on the member states but had a more symbolical nature, combining the Union’s fundamental principles of human rights. The Articles 7 of the Charter reiterated the definition of privacy given by the 1950 Convention of Human Rights. However, it introduced the privacy and data protection issues in Article 8 (“Protection of personal data”). This clause states that “everyone has the right to the protection of personal data concerning him or her” and the process of such data should be done in accord to the law, with the consent of the data subject and granting him/her a right of access to the data concerned.
In December 2007, the Treaty of Lisbon gave this Charter a legally binding feature, which now enables the Union to ensure that human rights, including the right for privacy, would be enforced in the framework of both the international Council of Europe and the European Union.

In parallel to the Charter and the Convention, some European countries had already developed national privacy legislation since the 1970s. For instance, the German province of Hesse was the first to pass a privacy act in 1970, in reaction to computerization and centralization of personal information (Klosek, 2007). Six years later, Sweden introduced the first national data protection law, prohibiting the government from keeping information about its citizens, if not used for legitimate purposes. France followed and enacted on January 6, 1978 a law on Data Processing, Data Files and Individual Liberties. By the early 1990s, most E.U. members, such as France, Germany, Italy and Spain had adopted privacy legislation, with requirements that vary in their level of restrictions (Swire, 1998).

The European Union took another decisive step for privacy rights when the Parliament and Commission adopted the European Data Protection Directive 95/46/EC on October 24, 1995. This new regulation, which aimed at harmonizing national
privacy legislation, strongly influenced the international privacy standard. The Directive defines personal data as “any information relating to an identified or identifiable natural person.” Since European directives do not apply directly to the Member States’ citizens, each country had to transpose the Data Protection Directive into a national law. Directives can be slightly altered in order to reflect the identity and culture of each Member State, so by 1998, 15 harmonized, but still slightly diverse pieces of legislation were adopted in the European Union.

Although the Data Protection Directive is a very comprehensive law, its scope is limited to the private sector. Indeed, the European Union Member States still retain sovereignty on their governmental activities, which renders the Directive inapplicable to the public sphere. Nonetheless, the Directive still strongly recommends that Member States introduce similar legislation to cover the public sector.

The European Directive incorporates the 8 principles described in the privacy guidelines enacted by the Organization for Economic Cooperation and Development in 1980: (1) Collection limitation: only the necessary amount of information should be collected and by lawful and fair means; (2) Data Quality: information should be relevant to the purpose they are collected, so it must be kept accurate and up-to-date; (3) Purpose Specification: the reason why the information is collected should be
clearly notified; (4) *Use Limitation:* the data should not be shared with a third party, unless specified. If the information is to be transferred, it should be done with the consent of the data subject and in accordance with the law; (5) *Security Safeguards:* the data collected should receive the appropriate amount of security; (6) *Openness:* the data subject has to be aware of the collection of his/her information; (7) *Individual Participation:* the data subject has the right to know if information is gathered about him/her, to access the record and to request changes; (8) *Accountability:* the data collector should be accountable for managing the information in accordance to the policy in effect.

The European Directive includes these principles, but it also goes further than the OECD guidelines and adds three main dimensions. First of all, the Directive is binding whereas the OECD guidelines were not. In this regard, it sets a list of penalties and sanctions for non-respect of the law. Then, it creates the “Article 29 Working Party,” an advisory and independent group representing the privacy authority of each Member States. Finally, it brings the concept of adequate level of privacy protection in regard to the exchange of data with third countries (Article 25).

This last point is crucial, as it determines which countries are eligible to share information with the European Union and which are not. If the European Commission
considers that the privacy framework of a nation does not offer a protection comparable to the European Data Protection Directive, it will prohibit the transfer of information. Article 26, however, provides an extensive list of exceptions to specific cases, allowing more flexibility and giving ways to get around the tightness of the regulation: “(a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation” are fulfilled in the particular case.”
Although the Data Protection Directive of 1995 represents the most fundamental privacy legislation in Europe, other directives were enacted to cover certain areas more specifically. For instance, the Privacy and Electronic Communication Directive was enacted in July 2002 to regulate the telecommunications sector. Likewise, the Data Retention Directive, passed in March 2006, defines the conditions under which data is made available to law enforcement for investigation and prosecution of serious crime, while at the same time protecting the privacy of the data users.

This overview of Europe’s privacy regulation emphasized the importance given by the European Member States to civil liberties and the consequent comprehensiveness of the law. The following section will analyze the privacy legislation in the United States.

*American privacy legislation*

The development of a privacy statute in the United States has been particularly slow and uneven. Although the concept of privacy had long existed in America, it was first referred to as a legal right by Samuel Warren and Louis Brandeis in the late 19th
century. In 1890, the two authors wrote an article in the Harvard Law Review entitled “the Right to Privacy” which introduced privacy as “The right to be left alone.” In their piece, they argued that “Political, social and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.” According to Ken Gormley (1992), the growing request for recognition of privacy rights was triggered by the explosion of the media, and especially “the significant upheaval in American journalism and photography between 1870 and 1890--and the concomitant abuses of the press and photographers in culling and disseminating information.”

In the 20th century, this demand for more privacy increased again, generally in accordance with the public fear of government misusing information and the media coverage of political scandals. As Gormley (2002) indicated, the surveillance and wiretapping technologies grew in availability and sophistication in the 1940s and 1950s, accelerating the need for privacy. Moreover, when the extensive use of wiretaps by the government was made public in the 1960s, the population became much more


aware of the privacy risks at stake and thus demanded more protection. Gormley also emphasized that the 1960s “witnessed a national uproar over the unchecked ability of government and private investigators to eavesdrop⁹.” Finally, the scandal of the Watergate reinforced this mistrust in the federal government and was immediately followed by the enactment of several laws protecting privacy (Gormley, 1992).

On the judiciary side, privacy became more and more visible during the 1960’s, mostly following the events mentioned above. When Warren and Brandeis’ definition of privacy became too vague, Prosser introduced four components to the right to privacy: no intrusion into a person’s private affairs, no public disclosure of embarrassing facts, no publicity that puts an individual in false light and no appropriation of an individual’s information for one’s own advantage (Heisenberg, 2005).

Another important step for privacy was taken in 1965, when the Supreme Court acknowledged for the first time the existence of an implied right to privacy in the Constitution. During the following few years, several court cases such as *Griswold v. Connecticut* (1965) and *Katz v. the United States* (1967) reflected the increasing recognition of privacy.

---

⁹ Id.
Various laws followed these cases, such as the Privacy Act, enacted by the U.S. Congress in 1974, the Freedom of Information Act (1974) and the Family Educational Rights and the Foreign Intelligence Surveillance Act (1978).

When the OECD principles were compiled in 1980, the United States considered these standards but unlike the European Union, the American government did not create a binding law around the propositions.

The American legislation is based on a piecemeal approach to privacy, growing up through statutes and precedents established by the court. Heisenberg (2005) argues that these laws were enacted on the basis of emerging needs to counter the increase in abuses occurring due to an absence of legislation. As a result, the regulation at the federal level is fragmented to cover three main sectors and apply to particular types of data within these fields.

The first segment protected by the legislation is finance. In this domain, the Fair Credit Reporting Act (1970), Bank Secrecy Act (1970), the Right to Financial Privacy Act (1978) and the Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act) represent the main Acts enacted to cover specific issues.

The federal legislation also encompasses telecommunications activities. This sector, including online privacy, gathers an extensive set of regulations, as it represents
the field were most breaches have occurred. The new technologies increased the access, exchange and flow of information, thus jeopardizing the citizens’ privacy. The Cable Communications Policy Act was enacted in 1984, followed by the Electronic Communication Privacy Act in 1986, the Video Privacy Protection Act in 1988 and the Children's Online Privacy Protection Act in 1999.

Finally, health is the last sector extensively covered by federal privacy regulation. The principal piece of legislation is the Health Insurance Portability & Accountability Act (HIPAA) adopted in 1996, in response to increasing breaches of confidentiality tort. This law covers health care providers, insurers and information clearinghouses.

In addition to these legislations, the Federal Trade Commission (FTC) plays an important role in the privacy debate, as it dedicates parts of its mission to the protection of consumer privacy protection. The FTC specializes in four areas. It enforces (1) the compliance of companies with legal handling of consumer’s personal information and the avoidance of unfairness and deception, (2) the respect of financial privacy, (3) the enforcement of the Fair Credit Reporting Act and (4) the protection of children’s privacy.
It is important to point out that contrary to the European Union Directive, which covers the private sector, most of the national legislation enacted by the American Congress mainly applies to governmental activities, leaving a great part of the private sphere to self-regulation. Several companies and associations are thus in charge of enacting privacy norms for their industry. The main organizations include Online Privacy Alliance, which developed guidelines for privacy policy and effective enforcement of self-regulation and the Better Business Bureau Online and TRUSTe, which both promote the development of trust between consumers and companies through the respect of privacy. These three organizations also offer a great amount of resources on privacy and aim at increasing consumers’ awareness. Self-regulation is also carried out by State bar associations, medical boards, and organizations such as the National Association of Securities Dealers, the American National Standards Institute, the Direct Marketing Association and Consumer Bankers Association. Peter Swire (1998) discusses the pros and cons of self regulation, arguing that although it enables industries to add their own expertise and include ethic and community norms, the risk that prominent business players act together to exercise market power is high and balances positive aspects.
When the European Directive went into effect in 1995, it was clear that the American privacy framework would not qualify as adequate. Indeed, the problem arose due to the lack of comprehensive legislation and particularly the fact that the existing regulation mostly only covered the public sector. Moreover, as Heisenberg (2005) explained, sometimes even in the fields protected by the law, all the privacy elements required by the European Data Protection Directive are not incorporated. Finally, as the private sector is mostly subjected to self-regulation, it adds another level of inadequacy to the American framework.

As pointed out by Peter Swire (2005), this status of inadequacy had strong repercussions on international trade as it means that companies in the United States were not allowed to exchange information with citizens or businesses in the European Union. Because such restriction had a significant impact, the E.U. and the U.S. negotiated the Safe Harbor agreement in 2000 and managed to put their differences aside. This hybrid system of regulation authorizes the American companies abiding by the seven principles (notice, choice, onward transfer, security, data integrity, access and enforcement) to legally exchange information with Europe.

As mentioned before, the European Directive has had a strong influence on international privacy norms. Klosek (2007) pointed out that in addition to giving
privacy a strong importance, the E.U. also influenced very positively the development of privacy rights worldwide.

Heisenberg (2005) developed this reasoning further, arguing that because most European trading partners adopted comprehensive privacy legislation encompassing the European Data Protection principles, the European Union managed to set an international standard for privacy. Although only Canada, Argentina, Switzerland and Guernsey enacted privacy legislation recognized as adequate by the European Directive, Heisenberg argued that Latin America (e.g. Peru, Chile and Brazil), Japan and Australia have adopted regulations reflecting the European preferences. The Safe Harbor agreement remained an exception between Europe and America. Heisenberg also believes that Europe managed to set the privacy standards as the United States did not possess a competitive model of its own and thus could not impose its inclination. She suggested that because the European Union had the first-mover’s advantage, the Directive thus became an international norm.

Finally, Swire (1998) believes that the “Directive begins a new era. It has made the rules far more visible and has applied those rules to all member states. Some of its provisions are stricter than any current national rules. Perhaps most important, the process of agreeing on the Directive has given a new urgency and legitimacy within Europe to the enforcement of data protection rules” (None of your business, p42).
As numerous scholars have mentioned, the European Union appears to be better equipped to tackle the issue of privacy than the United States, which only enacted legislation when abuses could no longer be kept silent.

This issue of privacy is substantial, as it has repercussions on numerous levels, from the day-to-day life of a citizen, to international policy decision making. As such, it influences the behavior of both the United States and the European Union, impacting their national and international actions. The next part of this chapter will examine how the privacy issue is encompassed into the European and American national security policymaking and how the divergence in privacy perception affects the outcome of their security decisions.

**A different approach to privacy: implication for internal security**

The attacks of September 11 have triggered an immediate recognition of the need to improve national security in the United States and the European Union. However, as numerous scholars have expressed, each player opted for different approaches to prevent and counter terrorism. As Alexandre Adam (2005) and Daniel Hamilton (2006) explained, Europe chose to improve existing mechanisms and strengthen police and judiciary cooperation. On the other hand, the United States
reacted by increasing, among other provisions, the surveillance capacity of the
government. As such, the Bush Administration created new instruments and policies to
facilitate and expand federal agencies’ intelligence gathering and surveillance powers.

Rees (2006) explains this discrepancy by arguing that privacy is valued
differently depending on the extent of information control held by the authorities. In
Europe, governments centralize a fair amount of information on their citizens and
define strict rules on cooperation between Member States. Conversely, the U.S.
government holds less data on individuals and its attitude towards data privacy has
been more relaxed than that of Europe.

Anja Delgaard-Nielsen (2006) offers another hypothesis, suggesting that the
divergence in privacy policy occurs as both actors perceive the terrorism threat
disparately. Although this reasoning constitutes a valid approach, the issue of privacy
itself also needs to be addressed to complement these views. Indeed, as both the U.S.
and E.U. have a completely different estimation of privacy, they chose contrasting
models to reach equilibrium between security and privacy. The entities’ behavior
towards the adoption of certain national security policies will differ, sometimes
hindering transatlantic cooperation. The European Union, with its comprehensive
privacy legislation, tends to strike a fairer balance between privacy and security, and
thus traditionally adopts policies restricting civil liberties the least. On the other hand,
the United States, not relying on such developed regulations, clearly lets the balance tip in favor of security. Interestingly, the concept of threat perception advanced by Delgaard-Nielsen takes its entire signification here, as it adds another factor to the privacy and security debate. Depending on how high the European Union considers the threat, it will be more or less willing to give up privacy and shift its balancing.

National security in the United States

Although the American counter-terrorism legislation took an unprecedented turn after September 11, the United States had long included internal security matters in legislation. In April 1982, Ronald Reagan gave the first National Security Decision Directive entitled “Managing Terrorist Incidents.” Several directives followed, such as the Clinton presidential decision directive in 1992, dedicated to combating terrorism.

Several acts were also approved, e.g. the Foreign Intelligence Surveillance Act (FISA) passed in 1978, defining procedures for the physical and electronic surveillance and collection of foreign intelligence information in the United States. Another example of legislation is the Antiterrorism and Effective Death Penalty Act, adopted on 1996.
Concerns for privacy grew stronger and stronger in correlation to the faster development of security acts. However, the terrorist attacks of 2001 and the subsequent demands for greater internal security reduced the interest and legitimacy previously given to privacy advocacy groups. The reaction of the government was swift. Three days after the attacks on the World Trade Center and the Pentagon, President George W. Bush declared a state of emergency and drastically increased border control and surveillance. The Administration released the National Strategy for Homeland Security on September 17, 2002, developing eight objectives to reduce the risks of terrorism and enhance national security. Moreover, President Bush established in October 2001 the Office of Homeland Security (OHS) to coordinate the actions related to counter-terrorism. This organization was replaced by the Department of Homeland Security (DHS), following the signing of the Homeland Security Act on November 25, 2002. The DHS, merging 22 federal agencies into one, was created to improve coordination efforts and concentrate most of its activities on protecting the territory and the citizens against terrorist attacks.

Although numerous measures have been adopted in response to the September 11, 2001 attacks, the most discussed and controversial action taken by the government is the enactment of the Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act). This legislation,
approved by the U.S. Congress only six weeks after the attacks, mainly grants an increased authority to the government, expanding its power to spy on citizens, search and seize (Keenan, 2005). In December 2003, the Patriot Act was further enlarged allowing the FBI to request information from any third party and no longer be limited to traditional financial institutions.

Among its provisions, the Patriot Act allows the government to get a court order to enter homes and take property without notifying the owner until weeks or months later. It also gives the government access to sensitive information and increases the ability of law enforcement agencies to search telephone, e-mail communications and medical, business, financial and other records. In addition, the Patriot Act makes it illegal for providers of records to reveal that the FBI has searched or seized documents. Other articles of the Act are of controversial nature as well, such as the expansion and facilitation of the right to detain and deport immigrants suspected of terrorism-related acts. Following the adoption of this provision, deportation of foreigners (mostly Muslims and Arabs) as well as the number of non citizens’ arrests grew considerably (Keenan, 2005).

The Patriot Act also had repercussions on existing laws as it modified the Foreign Intelligence Surveillance Act of 1978 (FISA), Electronic Communications

Numerous scholars and civil liberty advocates have strongly criticized the Patriot Act for its recurrent violations of privacy and the elimination of judicial oversight of law-enforcement and domestic intelligence gathering. For instance, Giorgetti (Von Hipel, 2005) condemned the fact that “now both intelligence records and personal records can be collected without showing probable cause that a crime has been committed because when an investigation is directed at collecting evidence with a significant international anti-terrorism intelligence purpose, this by itself becomes a sufficient cause.” Adam (2005) described how the Patriot Act disregards privacy as he denounced the right given to the American authorities to detain foreigners without motive for 7 days. Rees (2006) deplored the decision to end the separation between information obtained by law enforcement and intelligence communities. Brimmer (Dalgaard-Nielsen, 2006) took another perspective, supporting the American Civil Liberties Union’s protests of the Patriot Act. As such, he criticized the detention and deportation policies, condemning the harsh condition of imprisonment.

---
Although the Patriot Act included numerous controversial initiatives, a relief could be found in the fact that most of these provisions were to expire by 2005, if not renewed. However, a massive public relations campaign was organized in support of the legislation and the Patriot Act was approved again on March 9, 2006, making the increased surveillance activity and data sharing between agencies long term policies (Klosek, 2007).

In *The War on Privacy*, Klosek (2007) stated: “while there has been a general decline in the focus on privacy rights, there has been a simultaneous increase in the focus placed on developing and implementing new mechanisms for aggregating, mining and sharing data” (Klosek, p44). This reasoning seems to be appropriate to the privacy and security balancing situation in the United States. Indeed, the American government did not stop this new wave of security reforms with the Patriot Act, but introduced several other projects following the same line and reducing privacy protections.

First of all, it would be a mistake to think that surveillance became prominent only in response to September 11. As mentioned before, the United States and especially the F.B.I. have been known for using surveillance technology extensively and sometimes inappropriately. For instance, the CARNIVORE program, allowing
internet wiretapping, was first used in 1999 (Klosek, 2007). Another controversial project is CAPPS, the Computer Assisted Passenger Profiling System, first developed in the late 1990’s. The program assigned a risk score to each airplane passenger, checking information obtained by Passenger Name Records against data stores, such as non-fly list profiles (Klosek, 2007)

It is true however, that the number of surveillance and data-mining projects drastically increased after the September 11 attacks. While some were terminated relatively quickly, due to the loud protests of privacy advocates, the government managed to pursue some of these works, sometimes using different sources of funding.

For instance, Dalgaard-Nielsen (2006) and Rees (2006) explained that in 2002, the White House proposed a pilot project called Operations TIPS (Terrorism Information and Prevention System), that would allow recruiting one million citizen volunteers in ten cities to report any “suspicious” activity. But by the end of the year, the Congress supported the public outrage and passed a law forbidding the implementation of the TIPS initiative.

Still in 2002, the U.S. introduced the Total Information Awareness (TIA) initiative. This program merged information from government and commercial databases and then matched the data against a terrorist profile to determine whether it
is suspicious. The Electronic Privacy Center (EPIC), one of the civil liberties groups criticizing the project, analyzed the issue and sent an alarming report to Congress in May 2003. The program, renamed Terrorism Information Awareness in May 2003 was officially terminated in September 2003. Although it was defunded by the Congress, the Pentagon outsourced its financial support to five states and TIA was incorporated into MATRIX, the Multistate Anti-Terrorism Information Exchange program (Klosek, 2007). MATRIX followed the same principles as TIA, using data mining tools to scan government and commercial records, in search of signs of terrorist activities or other wrongdoings. The MATRIX initiative was shut down in June 2005, after federal funding was cut in the wake of public concerns over privacy and state surveillance (Rees, 2006; Klosek, 2007).

Another controversial project came to the public attention in December 2005, as the New York Times published an article denouncing a program of warrantless domestic wiretapping, ordered by the Bush administration and carried out by the National Security Agency since 2002.

Furthermore, in 2003, the Transportation Security Administration (TSA) introduced CAPPS II, the successor of CAPPS I, which still checked the passenger information against comprehensive terrorist watch lists but gathered more data than its predecessor. In response to the significant opposition from watchdog groups like the
American Civil Liberties Union (ACLU), EPIC and ReclaimDemocracy.org which believed the program would undermine both privacy and safety and may be unconstitutional, CAPPS II was terminated in August 2004. Immediately, a similar passenger prescreening program was introduced under the name of Secure Flight, with the only difference that it would no longer compare passenger name records against commercial databases (Klosek, 2007). Due to important concerns over privacy and civil liberties weaknesses, the initiative was suspended in 2006. However, the Transportation Security Agency kept working on the project, and in August 2007 it published a Notice of Proposed Rulemaking (NPRM), proposing the implementation of an improved Secure Flight program. EPIC, among other advocacy groups, still believes that the program should remain grounded.

In addition to reducing privacy rights protections, the information gathering and surveillance programs discussed above are strongly criticized for the impact that mistakes and errors can have on travelers. Indeed, a passenger unjustly included on a terrorist watch list will encounter difficulties through customs and could be refused the entry into American territory without any true reason.

In terms of border security, the DHS developed the U.S. VISIT program (United States Visitor and Immigrant Status Indicator Technology), designed to monitor the pre-entry, entry, status and exit of foreign nationals in the United States
and enhance national security. The Patriot Act strongly reformed this program used for passenger profiling, as it added a biometric component to non-U.S. citizens’ passports. Since January 5, 2004, foreign travelers are now required to have fingerprints and digital photographs collected at 115 airports and 15 major seaports (Rees, 2006).

This overview of the American internal security strategy emphasizes the fact that the United States often tips the balance in favor of security. Although civil liberties advocates constantly denounced abuses of the security acts, the citizens’ privacy rights tend to be put aside by the priority given to surveillance and safety. Paradoxically, the Security Strategy for Homeland Security of September 2002, aiming at eliminating the terrorism threats, dedicated its first objective to the promotion of liberty, declaring that the U.S. will “champion aspirations for human dignity” and “advance freedom.”

Finally, this inconsistency is reinforced by the fact that the U.S. offensive actions and invasive legislation need to respect the privacy and civil liberty of the American citizens in the first place in order to be seen as legitimate (Winer, Dalgaard-Nielsen, 2006). This explains the strong criticism drawn from the European community.

---

regarding certain American policies and the lack of aspiration of some countries to follow American initiatives. Indeed, as the European Union adopted security measures, it seemed more inclined to grant privacy a greater importance than in the United States.

**National security in Europe**

The European Union has a long tradition of dealing with terrorism. Accordingly, a legislative framework was already in place long before the attacks on the World Trade Center (Adam, 2005). At the national level, several European countries had enacted their counter-terrorism laws balancing the concept of privacy in varying degrees: Italy, in response to the *Brigate Rosse* movement, France, to fight Algerian terrorist groups, Spain against the *ETA* Basque nationalist separatist organizations and the U.K., in response to terrorist attack carried out by the Irish Republican Army. These efforts were expanded at the European level with the creation in 1975 of the TREVI Group, which harmonized the defense initiatives and the national balances between privacy and security. This organization, named after the French acronym *Terrorisme, Radicalisme, Extremisme, Violence Internationale*, increased this internal security cooperation by coordinating national policies and
practices (Von Hippel, 2005). The TREVI group laid the foundation for Europol, which later became the European intelligence agency.

Finally, the special E.U. meeting in Tampere of October 1999 set up the European Union’s Area of Freedom, Security and Justice (including borders, internal security and criminal matters) as one of the fundamental objectives of the E.U.

In *Europe and Counterterrorism*, Kristin Archick (2003) described the main security decisions made by the European Union in response to the World Trade Center attacks. She distinguished three domains where the Member States have agreed to cooperate.

First of all is the enhancement of justice and police cooperation. Immediately after September 11, 2001, the European Union took several initiatives to carry out these goals. First of all, on September 13, the Member States decided on a common definition of terrorism and the penalties associated with it. This issue had long been discussed, but the attacks on the World Trade Center accelerated the process. Moreover, the European Union agreed on a list of terrorist organization the same year and the implementation of the European Arrest Warrant by 2004.

On September 20, the European Union adopted an action plan to fight terrorism. This document, consisting of 7 priority measures to implement, is once more
mostly dedicated to the strengthening of instruments and cooperation within spheres of police, justice and intelligence, more than the development of decisive security measures restricting privacy. As Dalgaard-Nielsen (2006) and Stevenson (2006) point out, only one of these seven issues was actually a direct response to 9/11 and of protective nature: the clause dealing with air transport security. Dalgaard-Nielsen (Winer, 2006 p 112) explains: “Vulnerability reduction and civil protection remains of relatively low priority. The post March 11 endorsement of solidarity clause and the appointment of an anti-terrorism coordinator indicate a dawning interest in the protective side of homeland security but concrete common and binding action remain limited due to diverging threat assessments, jealously guarded national competencies and arguably the lack of a strong coordinating center to prioritize and drive the E.U. effort and the numerous actors and agencies involved.”

In 2002, the E.U. expanded the powers of Europol by allowing the organization to launch specific criminal investigation in addition to its role of information clearinghouse.

Finally, Eurojust was established in 2002 and is designed to improve and facilitate judiciary cooperation (Von Hippel, 2005)
The second main cooperation area concerns the suppression of terrorism funding. In 2002, the Member States agreed on an E.U.-wide asset freezing order and in October 2005, the European Union adopted an expanded Money Laundering Directive.

The last field of increased collaboration regards the strengthening of external European border controls. Since the E.U. is welcoming new members and thus expanding its geographic limits to countries which sometimes do not have a high level of border protection, the Member States enhanced their efforts in security at the European boundaries. As a result, in 2002, the European Union introduced the External Border Management Plan to curb illegal immigrations. Moreover, in February 2002, the Member States agreed to implement Eurodac, a fingerprinting database of asylum-seekers. Finally, in April 2002, the E.U. established a visa database to improve coordination and control of visitors.

These various initiatives taken by the European Union following the attacks on the World Trade Center underline the importance given to both security and privacy. But unlike the United States, which clearly favors security even if it strongly reduces privacy safeguards, the Member States seemed to look for a better equilibrium. As
such, the global approach taken by the E.U. would be to try to ensure the most security and limiting privacy trade-offs.

However, although most of these security decisions reflect a preference for an improvement of judiciary and police cooperation with less emphasis on privacy weakening policies, the European Union has also adopted other agreements that impact more on civil liberties. For example, the Passenger Name Record (PNR) agreement signed with the United States in 2007 offers a relatively low protection of personal information. Likewise, in 2004, Member States agreed to incorporate several biometric identifiers in the European passport within the next few years.

It is however interesting to point out that although the European Union acts as an entity, the reactions to September 11 varied depending on the country. As a result, some states opted for tight security legislation while other maintained a better balance with civil liberties, in accordance to the national social norms on privacy and security (Koslowski, Dalgaard-Nielsen, 2006). Surely, Von Hippel (2005) stressed that “the UK passed policies to restrain civil liberties of foreigners, and other states took the opportunity to implement legislation to address long-standing concerns, such as immigration and evidence collection and to act against asylum-seekers.”
**Conclusion: shifting the European equilibrium**

This chapter has pointed out the fundamental differences in which the United States and the European Union approach security and privacy. While the lawmaking process was sped up in the European Union to adopt efficient security tools and still encompass privacy concerns, the United States realized an extensive concentration of powers at the federal level, expanding surveillance (Adam, 2005). Rees (2003) argued that these differences originate from the disparity between American and European cultures, saying that “while the European values are based on law enforcement and judicial process (which leads to demands of accountability and civil liberties), the United States relies on surveillance agencies and national security.”

The clash between the American and European privacy and security approaches became sensitive as transatlantic cooperation started to be necessary to combat multinational terrorism. On one side, the U.S. pressured the E.U. to loosen its privacy policies, arguing that the European legislation was too strict and impeded on international law enforcement requirements (Rees, 2003). On the other side, the Member States demanded that America consider and respect the European privacy regulations (Winer, Dalgaard-Nielsen, 2006).

Rees (2003) underlined the tremendous American strengths, stating that he U.S. and the E.U. are unequal partners, the United States acting as an imperial power and
regarding itself as the guardian of international order. Klosek (2007) also expressed her concern over the powerful influence of the United States, stressing that the E.U. has been under increasing pressure from the U.S. authorities to participate in efforts to combat terrorism by disclosing personal data regarding European citizens. Following this reasoning, one could then wonder how the European Union could possibly resist such pressure.

Rees (2003) argued that the European Union is often forced to comply with the American demands. For instance, a month after the September 11 attacks, George W. Bush sent a letter to the President of the European Commission Romano Prodi, describing 47 acts Europe should carry out in order to support the United States in its fight against terrorism. The United States demanded that the European members “consider data protections issues in the context of law enforcement and counterterrorism imperatives” and “revise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period” (Klosek, 2007, p92). The pressure intensified steadily. For instance, at the European Union forum on Cybercrime taking place on November 27, 2001, the American Department of Justice suggested that “data protection regime should strike an appropriate balance amount of the protection of personal privacy, the legitimate needs

62
of service providers to secure their networks and prevent fraud, and the promotion of public safety” (Klosek, 2007, p92).

The Americans also enlarged the scope of their insinuations to international forums. Indeed, at the May 2002 G8 meeting, the U.S. representation requested that countries ensure “that data protection legislation, as implemented, takes into account public safety and other social values in particular by allowing retention and preservation of data important for network security requirements, law enforcement investigations or prosecutions, and particularly with respect to the internet and other emerging technologies” (Klosek, 2007, p92).

As Rees (2003) points out, the U.S. made it clear that it wanted extraterritorial control over people and goods, going from the E.U. to its territory. But the author also considered that although the E.U. demonstrated its unease with the American approach towards enhancing domestic security, the “suggestions” made by the U.S. have been taken into account. Indeed, Rees believes that most of the cooperation agreements signed by the U.S. and the E.U. are directed only in one direction, clearly favoring the American preferences. John Occhipinti (2006) shares these views as he presents the case of the U.S.-Europol agreement as an example. Passed in December 2001, the arrangement allowed transfer of strategic and technical information but did not include personal information. Europol’s data protecting rules specified that Europe could not
share personal information with countries or organizations that did not have a singular supervisory data protection authority similar to its own. In 2002, the agreement was amended to include personal data, reflecting the American preferences.

In general, scholars tend to believe that the European Union is becoming more and more security oriented, shifting the balance away from civil liberties priorities. Although the privacy legislation in Europe remains in effect, the Member States seem to increasingly follow the American initiatives. The latest decisions to adopt biometric passports and to implement a European fingerprints database by the end of 2008, and the talks regarding the creation of a European Passenger Name Record system, reinforce the impression that the E.U. is changing its positioning.

This new trend takes us back to the question analyzed in this thesis: why has the European Union been giving more and more attention to security at the expense of civil liberties? The background information provided in this chapter has described the privacy and security foundations of the U.S. and the E.U.. It has also shown that the major force influencing this change seems to be coercion from the United States, an argument commonly shared. Although the European Union negotiated for more privacy, according to several scholars, it failed to make itself heard. What is more, in
some cases the American pressure seems so intense and the threats so clear that it appears impossible for Europe to resist.

However, looking at coercion as the only force influencing the European change would not provide a full understanding of the political dynamics at play. As mentioned in Chapter Two, other factors of policy change greatly impact the E.U. shift in positioning. This thesis argues that European interests have changed, constituting a crucial influence in the adoption of American policies and altering the general debate. The next chapter will demonstrate this argument by applying the theories selected in the previous chapter to two cases studies: the Passenger Name Record debate and the data retention directive.
Chapter Four: Presentation of the case studies

This chapter will introduce the two case studies developed in this thesis, pointing out the importance of American coercion in decisions on European security matters, as well as the internal debates going on at the European level.

In 2001, Passenger Name Record (PNR), gathering traveler’s journey information, became at the focus of a vigorous debate as the U.S. required European air carriers to hand these data to American Customs, which contradicted the European Union’s 1995 Privacy Directive. After several years of negotiations, the E.U. agreed in July 2007 on the transfer of PNR, which was widely perceived as a response to American pressure and influence.

However, coercion cannot alone explain the European shift in balance, as the second case study, the Data Retention Directive, demonstrated the same trend but was only debated at the European level. When the need for harmonization of data retention legislation surfaced following the September 11 attacks, the Member States and the European institutions appeared divided on how to address the issue. However, the Madrid and London bombings reinforced the urgency of adopting mandatory data retention legislation and despite critics from Data Protection Authorities and privacy
advocates, the European Union finally introduced a Data Retention Directive in March 2006.

These two case studies will be developed in greater detail in the following sections. They will demonstrate that Europe has clearly shifted its balance between privacy and security, due to American coercion as well as European internal dynamics pressing for more security.

The Passenger Name Record Agreement

A Passenger Name Record, referred to as PNR, is a file created by airline companies comprised of information on each passenger and his/her journey (e.g. name, billing information, address, meal preference etc.). Located in the airline’s reservation and departure control database, the PNR will allow the different agents within the air industry to recognize the passenger it is associated with, and the relevant information about his/her trip (European Commission MEMO/07/294, 2007).
The debate surrounding PNR started in 2001, due to the U.S. Air and Transportation Security Act, which was enacted on November 19 of that year. After the attacks on the World Trade Center, the U.S. government expanded surveillance and determined that PNR data constituted valuable tools of investigation in the fight against terrorism. As a result, the Air and Transportation Act required that every air carrier make PNR data available to the Bureau of Customs and Border Protection (CBP) and the Transportation Security Agency (TSA), 15 minutes prior to each plane’s takeoff.

However, the requirements of the Act conflicted with the European Privacy legislation and placed the European airline companies in a difficult situation. Indeed, Article 25 of the 1995 Data Protection Directive only allows the transfer of data between the European Union and a country with similar level of privacy protection. As mentioned before, the United States does not fulfill the required conditions to access European data, outside the framework of the Safe Harbor Agreement. In early 2002, the European Commission reiterated the fact that transfer of PNR to the U.S. was illegal. As a result, the European air carriers found themselves stuck between breaching the American law or the European Directive. In any case, they faced
sanctions from the E.U. and potential prosecution by European citizens or the loss of landing rights and a $6000 fine per passenger, threatened by the U.S. in case of non-compliance.

*U.S. Interim Rules, June 2002*

In addition to the previous requirements, the CBP released interim rules in June 2002, emphasizing the necessity of using PNR as a mean to ensure aviation safety and national security. They demanded that each airline company provide CBP with electronic access to the PNR, contained in European databases. According to these rules, the air carriers were responsible for ensuring the good functioning of the interface. Moreover, CBP also pointed out that the PNR data will no longer only be accessed by TSA and CBP, but could also be shared with other governmental agencies upon request.

Following numerous talks with the European Union, the U.S. decided to postpone the entry into force of these new requirements as a sign of good faith. Accordingly, these measures and the waiving of the imposition of penalties on non-complying airlines were not implemented on November 14, 2002, as first planned, but on February 5, 2003 (Patten, 2003).
Areas of disagreement

The most outspoken European critics of the PNR agreement focus on six major points:

First, one of the Data Protection Directive’s main principles states that data can only be used for the purpose for which it has been collected. In the case of PNR, the data are gathered by the airline companies for commercial purposes. But by requesting the information in the framework of counter-terrorism legislation, the United States would use PNR for a different purpose than the one originally stated. This would thus constitute a breach in the European Directive.

Second, the use of PNR sensitive data (i.e. information specifying political beliefs, racial and ethnic origins) by the United States represented a strong violation of human rights and was vehemently criticized by the opponents of the PNR agreement.

Third, privacy advocates argued that control over the data transferred was almost non-existent. Indeed, CBP and TSA insisted on being able to share PNR with other federal agencies as they saw fit. They were not even required to inform the European Union of such disclosure of information.

Fourth, the Article 29 Working Party considered that the original request of 39 PNR fields by the U.S. was disproportionate and only 20 were justified. According to
the Limitation principle of the European Data Protection Directive, the collection of data must be limited to the minimum necessary. In this case again, the current state of the agreement would breach the European law.

Fifth, the European Parliament criticized the “pull” system proposed by the United States, which consisted in granting CBP full access to the European databases to collect PNR. Instead, the Members of European Parliaments (MEPs) favored a “push” system, where the air carriers would send the PNR data to the U.S. upon request, which would reduce the control and access of the United States government.

Finally, the PNR agreement opponents stated that retaining PNR data for 50 years as the American authorities requested was disproportionate and they demanded the time period be reduced.

Other controversial aspects of PNR regarded the use to which the data are put (e.g. profiling) and access, processing, use and protection of the PNR information. The legitimacy of such U.S. demands was also questioned. For instance, in an Opinion published in October 2002, the Article 29 Working Party recognized “that sovereign States do have discretion over the information that they can require from persons wishing to gain entry to their country” but still “wondered, in this regard, as to whether
such unilaterally adopted measures may be compatible with the international agreements and conventions\textsuperscript{12}.”

\textit{Joint Statement, February 2003}

Given the urgency of the situation, senior officials of European Commission and the United States Administration met on February 17-18, 2003, to work on an agreement answering the concerns of both parties, namely the respect of privacy and the need for security. After the meeting, they issued a Joint Statement, where they presented the current state of the negotiations and outlined the modifications the U.S. needed to accomplish in order to obtain an adequacy decision from the Commission.

Both parties agreed on several points. First of all, the U.S. Customs was to respect the principles of the Data Protection Directive. Secondly, the U.S. and the E.U. were to jointly develop measures protecting data of a sensitive nature (e.g. religious, ethnic and racial characteristics), preferably before March 5, 2003. Together, CBP and the European Commission would assess the implementation of this Joint Statement as well as potential improvements on a regular basis. Finally, U.S. Customs would be

allowed to transfer data to other US law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offenses, upon request.

This temporary arrangement allowed the transfer of PNR from the E.U. to the U.S. The European Commission also mentioned that, starting March 5, it would temporarily suspend prosecution of any air carrier transferring PNR to the United States. As a result, even without an official agreement, most major European air carriers started communicating passengers’ information to CBP (Foucart, 2004). Finally, both the E.U. and the U.S. agreed on the fact that a long term multilateral agreement was necessary.

Following another meeting on March 4, 2003, CBP gave additional Undertakings, agreeing not to use sensitive PNR data and to implement a special filter with the least possible delay as an additional protection. These Undertakings reiterated the crucial point defended by the U.S. that CBP and TSA would be allowed to share the data with other federal agencies dealing with counter-terrorism activities.

On March 12, Commissioner Chris Patten presented the situation to the European Parliament, emphasizing that the Commission obtained from the United States an additional set of Undertakings incorporating European concerns (Patten,
However, Patten’s address did not convince the Parliament, as the following day the MEPs adopted a resolution strongly criticizing the American requirements and the general development of the debate.

U.S. Undertakings of May 2004

On May 22, 2003, following the request of the European Commission, the U.S. Customs Service and TSA presented a set of new Undertakings. Several of the provisions had already been discussed (i.e. purpose of PNR collection as a tool to prevent and combat terrorism and serious criminal offenses or treatment of sensitive data) but clarifications or new clauses were introduced. The Undertakings stated that PNR data would be “pulled” by CBP until a “push” system could be implemented and the data retention of PNR was set to 3.5 years in active form and then 8 years as dormant. Moreover, the United States agreed to reduce the number of PNR fields required from 39 to 34. These new engagements aimed at soothing European privacy concerns and obtaining an adequacy decision from the European Commission. As a result, the Undertakings acknowledged the European Data Protection Directive and included several concessions.

The next table presents in greater detail the main Undertakings.
<table>
<thead>
<tr>
<th>Undertaking</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undertaking 1</td>
<td>Each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide CBP (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and maintained in the air carrier's automated reservation/departure control systems (“reservation systems”).</td>
</tr>
<tr>
<td>Undertaking 12</td>
<td>With regard to the PNR data, CBP personnel (previously) directly from the air carrier’s reservation systems for purposes of identifying potential subjects for border examination, CBP personnel will only access (as necessary) and use PNR data concerning persons whose travel includes a flight into or out of the United States.</td>
</tr>
<tr>
<td>Undertaking 13</td>
<td>CBP or TSA will “pull” passenger information from an air carrier until such time as an air carrier is able to implement a system to “push” the data to CBP or TSA.</td>
</tr>
<tr>
<td>Undertaking 14</td>
<td>CBP will pull PNR data associated with a particular flight no earlier than 72 hours prior to the expected departure of that flight, and will re-access the systems no more than three (3) times between the initial pull, the departure of the flight from a foreign point and the flight’s arrival in the United States, as between the initial pull and the departure of the flight from the United States, as applicable, to identify any changes in the information. In the event that the air carrier obtains the ability to “push” PNR data, CBP will need to receive the data 72 hours prior to departure of the flight, provided that all changes to the PNR data which are made between that point and the time of the flight’s arrival in or departure from the U.S., are also pushed to CBP.</td>
</tr>
<tr>
<td>Undertaking 15</td>
<td>CBP will limit on-line access to PNR data to authorized CBP users for a period of seven (7) days, after which the number of users authorized to access the PNR data will be even further limited for a period of three years and 6 months (3.5 years) from the date the data is accessed (or received) from the air carrier’s reservation system. After 3.5 years, PNR data that has not been manually accessed during that time will be destroyed. PNR data that has been manually accessed during the initial 3.5 year period will be transferred by CBP to a dedicated forensic file, where it will remain for a period of eight (8) years before it is destroyed. This schedule, however, would not apply to PNR data that is linked to a specific enforcement record (such data would remain accessible until the enforcement record is archived).</td>
</tr>
<tr>
<td>Undertaking 28</td>
<td>Without the exception of transfers between CBP and TSA (which jointly make representations herein in support of the European Commission’s Decision and have independent legal authority within the PNR data), Department of Homeland Security (DHS) components shall be treated as “third parties,” subject to the same rules and conditions for sharing of PNR data as other government authorities outside DHS.</td>
</tr>
<tr>
<td>Undertaking 29</td>
<td>Under this undertaking, CBP will provide PNR data to other government authorities, including foreign government authorities, with counterterrorism or law enforcement functions, in a case-by-case basis, for purposes of protecting and combating offenses.</td>
</tr>
<tr>
<td>Undertaking 35</td>
<td>No statement of these undertakings shall impair the use or distribution of PNR data for criminal, judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any U.S. legislation which materially affects the undertakings made in these undertakings.</td>
</tr>
<tr>
<td>Undertaking 43</td>
<td>CBP, in conjunction with DHS, undertakes to conduct once a year, or more often if agreed by the parties, a joint review with the European Commission, escorted by representatives of European law enforcement authorities and/or authorities of the Member States of the European Union, on the implementation of these Undertakings, with a view to mutually contributing to the effective operation of the procedures described in these Undertakings.</td>
</tr>
<tr>
<td>Undertaking 45</td>
<td>These Undertakings shall apply for a term of three years and six months (3.5 years). After these Undertakings have been in effect for two years and six months (2.5 years), CBP, in conjunction with DHS, will initiate discussions with the Commission on the possible extension of these Undertakings, and any agreement reached shall be mutually acceptable to the parties, and mutually acceptable arrangement can be concluded prior to the expiration date of these Undertakings, the Undertakings will cease to be in effect.</td>
</tr>
<tr>
<td>Undertaking 47</td>
<td>These Undertakings do not create or confer any right or benefit on any person, party, private or public.</td>
</tr>
<tr>
<td>Undertaking 48</td>
<td>The provisions of these Undertakings shall not constitute a procedure for any future discussions with the European Commission or the European Union, any related entity, or any third State regarding the transfer of any form of data.</td>
</tr>
</tbody>
</table>
On the other side, several of these Undertakings are particularly controversial. Indeed, Undertaking 47 states that these provisions constitute a statement of intent but cannot be relied on in a court of law. Moreover, Undertaking 35 says that a change in the American legislation requiring PNR data to be used for other purposes would override the Undertakings (House of Lords, 2007).

These critics were reflected by the Article 29 Data Protection Working Party’s Opinion adopted on June 13, 2003, discussing the level of protection ensured in the U.S. regarding the current proposition of PNR transfer. The Privacy representatives concluded that the U.S. Undertakings were still not sufficient to meet the adequacy standards and that further improvements were necessary.

However, six months later, the European Commission presented the details of a PNR agreement reached with the United States. Frits Bolkestein, the Commissioner for Internal Market & Services and in charge of the PNR debate, argued that the U.S. had offered substantial concessions and had move significantly from the initial position. On January 29, 2004, the Article 29 Working Party once more expressed the view that the American compromises still did not constitute a valid data protection framework.
Little changed between January and May 2004, but the Commission still adopted an Adequacy Decision on May 14, 2004, declaring that the U.S. Undertakings provided a sufficient protection of PNR data. Three days following this declaration, the Council adopted a Decision authorizing the signature of the PNR Agreement with the United States, on behalf of the European Community.

In this Agreement, the United States conceded to reduce the number of PNR data fields to 34, interestingly dropping 4 categories the Article 29 Working Party had approved before (House of Lords, 2007). The data retention time was also set at 3.5 years. Both the United States and the European Union also mentioned that the Agreement and the Undertakings would be reviewed annually by European and American representatives, as well as Data Protection Authorities. However, the European Parliament and the Data Protection Authorities still criticized the ambiguous wording of several clauses, the unclear list of U.S. authorities and agencies accessing the data (Schrader, 2006), the lack of explicit guarantees, and the fact that it was impossible for a citizen to appeal to an independent authority in cases of passengers’ right infringement. Finally, the agreement did not offer any safeguard against the U.S. changing the nature of their Undertakings.
The European Court of Justice Ruling, May 30, 2006

The adoption of the PNR Agreement by the European Commission and the Council angered the European Parliament, the Data Protection Authorities and the civil liberties advocates. The European Parliament, with the support of the European Data Protection Supervisor (EDPS), applied to the Court of Justice of the European Communities to obtain an annulment of the Council decision (Case C-317/04) and of the decision on adequacy (Case C-318/04). The MEPs argued that the Agreement was contrary to Article 8 of the Convention on Human Rights, as it unreasonably interfered with private life and allowed the transfer of a disproportionate quantity of PNR data held for an excessive length of time (Archer, 2006).

The Court of Justice finally cancelled both Decisions on the basis that the European Commission did not have the authority to give an adequacy decision, determining that the PNR issue fell into the scope of the third pillar. A brief description of the European Union’s structure is required here to understand the implication of the Court of Justice’s decision. The European Union is based on three pillars. In the first (internal market), integration is most developed since decisions are made by the European institutions: the Commission, Council and Parliament, and the resulting decisions are subject to review by the European Court of Justice. However, in the field
of policy and judicial cooperation in criminal matters (third pillar), the member States have not adopted such a deeply integrated model. As a result, on law enforcement matters the governments work together to find consensus on key issues, without working through European institutions, such as the Commission or the Parliament, and without strict judicial review (Schrader, 2006).

In the case of PNR, the European Court adopted its ruling by defining under which jurisdiction the agreement fell, either the European Community (first pillar), or the cooperation in criminal matters (third pillar). Although the collection of PNR by airline companies fell into the scope of the European Community as the sale of a plane ticket, the data processing was regarded as a necessity for safeguarding public security and thus fell into the scope of the third pillar. As a result, the European Commission and the European Council did not have the authority to sign the PNR agreement and the Court of Justice cancelled both decisions.

While at first this could be perceived as a victory for the European Parliament, in reality it is not. Indeed, the Court of Justice did not even address the issue of privacy and data protection but only discussed the Commission’s legal authority. Moreover, by deciding that PNR fell into the scope of the third pillar, the Court of Justice ruled out any kind of involvement of the Parliament, as only the governments of the Member States would make the PNR agreement decision unanimously. The Parliament would
no longer have the opportunity to even officially express its recommendations (The Economist, 2006).

Finally, the European Commission argued that the Court of Justice ruling actually supported their position, as Friso Roscam Abbing, spokesman for Commissioner Franco Frattini, said: “It is important to recognize that the court did not object to the content of the legislation, which is completely compatible with data protection rules” (Bilefsky and Clark, 2006).

The PNR Interim Agreement of October 2006

As the Court of Justice ruled that the decision on adequacy would only remain in effect until September 30, 2006, the European Union and the United States had only less than three months to sign a new agreement based on the third pillar.

The negotiations on the Interim Agreement were completed on October 6, 2006, and on that day, the Council adopted a Decision authorizing the Presidency to sign the new Agreement. This accord strongly resembled the previous agreement in terms of scope, data retention length, use of PNR and number of fields required (34).

---

13 D. Bilefsky & N. Clark. (2006, September 1). EU and U.S. plan deal to share traveler data; wide - ranging accord expected in weeks. The International Herald Tribune, pp. 4
However, it no longer included a mandatory joint review of the Agreement and Undertakings.

As this temporary accord expired on July 31, 2007 unless extended by mutual understanding, both parties started negotiating a final agreement early in 2007. Because of its similarity to the first PNR agreement signed in 2004, the United States was satisfied by the current situation and had almost no incentive to negotiate by July 31 a stricter agreement or even any agreement at all. Given this situation, the European Union had little leverage to ask for significant improvements of the current accord (Schrader, 2006).

**PNR Agreement of July 2007**

As a result of these dynamics, the final PNR Agreement, approved on July 23, 2007 and valid for 7 years, did not consistently changed from the 2004 and Interim accords. The new agreement included several compromises from the United States, but it was still condemned by the privacy advocates.

The PNR Agreement is composed of three parts: the actual agreement signed by both parties, a letter sent by the U.S. to the E.U. setting out assurances as to the way
in which it will handle E.U. PNR data, and a letter from the European Union to the Americans, acknowledging receipt of the assurances and confirming that, on this basis, it considers the level of protection of PNR data in the United States as adequate.

The PNR agreement and the letters present several major safeguards as well as limitations compared to the first Agreement passed in 2004.

First, no later that January 1, 2008, the European airlines would be required to “push” PNR data to CBP thus replacing the “pull” system still in place. This Article introduced a concrete deadline for the switch of system, a missing requirement in the previous agreement. However, it also indicated that after this date, if the air carrier did not implement a system in compliance with U.S. requirements, the “pull” mechanism would remain in place. In addition, the United States still constitutes the only deciding party on what, when and to whom information should be pulled. But by agreeing for the implementation of a “push” system, the U.S. still made a substantial concession. Indeed, although American authorities said that with the “pull” system they would only take PNR data, they could actually have looked at other information located in the European air carrier databases. Since the “push” system does not give authority to the U.S. to access the PNR data, all the records of European airline companies comport better data protection safeguards than provided by the “pull” system.
Second, the fields of PNR data collected were reduced to 19, instead of the 34 specified in the Interim agreement. However, this concession was strongly criticized by privacy advocates as a manipulation from the United States. Indeed, by looking at the list of data in the Interim and 2007 Agreements, one would see that almost the same amount of information is requested and the wording has just been altered to fit into 19 categories instead of 34 or 39.

The following chart demonstrates this, as only the categories underlined in yellow have been deleted, while the ones in blue have just been combined with other categories, resulting in fewer fields:
Table 3: Comparison of required PNR fields of data in the 2003, 2006 and 2007 Agreements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- PNR record locator code</td>
<td>- PNR record locator code</td>
<td>- PNR record locator code</td>
</tr>
<tr>
<td>- Date of reservation</td>
<td>- Date of reservation</td>
<td>- Date of reservation/issue of ticket</td>
</tr>
<tr>
<td>- Date(s) of intended travel</td>
<td>- Date(s) of intended travel</td>
<td>- Date(s) of intended travel</td>
</tr>
<tr>
<td>- Name</td>
<td>- Name</td>
<td>- Name(s)</td>
</tr>
<tr>
<td>- Other names on PNR</td>
<td>- Other names on PNR</td>
<td>- Other names on PNR, including number of travelers on PNR</td>
</tr>
<tr>
<td>- Number of travelers on PNR</td>
<td>- Number of travellers on PNR</td>
<td>- Available frequent flyer and benefit information (i.e., free tickets, upgrades, etc)</td>
</tr>
<tr>
<td>- Seat information</td>
<td>- Seat information</td>
<td>- All available contact information</td>
</tr>
<tr>
<td>- Address</td>
<td>- Address</td>
<td>- All available payment/billing information</td>
</tr>
<tr>
<td>- All forms of payment information</td>
<td>- All forms of payment information</td>
<td>- Travel itinerary for specific PNR</td>
</tr>
<tr>
<td>- Billing address</td>
<td>- Billing address</td>
<td>- Travel itinerary for specific PNR</td>
</tr>
<tr>
<td>- Contact telephone numbers</td>
<td>- Contact telephone numbers</td>
<td>- Travel itinerary for specific PNR</td>
</tr>
<tr>
<td>- All travel itinerary for specific PNR</td>
<td>- All travel itinerary for specific PNR</td>
<td>- Travel itinerary for specific PNR</td>
</tr>
<tr>
<td>- Frequent flyer information (limited to miles flown and address(es))</td>
<td>- Frequent flyer information</td>
<td>- Travel itinerary for specific PNR</td>
</tr>
<tr>
<td>- Travel agency</td>
<td>- Travel agency</td>
<td>- Travel agency/travel agent</td>
</tr>
<tr>
<td>- Travel agent</td>
<td>- Travel agent</td>
<td>- Code share PNR information</td>
</tr>
<tr>
<td>- Code share PNR information</td>
<td>- Code share PNR information</td>
<td>- Code share PNR information</td>
</tr>
<tr>
<td>- Travel status of passenger</td>
<td>- Travel status of passenger</td>
<td>- Split/divided PNR information</td>
</tr>
<tr>
<td>- Split/Divided PNR information</td>
<td>- Split/Divided PNR information</td>
<td>- Split/divided (PNR) information</td>
</tr>
<tr>
<td>- Identifiers for free tickets</td>
<td>- Identifiers for free tickets</td>
<td>- Travel status of passenger</td>
</tr>
<tr>
<td>- One-way tickets</td>
<td>- One-way tickets</td>
<td>- Ticketing information</td>
</tr>
<tr>
<td>- Email address</td>
<td>- Email address</td>
<td>- Baggage information</td>
</tr>
<tr>
<td>- Ticketing field information</td>
<td>- Ticketing field information</td>
<td>- Seat information</td>
</tr>
<tr>
<td>- ATFQ fields</td>
<td>- ATFQ (Automatic Ticketing Fare Quote) fields</td>
<td>- General remarks including OSI, SSI and SSR information</td>
</tr>
<tr>
<td>- General remarks</td>
<td>- General remarks</td>
<td>- Any collected APIS information</td>
</tr>
<tr>
<td>- Ticket number</td>
<td>- Ticket number</td>
<td>- All collected APIS information</td>
</tr>
<tr>
<td>- Seat number</td>
<td>- Seat number</td>
<td>- All historical changes to the PNR</td>
</tr>
<tr>
<td>- Date of ticket issuance</td>
<td>- Date of ticket issuance</td>
<td>- All historical changes to the PNR</td>
</tr>
<tr>
<td>- Any collected APIS information</td>
<td>- Any collected APIS</td>
<td></td>
</tr>
<tr>
<td>- No show history</td>
<td>- No show history</td>
<td></td>
</tr>
<tr>
<td>- Number of bags</td>
<td>- Number of bags</td>
<td></td>
</tr>
<tr>
<td>- Bag tag numbers</td>
<td>- Bag tag numbers</td>
<td></td>
</tr>
<tr>
<td>- Go show information</td>
<td>- Go show information</td>
<td></td>
</tr>
<tr>
<td>- Number of bags on each segment</td>
<td>- Number of bags on each segment</td>
<td></td>
</tr>
<tr>
<td>- OSI information</td>
<td>- OSI information</td>
<td></td>
</tr>
<tr>
<td>- SSI information</td>
<td>- SSI information</td>
<td></td>
</tr>
<tr>
<td>- SSR information</td>
<td>- SSR information</td>
<td></td>
</tr>
<tr>
<td>- Voluntary/involuntary upgrades</td>
<td>- Voluntary/involuntary upgrades</td>
<td></td>
</tr>
<tr>
<td>- Received from information</td>
<td>- Received from information</td>
<td></td>
</tr>
<tr>
<td>- All historical changes to the PNR</td>
<td>- All historical changes to the PNR</td>
<td></td>
</tr>
</tbody>
</table>
Another important clause of the final PNR Agreement is data retention. Whereas this period was set to 3.5 years in active state in the 2004 and Interim agreements, the final data retention length selected is 7 years. The dormant status of 8 years remains the same. The CNIL also argued that the data would now be kept for 15 years with no guarantee that the files not consulted will be destroyed (CNIL, 2007).

Moreover, although privacy advocates pushed for PNR data collection to be solely for the purpose of preventing and combating terrorism, “other serious offences” were included as well.

Regarding sensitive data, the United States reiterated its commitment to implement filters, but still reserved the right to access these data in exceptional cases. If such exception should occur, the United States would notify the Commission. The 2007 Agreement provides a definition of “exceptional cases” as “where the life of a data subject or of others could be imperiled or seriously impaired.” However, it still remains unclear as to who makes this decision and on which criteria.

Finally, the 2007 PNR Agreement stated that implementation of the accord, as well as the assurances, would be reviewed regularly by the Commissioner for Justice, Freedom and Security or a person designated by him. However, as Data Protection authorities criticized, the mandatory nature of such review no longer appears on the
final Agreement. Only the European Commissioner of the Justice and Home Affairs will be in charge of this inspection, without any control given to the national Data Protection Authorities (CNIL, 2007).

The privacy advocates critiques mentioned above are only examples of disagreements. In general, the new Agreement still failed to satisfy the Data Protection Authorities and the civil liberty groups. In August 2007, the CNIL expressed its concerns, criticizing the PNR Agreement because the number of US agencies having access to the PNR had been expanded, the ways in which PNR data would be used could be changed by unilateral modification of the U.S. legislation, the potential transfer of PNR data to third countries would unilaterally be decided by the U.S. without consulting in advance the E.U. and the U.S. authorities would unilaterally decide whether to accept the request by European citizens to rectify their data\textsuperscript{14}.

The following table represents the changes implemented between the first Agreement in 2004 and the final Agreement in 2007, with the highest level of data protection components highlighted in yellow. The concessions from the United States

\begin{table}
\centering
\begin{tabular}{|c|c|c|}
\hline
Component & 2004 Agreement & 2007 Agreement \\
\hline
Data Protection & Low & High \\
\hline
Access & Restricted & Unrestricted \\
\hline
Usage & Limited & Unlimited \\
\hline
Transfer & Controlled & Uncontrolled \\
\hline
\end{tabular}
\end{table}

concern the “pull” and “push” systems and the reduction in the number of PNR data fields required, both aspects strongly criticized by the privacy advocates as irrelevant.

Table 4: Comparing the 2004 and 2007 PNR Agreements

<table>
<thead>
<tr>
<th></th>
<th>2004 Agreement</th>
<th>2007 Agreement</th>
</tr>
</thead>
</table>
| **Access**           | CBP has electronic access to carriers’ control system, until push system implemented | Transfer from pull to push starting no later than January 1, 2008  
Need to comply with U.S. requirements or pull system would remain in place. U.S. control on data to push and transfer to third party |
| **Review**           | Joint Review once a year, including Data Protection Authorities                | Periodical review with representative of the E.U. Commission and DHS (not mandatory) without Privacy authorities |
| **Data retention**   | 3.5 years active and 8 years dormant. Does not include PNR data linked to specific enforcement record | 7 years active and 8 years dormant. Whether and when erase data to be addressed in further talks |
| **Scope**            | Prevent and combat terrorism and other serious crime                           | Prevent and combat terrorism and other serious crime                           |
| **Transfer to third party** | Transfers to federal law enforcement and security agencies (except TSA for CAPPs testing), considered as exchange with third countries | Transfer with federal law enforcement and security agencies on a bulk basis |
| **Sensitive data**   | Not used in any case. Filter to be implemented as soon as possible            | Not used. Filters implemented. Data will be used in “exceptional case” |
| **Fields required**  | 39                                                                              | 19                                                                              |
The presentation of the PNR debate has underlined the major sources of conflict between the United States and the European Union. This study also emphasized the influence and power of persuasion of the United States to obtain the desired outcomes. Indeed, even the two main concessions granted by the United States, the switch of PNR access system from “pull” to “push” and the reduction in the number of PNR data fields, are considered by many critics to be irrelevant. The American influence thus appears to be a dominating force, pushing the European Union to adopt a decision that weakened European regulations protecting civil liberties.

However, looking at coercion as the only factor of policy diffusion would not offer a comprehensive explanation of why the E.U. signed the PNR Agreement. Indeed, though the next case study also shows the same inclination for security over privacy, the debate surrounding data retention was completely European and did not involve any influence from the United States. Other factors thus seem to be at play, pushing Europe towards new security priorities.
The Data Retention Directive

The police investigations after the London and Madrid bombings highlighted the use of “traffic data” in the fight against terrorism. These data, generated by electronic communication, such as the number called, the time and duration of the call or the location of the caller, have helped law enforcement agencies carry out their work more efficiently. Indeed, the Madrid terrorists were rapidly tracked down thanks to phone and Internet records (Meller, 2005). Moreover, the investigations of both London and Madrid bombings have demonstrated that terrorists use the Internet as a tool to plan their criminal activities (Louvet, 2005), so having this information available could prevent other attack.

Before the events of September 11, there was no unified data retention legislation at the European level. Several Member States had already set up procedures requiring the telecommunication providers to store data, while others did not or forbade the retention of such information. For instance, in the Netherlands and Germany, the providers were supposed to erase data after 3 months. In Ireland, the data retention was expanded to 3 years and in Italy, 4 years (Bouilhet, 2006). The British
did not have a law in force but agreed with the industry on a data retention period of 12 months (Smolar, 2005).

Data retention thus became a sensitive issue as the European institutions tried to harmonize the various national laws and improve judiciary cooperation (Ciprut, 2004).

**Timeline**

The debate over data retention began in July 2000, when the European Council introduced a proposal for a new Directive on electronic communications that would adjust the laws to innovative digital technologies and better define how consumers’ data would be protected. The proposal, including data retention provisions, was strongly opposed by the European Parliament and the privacy advocates, who criticized the negative impact such a clause would have on privacy. They based their argument on Article 6 of the 1997 Directive in force at the time, which stated that telecommunication providers were required to erase data by “the end of the period during which the bill may lawfully be challenged or payment may be pursued,” to protect consumers’ privacy. These billing purposes were equivalent to only a couple of months (Meller, 2005).
Following the September 11 attacks, the European Council increased its support for data retention and the Parliament gave in to their pressure. The European Council’s proposal was made into a Directive on July 12, 2002, and replaced the 1997 Directive on privacy and electronic communication. This new law included in Article 15 the rights of Member States to adopt their own data retention legislation, “to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.”

But the debate did not stop then and in August 2002, the Belgian government addressed the issue of mandatory data retention. Although the initiative was widely condemned, the Member States still continued to address the issue of data retention in the European and national policy debates.

The need for harmonized mandatory data retention was reinforced following the 2004 Madrid attacks. Indeed, in the Declaration on Combating Terrorism presented on March 25, 2004, the European Council required that “proposals for establishing rules on the retention of communications traffic data by service” should be adopted by June 2005. The Justice and Home Affair (JHA) Council immediately started working on this project and in April 2004, France, Ireland, Sweden and the U.K. proposed a
Framework Decision on Data Retention, based on the third pillar. The four Member States argued that data retention legislation was already in effect in many Member States, and other European countries were working towards the implementation of such regulations. However, they insisted that because the content of the laws varied considerably, it undermined cooperation on law enforcement, prevention, investigation, detection and prosecution of crimes (Draft Framework Decision on data retention, 2004). As a result, France, the U.K., Sweden and Ireland emphasized the urgency of the need for harmonization.

Although these four countries had favoured a data retention length of five years at first, the Framework Decision they proposed included a storage period of only 12 to 36 months, durations that could be increased or reduced to no less than 6 months if the national government saw fit. The JHA Council, which adopted the proposal in February 2005, only required a period of 12 months with a possible extension to 36 months, and to 48 months since June 2005, if national governments considered that “such retention constitutes a necessary, appropriate and proportionate measure within a democratic Society” (JHA Council draft Framework Decision, October 2005). Although this proposal left the Member States the ability to adjust the data retention
length, Irish Justice Minister Michael McDowell, still pushed for a longer mandatory time, arguing that all Member States should be allowed to store telephone and internet data for even longer (Rennie, 2005). Regarding the scope, the JHA proposal would require data to be kept for law enforcement regarding all sorts of crime. Moreover, the Decision did not include any clause compelling the Member States to reimburse the high costs faced by the telecommunication providers. Finally the proposal did not address the retention of communications content, but only the details surrounding it, (e.g. name of caller and person called, location, length of conversation, etc.) (Smolar, 2005).

However, the European Parliament still rejected the proposal for its negative impact on civil liberties. It also opposed it on legal basis grounds, arguing that the data retention issue fell into the scope of the first pillar, which should give the MEPs co-decision powers with the Council. The Parliament also condemned the lack of compensation for the high costs the industry would face and argued that such a law went against Article 8 of the European Convention on Human Rights.

The telecommunication providers took the side of the Data Privacy Authorities, pointing out that implementing such procedures would be expensive and would jeopardize their international competitiveness. Indeed, they would be obliged to collect
data but limited in their ability to use them for their own purposes. But the real costs were also hard to evaluate and depending on the survey, the results varied greatly. For instance, the U.K. government estimated the cost to be €1.2 million per year (Smolar, 2005). On the other hand, Bitkom, an association representing 1,300 German telecommunications companies, and the BDI Federation of German Industries, argued that it would bring an additional global cost of at least €150 million (O’Brien, 2005). Responding to the German industry complaints, the British Prime Minister stated that the telecommunication industry was very profitable in Europe and could afford spending several million to ensure the citizens’ security (Bouilhet, 2006).

The second argument advanced by the industries and privacy advocates regarded the legitimacy of such legislation. The telecommunication providers argued that data retention could not prevent terrorism but could only facilitate the investigations following an attack. They also emphasized that these measures may be inefficient, as terrorists could manage to secure their communications, using, for instance non-European service providers (Meller, 2005).

On February 5, 2005, Alexander Alvaro, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) rapporteur, issued a report on the proposal, questioning the effectiveness, high costs and necessity of mandatory data retention and
describing the proposal as disproportionate. He pressed for a limitation of 6 to 12 months, the reduction of scope to only the definition of “serious crime” developed in the European Arrest Warrant and the full reimbursement of telecommunication providers by Member States. Although his report was fully endorsed by the European Parliament and the civil liberties advocates, it did not alter the positioning of the Council.

The debate reached a higher level after the London attacks in July 2005 and the U.K. Presidency, strongly supported by several other Member States, made the data retention directive a priority to be adopted by December 2005. The European Parliament still opposed the Council’s draft Framework Decision, emphasizing again that the legal basis should be the first pillar.

The British increased their pressure, as Foreign Office Secretary Jack Straw argued that with proper safeguards no one’s privacy would be threatened and the security of all would be enhanced. He reiterated the British positioning regarding costs, insisting that “saving life did not have a price.” Charles Clarke finally repeated that data retention was essential to prevent more attacks (Bouilhet, 2005).

In September 2005, the European Commission made clear to the JHA Council that there was no legal basis for a Data Retention Framework Decision in the third pillar, and on September 21, it presented its own proposal based on the first pillar. The Commission’s Draft Framework Decision was closely similar to the JHA Council’s proposal as telecommunication providers would have to store telephone data identifying the time, location, identity of callers, and Internet data including individual computer users, location, device and websites visited, without keeping the communication or webpage content (O’ Brien, 2005). However, unlike the JHA Council’s proposal, it required Internet data to be held only for 6 months and phone data for 12 months and it addressed the issue of compensation for the telecommunication providers.

In October 2005, the U.K. Presidency once more intensified the pressure to pass the legislation, as it declared that if after two months the Parliament and the Commission could not reach a compromise, the latest version of the JHA Council proposal would be adopted as final. This pressure was emphasized by the Danish Justice Minister, as she said: “Are we most afraid of the European Parliament or of
terrorism? We must reach a decision in December. If the European Parliament cannot help, then MEPs are not adult enough to take part in the discussion. 16

The Article 29 Working Party sided with the European Parliament as it criticized the proposals from both the Council and Commission. However, as it appeared clear that a Directive would eventually be adopted, the European Data Protection Commissioners tried to press for the least damaging policy and reinforced their calls for better safeguards. Although Alvaro kept pushing for the Council to take his recommendations into account, he did not manage to even influence the debate in his home country, as the main German political parties had already informally agreed to support the Council’s draft (Meller, 2005).

Following Parliament’s threat to take actions with the European Court of Justice to contest the legal basis of the proposal (as it had previously done with PNR), the U.K. Presidency suggested a compromise with the MEPs and finally accepted the Parliament’s co-decision powers. In return for this action, he asked the Parliament to approve the flexibility of the proposal, which grants the Member States the power to adjust the data retention length at the national level (Ferenczi, 2005). As a result, in early December, the Council started negotiating with the European Parliament to reach an agreement. The U.K. Presidency still intensified its pressure and lobbying efforts,

16 Jenny Booth. Clarke threatens MEPs over EU terror laws. The Times, October 12, 2005
arguing that the costs involved were modest, since the telecommunication providers were already collecting this information and would just have to keep it longer (Liberty and Security: Striking the Right Balance, 2005).

Finally, the European Parliament approved the proposed directive on December 14, based on the first pillar. On March 15, 2006, the European Union followed and the Directive 2006/24/EC, on “the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,” was officially adopted.

The telecommunication providers are from now on required to identify the source, destination, data, time, duration and type of a communication, the communication device and the location of mobile communication equipment, but not the content of the communication (Pinson, 2005). The final data retention length was approved at 6 to 24 months, but Article 11 states that Member States could adjust these periods as they see fit. The Directive also left the issue of cost to Member States with no obligation to enforce reimbursement. Finally, the scope of the Directive is no longer limited to the fight against terrorism and organized crime but included all “serious crime”, without defining “serious” or any limits to data access.
The debate is still ongoing and continues at the national level, particularly regarding the reimbursement of costs and the adoption of data retention length. Interestingly, France, Spain and the U.K, which originally pushed for data retention, only required the telecommunication provider to retain data for one year, as set by the Directive.

Although the Data Retention Directive seems to affect negatively protection of civil liberties, the Data Protection Authorities still managed to obtain an important concession from the JHA Council and the Commission. Indeed, their pressure for a reduction of the length of time during which data would be retained led to a shorter time period than the Justice Ministers originally asked for.

Conclusion

Both the PNR and Data Retention agreements show a clear change in the European position as they altered the balance between security and privacy to lean more towards national safety. This chapter has presented the different dynamics influencing the outcome of the debates, from the political and economic pressure of the United States to European internal conflicts of interests. The next section will analyze
the underlining forces and assess the reasons why the European Union is becoming more security-oriented. This in-depth analysis will allow me to closely evaluate the implications of the most relevant policy diffusion theories discussed in Chapter Two (coercion, domestic preferences, economic interdependence, security dependence and bureaucratic structure) and present the views of the main players influencing the policymaking process.
Chapter Five: PNR and data retention—empirical findings

This chapter will analyze the dynamics of the PNR and data retention case studies, focusing on the five theories discussed in the Chapter Two: coercion, domestic preferences, economic interdependence, security dependence and bureaucratic structure. Each of these hypotheses offers a complementary explanation of why the European Union has become more security-oriented and has aligned its policies with the American model.

In order to explain the implication of these theories in influencing the European position, I have drawn two diagrams, the first depicting the European and American level of privacy protection before September 11 and the second, describing the situation after the attacks.

The red arrows pointing towards less privacy (↑) represent a “pull” movement from the factors on the left. On the contrary, the pink arrows pointing towards stronger privacy safeguards (↓) indicate a “pull” movement towards greater privacy from the factors on the right. Finally, the thickness of the arrows represents the degree of influence of each theory.
The first diagram shows that before September 11, the European Union tended to tilt the balance towards greater privacy. In general, national governments pressed hard for civil liberties, in association with Data Protection Authorities. Given that these privacy advocates were not challenged at this time by urgent needs of increased security, the weakness of their bureaucracy structure did not matter much. Likewise, economic interdependence and security dependence had only a relatively low impact, as security did not represent a priority issue before September 11. For this reason, both have limited influence and do not pull in any particular direction. Finally, the United States tries to pull the European Union in becoming more security-oriented, as a way to reflect its own preferences.

Figure 1: Balancing privacy and security before September 11
The second diagram illustrates a clear shift in the European priorities. Indeed, the position of the E.U. on the spectrum has moved closer to the United States’ and towards weaker privacy protection. This can be explained by the fact that factors previously pulling for more privacy protection or not pressing for any change have now switched sides. Indeed, the domestic preferences of Member States have shifted towards more security-oriented measures, which tend to be associated with a weakening in privacy protection. Likewise, security dependence arose after the September 11 attacks as both the U.S. and the E.U. needed to collaborate to ensure citizens’ protection. As a result, this dependence tends to push the European Union towards an increase in security measures, often at the expense of privacy. The economic interdependence followed the same logic, as counter-terrorism measures and cooperation with the United States involved financial implications, pushing the European industries to follow the American preferences and to loosen privacy protections. Finally, the U.S. intensified its pressure to influence the European Union in adopting a position closer to American preferences.

The only forces pulling back the European Union towards stronger privacy protection are the Data Protection Authorities. However, now that security measures are at play, the bureaucratic structure of the European Union does not act in the privacy advocates’ favor, limiting their influence. Even if the Data Protection Authorities
vehemently criticized the shift in European position, they only managed to obtain concessions to a certain point. As a result, while other factors strongly pulled the E.U. towards more security and in general weaker privacy safeguards, the privacy representatives were not able to counter this trend.

Figure 2: Balancing privacy and security after September 11

The following sections will present an in-depth analysis of each theory and how these hypotheses impact on the PNR and data retention case studies presented in the previous chapter.
Because coercion is a factor of policy diffusion that is easy to determine and is often used as the only justification for the European shift, I will only develop it briefly and delve more deeply into the other explanations. I will then argue that coercion alone cannot explain every aspect of the European policy change and that European interests represent a crucial factor, with many of the individual Member States favoring security at the domestic and supranational levels.

Coercion

The argument that Europe was forced to adjust to the preferences of the United States and could not resist the pressure is commonly put forward. Regarding PNR, the United States clearly threatened European air carriers of cutting their landing rights and imposing a $6000 fine per passenger in cases of noncompliance. Although it has proven hard to find official statements expressing such sanctions, dozens of articles from American and European newspapers have reported the American coercive actions. Le Monde, The Washington Post, The Times, Le Figaro, Deutsche Welle, and The Financial Times are some of the publications describing those threats. Members

---

German Ministers at Odds Over EU Passenger Data Plan, Deutsche Welle. January 29, 2008
of the European Parliament and Commission have also reported the threat of economic sanctions. Moreover, according to *The Financial Times*, Secretary Chertoff pushed coercion further, saying that “even without a deal, the US government would have to satisfy its legal obligation to gather the information” (Sevastopulo, 2007).

But traces of coercion can also be found at the diplomatic level. As such, many of the newspapers mentioned above as well as European officials (Heisenberg, 2005) condemned the unilateralist actions of the United States and authored articles with titles such as: “Once more the EU caved in to U.S. pressure at the expense of EU citizen’s civil liberties,” “America dictates its anti-terrorist law,” and “the EU gave in to the U.S. demands.” Numerous scholars have also mentioned this fact, such as Alexandre Adam (2005) and Wyn Rees (2006). Finally, Jacqueline Klosek (2007) mentioned several American officials’ statements “suggesting” the European Union reconsider its privacy standards to fight terrorism more efficiently.


In its 21st Report of Session 2006-2007, the British House of the Lords denounced this power of manipulation of the United States, particularly during the negotiation of the PNR agreements. The House strongly criticized the changes adopted in 2004 and 2005 in the American national laws that impacted on the Undertakings of May 2004. For instance, provisions in the Intelligence Reform and Terrorism Prevention Act of 2004 required the President to create a new Information Sharing Environment. The Executive Order 13388 issued on October 25, 2005 required that the DHS and other agencies “promptly give access to terrorism information to the head of each other agency that has counterterrorism functions.” This new legislation went against Undertakings 28-32, which forbade the routine sharing of PNR between other federal agencies, considered as third parties. But again, Undertaking 35, stating that “No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law,” allowed the U.S. to act unilaterally.

Another controversial aspect of the PNR debate underlined by the House of Lords is that the 3.5 year period for data retention negotiated in the Interim Agreement had no real effect. Indeed, the Undertakings would apply for 3.5 years but “if no mutually acceptable arrangement can be concluded prior to the expiration date of these

---

Undertakings, the Undertakings will cease to be in effect.” Thus, if the agreement expired before the end of the agreed data retention period, the American authorities were no longer forced to respect it (House of the Lords, 2007).

In the case of data retention, pressure for greater collection of data came from within the European Union. Indeed, the Justice Ministers and the U.K. Presidency coerced the European Parliament into adopting the Directive. They even threatened the MEPs with adopting the JHA Council’s proposal as final, in case the Parliament could not reach an agreement within two months. However, the extent of the threat was not as definitive as the ones used by the United States for PNR, as the U.K Presidency and JHA Ministers did not imply any concrete sanctions, but their force of persuasion was sufficient to compel the Parliament to accept the Commission’s proposal.

Because in the case of PNR the outcome of the threats was so real and serious, it had more obvious repercussions. As a result, the European Commission often used American coercion as a means to explain its decision to regard the PNR Agreement as adequate. The Commissioners argued that they had no choice, the threats were too great to ignore and that finally, the air carriers were already transferring PNR since March 2003 without any safeguards, so any U.S.-E.U. agreement was better than nothing (Kerr, 2003). The Daily Telegraph reported in July 2003 the words of Chris Patten, European Commissioner for external relations, explaining to the European
Parliament that “The stakes . . . were very high. We had to ensure, so far as we could, that the important interests of EU citizens in preserving their right to privacy were balanced against the need to protect thousands of jobs in our airlines and associated industries.”

However, the European Union has enough economic and geopolitical power and should be powerful enough to resist such pressure. Indeed, it should be able to influence the United States and find a compromise that is better aligned with European privacy laws. Given the large number of protests from Data Protection Authorities, the Members States could have argued that they had no choice but to listen to these concerns. By saying that their hands were tied, they could have obtained more concessions from the United States. It is even conceivable that national data protection authorities could have threatened to impose large fines on airlines that transferred data to the United States. The only relevant explanation for their timid resistance seems to be that the Member States actually favored an improvement of security measures and used coercion as a justification to limit privacy advocates’ protests.

Another clear example that American coercion alone is not sufficient to explain the shift in European policy is data retention. Indeed, the debate surrounding this issue

---

20 Kerr, M. (2003, July 19). You won't have noticed, but Uncle Sam is watching you. The Daily Telegraph (London)
was European and the United States was not directly involved in it. Furthermore, the U.S. does not even have mandatory data retention legislation, so it would not make sense to say that the Americans are pushing their own policies abroad. As such, arguing that the E.U. is becoming more security-oriented only because the U.S. is forcing the Member States to do so appears incorrect. Instead, the push for more security seems to arise from the Member States themselves, as a response to a shift in European interests. The American pressure is not a negligible factor but as it does not apply in every case, one should look at other influences to get a comprehensive understanding of the European policy change.

The rest of this chapter will take a closer look at these European interests, focusing on the Member States’ domestic preferences, the bureaucratic structure, the economic interdependence and the security dependency between E.U. and U.S.

**Domestic preferences**

In order to analyze the domestic preferences of the Member States, I have decided to focus on three countries: Germany, France and the United Kingdom. The rationale for picking these cases lies into the fact that these three states expose features relevant to this study: they have a long history of repeated terrorist attacks, they
struggle with immigration concerns and they have faced the dilemma of balancing privacy and security. Moreover, these countries represent the “old Europe,” and enjoy a strong influence within the European Union.

*Germany*

Since the 1970’s, Germany has been confronted with different forms of terrorism acts, carried out by extreme leftist groups, such as the Red Army Faction (RAF), the Kurdistan Worker’s Party (PKK) or, more currently, attacks involving hate crimes (Gallis, 2003). As a result, Germany already had passed counter-terrorism legislation before the September 11 attacks and had signed several international Acts regarding security (Szyszkowitz, 2005). However, the memories of the Nazis’ information gathering to track down Jews and surveillance by the Stasi in East Germany have strongly affected the population, which cherishes civil liberties and seems reluctant to trust the government with personal information.

Nonetheless, the attacks on the World Trade Center changed this perception. Although Germans did not consider themselves as primary targets of terrorism acts, pressure to tighten the existing security laws grew. Moreover, several key perpetrators of the September 11 attacks lived in Hamburg, benefiting from limited police
surveillance and the high respect for the rights of privacy and religious expression. This fact constituted another impulse for the government to introduce tougher security measures. Otto Schilly, the Interior Minister at this time, immediately introduced two packages of laws, the first making it harder for terrorists to live in Germany and raise money, the second expanding the powers of the law enforcement and intelligence agencies (Gallis, 2003). Among these provisions, the government dedicated hundreds of millions of dollars to enhance intelligence gathering, tighten airport security, facilitate information sharing among various agencies, broaden the types of information allowed to be collected, increase the access to personal data (phone records, e-mails, bank records etc.) and introduce fingerprints and other biometric components on identification cards and passports. In terms of international cooperation, Germany increased its contact with the United States, carrying out joint investigations.

By December 2002, both packages were accepted, even if some of the laws were strongly criticized. Opponents of Schily’s measures argued that the government had wanted to introduce this legislation before 9/11 but was opposed by the strong public preference for civil liberties. To these critics, Schily’s responded with his mantra since 9/11: “no freedom without security” (Martin, 2002). The Interior Minister repeatedly emphasized the fact that Germany could be targeted at any time and that the
government had to adjust security concerns to the modern threats (Farnam, 2001). This fear of terrorist attack by Islamic terrorists, particularly increased by the German military engagement in Afghanistan as well as the rising tension within Germany’s large Muslim population (40% of total immigrants, between 3 and 3.5 million), facilitated the acceptance of the laws even if they reduced privacy protections.

Schily’s involvement in the data retention debate also points out his strong support for more-invasive security measures. Although the German Parliament had actually forbidden the Minister of Interior from agreeing with the Council’s and Commission’s proposals, Schily still expressed his support for mandatory data retention (EDRI-gram Number 3.6, 2005). The European Digital Rights (EDRI), an international non-profit organization monitoring civil rights in Europe, even said: “Germany's minister of Interior Affairs, Otto Schily, is known to be the driving force behind a new law to introduce mandatory data retention in Germany and to also put pressure on other EU states' governments to introduce similar measures”(EDRI-gram Number 2.13, 2004). The Interior Minister’s position was strongly criticized by the German Data Protection Authorities, which had been relatively quiet following the decision of the German Parliament. The German MEPs opposed the legislation and their preference for privacy remained a strong obstacle for the European Council to have the Directive adopted. The new government coalition arising following the
November 2005 federal elections lifted the JHA Council’s concerns, as the German government now showed strong support for data retention.

After the elections, Interior Minister Schily was replaced by Wolfgang Schäuble, who followed similar security policies. Indeed, since his appointment, Schäuble has called for tighter security policies (Landler, 2007). In 2007, he presented a set of measures, arguing that their implementation would enable the government to better equip security services to fight terrorists. Among the measures were the adoption of a law enabling the shooting down of a plane commandeered by hijackers, the authorization for the government to carry out online searches of computers and the extension of suspects’ detention time. Most of the provisions proposed were accepted and for instance, as of 2008, the government is allowed to monitor computers of people suspected of crimes or terrorism (The New York Times, 2008). Moreover, Schäuble strongly influenced the outcome of the data retention debate, as he showed his full support for the Decision, even emphasizing that access to information collected from telecommunications companies should be made available broadly within the security services, given that the purpose of this legislation was to prevent terrorism (EDRI-gram Number 3.24, 2005).

However, this preference for security over privacy is not shared by every member of the German government. For instance, the Justice Minister, Brigitte Zypries,
strongly criticized Schily’s and Schaüble’s domestic security measures. Regarding PNR, Zypries again opposed the views of Schaüble, as Der Spiegel condemn the fact that the first 2004 PNR agreement did not take into consideration the Justice Minister’s concerns (Agence France Press, 2004). Zypries also warned against the damage to civil liberties such an agreement would cause and how it was not consistent with the German Constitution (Deutsche Welle, 2008). Her concerns were reinforced by the position of Peter Hustinx, the European Data Protection Supervisor, expressed in a letter to the German Interior Minister dated June 2007 (Hustinx, 2007). Interestingly, Zypries strongly pushed for data retention, which seems to contradict her position towards PNR.

Although civil liberties groups and privacy advocates vehemently criticized the security measures adopted since 9/11, the German preferences clearly seem to have shifted towards a more security-oriented approach that was more aligned with the American policies. Because parts of the September 11 attacks were orchestrated in Germany, the government realized that the security policies in place were no longer sufficient to prevent the organization of more terrorism acts. This weakness also threatened the security of German citizens, who could become the next target of Al Qaeda. Schily and Schaüble have repeatedly underlined this new threat for Germany,
pressing the population to become aware that security has to be reinforced even if it has to be at the expense of some privacy. The London and Madrid bombings bolstered the Interior Ministers’ arguments and the population was faced with the reality that they were as likely to face terrorist attacks, as much as the U.K. or Spain. It is still important to point out that although Germans agreed on trading off some of their civil liberties, they still strongly opposed data retention legislation and managed to have the Supreme Court partially suspend the agreement in March 2008. Indeed, even if the Directive was approved within the European Union, the German Data Protection Authorities fought harder at the domestic level and obtained a limitation in the use of telecommunication data21. However, the general approach to security and privacy remains focused on increasing safety by implementing stricter measures and preventing other terrorist acts. As the German representatives push towards their interests at the supranational level, these internal dynamics offer a valuable approach to understanding the influence of Germany in European policy shifting.

21 The Supreme Court stated that information would only be transferred to law enforcement agencies in case of serious crime and with judicial warrant. Moreover, the data will only be made available when other evidences have proven inaccessible or insufficient. EDRI-gram - Number 6.6, 26 March 2008. German Constitutional Court limits data retention law. Retrieved in April 18, 2008 from http://www.edri.org/edrigram/number6.6/germany-data-retention-decision-cc.
Like Germany, Britain has faced terrorism for several decades, especially attacks orchestrated by the Irish Republican Army (IRA), whose members aimed at ending the British rule in Northern Ireland. In 1974, the U.K. adopted its first counterterrorism law, the Prevention of Terrorism Act. Although the law was reviewed over the years, it was mostly adapted to counter Irish terrorist groups. Soon after his election in 1997, Prime Minister Tony Blair started working to enhance U.K. terrorism laws and in 2000, the new Terrorism Act was passed (Caldwell, 2006). This legislation broadened the scope of the law, applying it to any form of domestic or international terrorism (Gallis, 2003). These terrorism concerns also reflect the immigration problems of a country that hosts a largely unassimilated Muslim population of an estimated 1.6 million. Before the September 11 attacks, British asylum and immigration laws were also particularly flexible, which attracted extremists groups and made the country more vulnerable to attacks.

---

As a response to 9/11, Tony Blair announced that “The rules of the game are changing” (Caldwell, 2006). The government introduced the 2001 Anti-terrorism, Crime and Security Act, which enhanced the current legislation and expanded the powers of law enforcement and surveillance agencies. In particular, the new Act improved information sharing between the various law enforcement authorities, tightened transport security, strengthened the laws on terrorism financing, expanded the time of detention of suspected terrorists and reinforced the asylum and immigration laws. Interestingly, some of the provisions (information sharing, detention of suspects and access to records) are strongly reminiscent of the American PATRIOT Act (Pike, 2006).

One of the biggest controversies surrounding Blair’s proposition regarded the derogation of the European Convention on Human Rights Article 5, which renders illegal the indefinite detention of a suspect without trial. The government introduced the idea that this article would be suspended in case of “public emergency” (Lennon, 2002). According to Time Europe (2001), this clause was particularly criticized by civil liberties groups, but on the other side, it was strongly defended by Home Secretary David Blunkett.

This measure was not the only one drawing strong protests and the privacy advocates managed to obtain several concessions from the government, regarding for
instance the length of telecommunication data retention and the law proposal aimed at making religious hatred a criminal offense (Gallis, 2003). Some provisions were even repealed because they were in conflict with E.U. legislation (Pike, 2006). To these European refusals, Blair argued that the European human rights laws prevented Britain from dealing with supporters of terrorism (The Economist, July 23, 2005). The civil liberties groups often claimed that the government used the fight against terrorism as a justification to implement strong security measures (The New York Times, 2006). Moreover, Clive Crook (2005) argued that “unlike in America, these liberties are not protected by a written constitution. A government like Blair's with a secure parliamentary majority can trample them with impunity, so long as it has at least the tacit support of the public. And Blair does” (National Journal, 2005).

However, the London bombings of July 7, 2005, completely changed the situation, emphasizing that the current counter-terrorism legislation was still insufficient (Caldwell, 2006). During the following monthly news conference, Blair declared that both Conservatives and Democrats had cast their differences aside and announced a “cross-party consensus” on a terrorism fighting strategy. The two parties had previously often disagreed on how to handle terrorism and how far the measures should go (Lyall, 2005). Blair presented a 12-point plan, which, for instance, involved strengthening enforcement of asylum and deportation and banning hard-line Islamist
groups. The Prevention of Terrorism Act was passed in 2005 and a new Terrorism Act in 2006, both extending again the powers of law enforcement and intelligence agencies to search and detain suspects (Klosek, 2007). Moreover, the London bombings also silenced the critics accusing Blair of using the fear of terrorism as a justification to introduce laws curtailing liberties as such comment could no longer appear credible (Crook, 2005).

Although the privacy advocates repeatedly criticized the new provisions presented by Blair, most citizens seemed to believe that such action was justified. A poll published by The Times reinforced this trend. The survey, carried out by Populus in July 2005, demonstrated that 86% of the population agreed to give the police new powers to arrest suspected terrorists, 88% approved the introduction of tighter controls at the borders, 70% favored the increasing of police powers to stop and search people on the streets and 61% approved the introduction of national identity cards. Although one could argue that the figures were biased by the shock of the bombings that occurred a couple of days before, a second poll carried out by Populus in September 2006 showed that support for these measures was still strong. Indeed, only 29% of the interviewees believed that the airport authorities overreacted to the threat of terrorism and introduced excessive security measures.
But a year after the attacks, 73% of the population also thought that the British involvement in the Middle East conflict significantly increased the terrorism threat (The Times, 2006). Blair had already admitted this fact two weeks after the attacks, saying in a press conference that the support for the Iraq war and the British involvement in Afghanistan increased the risks of attacks on Britain (Economist, 2005).

In June 2005, the United Kingdom became President of the European Council and tried to use this opportunity to implement more security-oriented measures, such as the introduction of biometric identity cards and the use of PNR and CCTV cameras (Liberty and Security: Striking the Right Balance, September 2005).

The British also increased their lobbying efforts to push for the adoption of mandatory data retention legislation by the end of the year (Meller, 2005). They had already pushed hard for the April 2004 Framework Decision, along with France, despite resistance from other Member States and the European Parliament. As early as 2000, the British government had already proposed that all telecommunication providers retain data for 7 years (Hosein, 2005). The Presidency gave the U.K. additional influence to have the British preferences pushed forward or even adopted.
Interestingly, the United Kingdom used an argument in favor of data retention that had been mentioned before, namely that the European Convention of Human Rights (ECHR) was outdated. Charles Clarke, the U.K. Home Office Secretary, said on September 7 that the balance between individuals’ rights and security “is not right for the circumstances which we now face – circumstances very different from those faced by the founding fathers of the European Convention on Human Rights - and that it needs to be closely examined in that context." (Liberty and Security: Striking the Right Balance, 2005). Similar attacks on the ECHR had created outrage in the past, but particularly because of its position as Presidency of the Council, the U.K. was able to effectively push its position.

Moreover, the British attitude towards data retention reflects even more domestic preferences and helps explain why the UK, along with France and Sweden, tried to bypass the European Parliament and Commission. Indeed, by introducing the draft proposal on the third pillar basis, they left the European institutions out of the decision-making process. By doing so, the U.K. pushed its own interest (in this case, blocking the European Parliament’s opposition) at the European level.

Finally, Gus Hosein (2005), a Privacy International representative, argued that the U.K. and Ireland have doubled their efforts for mandatory data retention in the
European policy arena, as the national proposals met strong resistance and could not be passed.

The appointment in June 2007 of Prime Minister Gordon Brown did not change the positioning of the British head of government, as he follows the same security goals previously advanced by Tony Blair. Mr. Brown immediately presented two proposals. The first was to grant the government powers to detain suspected terrorists without charges for more than 28 days, already the longest detention time in Europe. This proposal had previously been introduced by Tony Blair's government, which had pressed for a 90 day detention period, but was blocked by the Parliament (Shenon and Lewis, 2006). The second provision regarded the introduction of national identity cards including biometrics for the whole population (Economist, 2007). Again, some measures were condemned by civil liberty groups, as infringing on privacy. One of the controversies surrounded the provision that made it a crime to “glorify” terrorism (Pike, 2006).

All the issues discussed above emphasize the fact that the United Kingdom has been adopting more and more security measures that compromise privacy protections. In 2006, human rights advocacy group Privacy International even ranked Britain as an
“endemic surveillance society\textsuperscript{23},” along with Russia and China and giving the United Kingdom a worse ranking than the United States (\textit{New York Times}, 2006). The differences between the U.S. and the U.K. had already been underlined in the past as, for instance, British law enforcement agencies have greater authority than the Americans to carry out domestic surveillance and hold suspects without charges (Shenon and Lewis, 2006). The London bombing also strongly reinforced the political alignment towards a more security-oriented approach (Caldwell, 2006).

“Learning to live with Big Brother”, an article from \textit{The Economist} (September, 22 2007), described at length the situation in the United Kingdom and the loss of civil liberties there. The author demonstrated that the time when Britain used to pride itself on respecting civil liberties more than any other nation is long gone, as he described the privacy implications of talking surveillance cameras, miniature drone aircrafts scanning the crowds for suspicious behavior, the national biometric identity card, DNA database gathering samples of more than 4 million citizens and the 5 million CCTV cameras operating in public spaces.

Finally, Britain’s willingness to align its security policy with the United States’ model does not represent a new trend. Blair frequently cited the “special relationship”

between the United States and the United Kingdom. Cooperation was intense at numerous levels, and the British have repeatedly expressed their support for American foreign policy. In January 2003, the collaboration between American and British law enforcement and intelligence agencies increased further, as U.S. Homeland Security Secretary Ridge and British Home Secretary Blunkett announced the implementation of a joint working group to share counter terrorism expertise and “best practices” (Research and Documentation Centre of the Dutch Ministry of Justice, 2006). Although communication was already strong between both countries’ security agencies, this new level of partnership aimed at fostering electronic information sharing (Congress daily, 2003).

This strong cooperation with the United States and the domestic preference for security over privacy constitute a significant influence in the European policy-making process. Because of Britain’s “special relationship” with the United States and its support in Afghanistan and Iraq, the U.K. government became more aware of the growing terrorism threat for Britain. This need to ensure the safety of the population became urgent, and since September 11, the British authorities introduced stricter security measures. Pressure for additional security measures reached a peak when London was attacked in July 2005, convincing even unconditional supporters of civil liberties that the safety protections in place needed to be enhanced. As a result, Britain,
along with Germany, pressed to have tighter security measures adopted at the European level.

**France**

Like their British and German neighbors, the French are concerned about Muslim immigration (representing 5%-10% of the population), have past experience with terrorism and are trying to strike a fair balance between security and privacy. Since the 1970’s, France has faced attacks from members of Basque terrorist movement ETA, Algerian Islamist extremists (GIA Algerian Armed Islamic Group) and Corsican separatists (FLNC). Between 1986 and 1996, there were 23 bomb attacks attributed to Islamic movements (Research and Documentation Centre of the Dutch Ministry of Justice, 2006).

In order to respond to these threats, the French government based its counter-terrorism strategy on two pillars. The first focuses on operational prevention, a task carried out by the Central Liaison Committee Against Terrorism (CILAT) and the Anti-Terrorist Coordination Unit (UCLAT), and the second is repression. The second pillar consists of legislation and judicial measures, set up in accordance with the Act of September 9th of 1986. This Act represents a cornerstone of the French anti-terrorism
efforts, defining terrorism and harsher legal procedures and sanctions (O’Brien, 2005). These measures enabled the government to create a strong network of intelligence agencies, progressing quickly and efficiently (Gallis, 2003).

In reaction to 9/11, the French government adopted tighter measures regarding air travel security (O’Brien, 2005), increased the budget of law enforcement agencies (Gallis, 2003), facilitated intelligence sharing and expanded the access to data. The government reactivated the Vigipirate Plan, which consists in extensively deploying policemen and security forces in the cities, as well as increasing surveillance (Laushway, 2002).

The French government even went against the 1997 Directive, when in November 2001, it required data retention as an allegedly urgent procedure to fight terrorism. This measure was contested by the French Parliament and criticized by the privacy advocates as violating the E.U. legislation of the time. However, the 2002 e-communication Directive and the 2006 data retention legislation made these objections obsolete. Some of the provisions in the 2006 legislation were adopted partly because of the influence and pressure of France, as it reflected the French domestic interests. Indeed, France was among the several countries that wrote the April 2004 draft and lobbied for its adoption. Following the passage of the Directive in March 2006, France
extended the provisions in two ways. First, the access to data was no longer restricted to judicial authorities but was extended to police forces as well. In France, the data retention law now applied to any kind of Internet access provider, including Internet cafes or hotels (Barbry, 2006). The length of data retention chosen also reflected the French interests in increasing security measures, as it corresponds to the maximum period allowed by the national law, namely one year, for both internet and telephony data (Bouilhet, 2006).

The security measures adopted after 9/11 received general support from the population, which seemed willing to trade off some privacy for more security. Several polls demonstrate this trend: on October 7, 2001, Dimanche Ouest France published a survey by Ifop, showing that 99% of the French population agreed to the strengthening of airport controls and 73% approved the monitoring of emails. A year later, another Ifop poll demonstrated that 76% of the French trusted their government to take the adequate counter-terrorism measures. Finally, a survey carried out by Harris Interactive and published by the Financial Times in October 2006 showed this same support, as 68% of the French population considered that the country should tighten up border control.
It is also important to mention that France has faced recurring problems integrating immigrants, increasing the insecurity on the streets and causing civil unrest in October 2005 and riots in May 2007. Security even became a central priority debated in the 2002 and 2007 presidential elections as tensions with difficult French suburbs intensified. This could also explain why the French public did not oppose the new security measures, as the citizens would gain protection from domestic racial conflicts and at the same time, terrorism.

The London bombing of July 2005 accelerated the introduction of more security-oriented measures as Nicolas Sarkozy, Interior Minister at the time, introduced a proposed law to step up national security. He presented the “zero tolerance” policy, a new approach consisting of three main elements: 1. Increasing surveillance, monitoring Muslim activity and fighting terrorism recruitment; 2. Implementing “offensive harassment” raids to deter terrorist activity and upset the network; 3. Setting up a tougher criminal justice system, including the expansion of the sanctions for terrorism acts (pushed by Justice Minister Pascal Clément) and the detention time of suspected terrorists, currently 96 hours (Bernard, 2005). As far as surveillance was concerned, Sarkozy argued that the CCTV in London enabled the authorities to rapidly identify the terrorists, and as a result he pressed for the increase in the number of cameras in France (Klosek, 2007).
By December 22, 2005, the bill was adopted by the Parliament and the Senate. The CNIL and the human rights groups denounced the new measures as infringing on privacy, without much success. Ariane Bernard (2005) once again complained that the “French seemed happy to forgo some civil liberties in the name of security, even before the latest terrorism threat.”

In terms of international cooperation, France has long participated in joint efforts within the framework of the United Nations, the G8 and NATO, taking part in conferences and signing several multilateral and bilateral agreements (O’Brien, 2005). The attacks of September 11 particularly reinforced the cooperation between France and the United States at the law enforcement (Gallis, 2003) and intelligence sharing levels (Economist, 2005). France also increased collaboration with its European counterparts, exchanging liaison officers with UK, Germany, Italy, Spain and Belgium (O’Brien, 2005).

Looking at the French interests once more shows the domestic preference for security over privacy. The public demands for greater safety may be responding more to a domestic insecurity concern than a fear of terrorism, but the result ended up the same: the French government introduced tighter security measures, pressing its
European counterparts to adjust to these predispositions while negotiating at the supranational level.

The analysis of British, German and French preferences demonstrates that several national governments within the European Union had already strengthened security at home, placing this issue at the core of their interests. For this reason, these three influential countries used their individual and common pressure to convince the more reluctant European partners to adopt similar security measures.

In some cases, the amount of persuasion needed was not very great, as several terrorist attacks seemed to gather European countries together. The two terrorist attacks in London and Madrid made the Member States realize that they were potential targets of terrorists as much as the United States and European countries started to believe that they should step up security, even if it was at the expenses of security (Bernard, 2005). As such, following the bombings in Spain, they vowed to drastically increase their cooperation in the fight against terror. But few of the measures discussed were actually implemented as, for instance, big Member States were reluctant to share sensitive intelligence with the entire Union (Economist, 2005). However, the European countries continued to address the terrorism issue together. In August 2006, following the alleged terrorist plot in London, Interior Ministers from France, Finland, Germany,
Portugal, Slovenia and Britain met to set up new anti-terrorism measures, representing a shift for Europe (The New York Times, 2006). This included the increase in cooperation between the national intelligence agencies and the expansion of data-sharing on airline passengers, potentially incorporating details of travelers’ biometric identifiers (European Parliament News, 2006).

Finally, the data retention case demonstrates that domestic preferences play an important part in Europe’s shift in position, as Member States pushed for measures controversially adopted or discussed at home. Moreover, the Justice Ministers gathered and pushed together for a decision based on the third pillar, limiting the influence of the opposition acting against their own interests.

**Economic interdependence**

The economic aspect of the privacy and security debate also has an important part to play in the shift of the European position.

At first, one could consider that economic interdependence between the United States and the European Union reinforces the coercion argument. Indeed, if the economic threats of the U.S. had no effect on European businesses, they would be useless. The negotiation of the PNR agreements underlined this point as the American
authorities threatened to sanction European airline companies on economic grounds if they did not comply with the U.S. law requirement. Although the European air carriers strongly denounced the costs of implementing such demands and the Association of European Airlines argued that the European air carriers should not be responsible for the security of American citizens (*Le Monde*, 2004), the airline companies needed an agreement to avoid American sanctions. They also tried to use the argument of privacy to obtain concessions. However, even if they would have preferred not to transfer any data at all, they were more concerned with being in compliance with American laws more than with privacy itself. As a result, the companies approved the PNR agreements in order to remain competitive.

More generally, the economic interdependence can be demonstrated by the fact that the United States and the European Union are the two largest economies in the world, generating about 40% of world trade (EuroStat, 2007). Moreover, they also have the biggest bilateral trading and investment relationship. Indeed, Europe’s major partner is America, with the sum of imports and exports to the U.S. amounting to €444.410 million in 2006 (17% of all trades). Europeans export more to America than any other country, dedicating 23% of the total exports and generating €267.895 million in 2006. The European Union is also the most important partner of the United States, and their general trade represents 19.1% of the US trade (EuroStat 2007). Finally, in
2007, the United States invested $175,791 million in Europe, which is more than half of its total investment for the year (Bureau of Economic Analysis, DoC, 2007). On the other side, the European Union invested two-thirds of their annual direct investments in the United States (Brussel Forum, 2007).

These figures emphasize the economic interdependence between the United States and the European Union. This tremendous amount of trade, in addition to the threat of economic sanctions, help explain why the European airline companies easily accepted the American conditions. Once more, the only leverage possessed by the business groups was to increase public awareness of the privacy implications and the high costs, which could be passed on to the passengers (Le Figaro, 2006).

However, the sole explanation of coercion as the justification for the European shift in positioning is not complete. Indeed, because the United States economy is so closely linked to that of Europe, the E.U. could have resisted or compromised for better conditions. However, it chose not to, which reflects the fact that signing the PNR agreement had become part of the European interests. Moreover, the European population did not seem to react to the air carriers’ timid complaints, which may reflect their real interests: an increase in security.
Security dependence

In order to push for more security-oriented policies, the European Union also argues that the only efficient manner to fight terrorism is to cooperate with its allies. Most of the Member States who have already experienced terrorism have faced domestic threats from smaller groups, acting at the national level. However, the latest form of terrorism represented by Al Qaeda is characterized by its transnational nature. The terrorists are not based in one single country and are constantly moving, making national counter terrorism laws inadequate. For this reason, the United States or the European Union alone cannot efficiently fight terrorism. Both are dependent in the sense that they need each other to protect their own population. As a result, there is a greater need for cooperation, and thus harmonization of policies. Although one could argue that the harmonization could be carried out as the United States following the E.U. preferences, the ultimate common goal is the security of individuals, and this requires tighter measures.

This theory can be demonstrated as since September 11, the European Union and the United States have recognized the need for collaboration and increased their joint efforts to fight terrorism. Both actors have met regularly to discuss this issue in the framework of various international summits such as Europol, Interpol, G8 and NATO. For instance, during the G8 Summit on Counter Terrorism on June 8, 2007,
both parties stated: “we pledge to do everything in our power to counter the conditions that terrorists exploit, to keep the world’s most dangerous weapons out of the hands of terrorists, to protect critical transport and energy infrastructures etc.” The previous summit in Sea Island (2004) was also dedicated to the fight against terrorism and the G8 countries adopted the Secure and Facilitated International Travel Initiative (SAFTI). In June 2007, these States announced the “successful completion of all [the SAFTI] 28 projects” and said they were “convinced that this work has made international travel more secure”.

This intensification of cooperation has also been underlined by American officials, as for instance, Frank Kerber, the former point person on counter terrorism cooperation with the E.U., emphasized the increasing interactions between E.U. and U.S. law enforcement and surveillance agencies.

Another demonstration of these joint efforts can be made by the U.S.-E.U. Declaration of June 2004 on Combating Terrorism. The text states “Since the attacks of 11 September 2001, the United States and the European Union have been working together closely to combat the threat of terrorism. In the aftermath of the attacks on Madrid on 11 March 2004, the European Council adopted a this Declaration,

---

reinforcing its determination to prevent and fight terrorism. Today we have renewed our commitment to further developing our cooperation against terrorism within the framework of the New Transatlantic Agenda”

Among the clauses discussed, several articles appear as strong demonstrations that the E.U. and the U.S. have stepped up their cooperation efforts.

The following table presents these clauses in more detail.
Table 5: U.S.-E.U. Declaration on Combating Terrorism, June 2004

<table>
<thead>
<tr>
<th>Article 1</th>
<th>“We will work together to deepen the international consensus and enhance international efforts to combat terrorism”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 3</td>
<td>“We commit to working together to develop measures to maximize our capacities to detect, investigate, and prosecute terrorists and prevent terrorist attacks.</td>
</tr>
<tr>
<td></td>
<td>3.1 We will promote cooperation between our law enforcement agencies and institutions, taking account of our respective legislation, for the purpose of the prevention, detection, investigation, and prosecution of terrorist offences. In particular:</td>
</tr>
<tr>
<td></td>
<td>3.3 We will work together to enhance, in accordance with national legislation, our abilities to share information among intelligence and law enforcement agencies to prevent and disrupt terrorist activities, and to better use sensitive information as allowed by national legislation in aid of prosecutions of terrorists in a manner which protects the information, while ensuring a fair trial.</td>
</tr>
<tr>
<td></td>
<td>3.4 We will collaborate on enhancing legal frameworks to prevent terrorism, including by ensuring appropriate legislation is in place to investigate and prosecute offences linked to terrorist activities and facilitate legal cooperation in relation to such offences.</td>
</tr>
<tr>
<td></td>
<td>3.6 We will work together to promote the use of appropriate investigative techniques, such as electronic surveillance, in combating terrorism and will collaborate in the development of mechanisms to protect witnesses and assist law enforcement.</td>
</tr>
<tr>
<td></td>
<td>3.8 We will seek to strengthen the exchange of information and the capacity for cooperation between the U.S. and Europol in accordance with the U.S.-Europol agreements.</td>
</tr>
<tr>
<td></td>
<td>3.9 We will explore ways to strengthen cooperation between U.S. prosecutors and Eurojust in accordance with the Council Decision establishing Eurojust.”</td>
</tr>
</tbody>
</table>
It is interesting to point out that by making this joint declaration, the European Union confirms its support for increased information sharing with the United States, the intensification of screenings and controls, the introduction of biometric identifiers and the development of better surveillance techniques. The expansion of these relationships has been strongly criticized by privacy advocates who argued that stepping up security measures would reduce the protection of civil liberties. The point argued in this thesis is not that the privacy advocates are against E.U.-U.S. cooperation, but that they push for a better balance between privacy and security. As a
result, this joint declaration reflects the desire of the Member States to increase security, even if it is at the detriment of civil liberties. Because of their dependence with the United States to succeed in the fight against terrorism, it has become in the European interest to favor security instead of privacy.

At the Union level, the same need for cooperation arose, especially as the London and Madrid bombings impacted on the Member States’ perception of threat. Indeed, after each attack, the Member States became less reluctant to trade off some privacy for more security. This is the case for the Data Retention Directive, which received greater acceptance following the bombings (Bouilhet, 2005).

The two waves of enlargement in 2004 and 2007 integrated 12 new countries in the E.U., pushing the European geographic limits further east. Some of these new countries are now in charge of ensuring border security and may not be well equipped to do so efficiently. As a result, the need for increasing security intensified and pressed for a greater collaboration between the Member States.

Finally, the awareness that Europe could also face terrorist attacks reinforced the dependence between Member States in terms of security and the need for law enforcement agencies to have appropriate tools to fight terrorism. The following Parliament News (2005) demonstrates this recognition of the cooperation importance: “New terrorist attacks on London public transport in July 2005 came as a powerful
reminder that EU Member States must step up co-operation in the fight against terrorism. Parliament has since voiced its concern at the lack of operational police and judicial co-operation and co-ordination needed to prevent attacks.” The EDPS, which also usually strongly criticizes the introduction of new security measures, took the same view and said it recognized “the importance for law enforcement agencies of the Member States of having all the necessary legal instruments at their disposal, in particular in the combat of terrorism and other serious crime. An adequate availability of certain traffic and location data of public electronic services can be a crucial instrument for those law enforcement agencies and can contribute to the physical security of persons” (Opinion, November 2005). The fact that, even these unconditional supporters of civil liberties agreed on the need to increase collaboration as a tool to fight terrorism, represents a significant argument in favor of harmonizing European national laws towards a more security-oriented approach.

**Bureaucratic Structure**

The bureaucratic structures of the European Union and the Member States influence the privacy and security debate as they determine the power of the opposition. In the scope of this thesis, I will analyze the role of Data Protection
Authorities and privacy advocates in regard to their place within the structure of the European Union. I will particularly analyze the influence of the Article 29 Working Party, the EDPS and the Data Protections Authorities, as they represent official institutions, set up by European laws. Because they have legal recognition, they should have more influence than independent privacy groups such as EPIC, Statewatch or Privacy International. However, I will argue that because of the independence (and isolation) of these institutions from their national governments and from most European Union institutions, they do not wield much power or influence.

Article 29 of the 1995 European Data Protection Directive set up the creation of the “Working party on the Protection of Individuals with regard to the Processing of Personal Data,” commonly known as the Article 29 Working Party. This institution, composed of representatives of the national Data Protection Authorities, the European Data Protection Supervisor (EDPS) and a member of the European Commission, has as its mission to advise the Commission on any project involving privacy issues, to contribute to the elaboration of European norms by adopting recommendations and to assess the level of protection in third countries.

The EDPS, an independent supervisory authority, was created in 2004 under Article 286 of the Treaty establishing the European Communities to harmonize data protection legislation in the European Union. This institution is in charge of ensuring
the respect of data protection and privacy in the European institutions and bodies and promoting good practices. Its main tasks are to supervise the actions of the European administration and assess the level of protection, to advise policies and legislation involving privacy issues and to cooperate with other data protections authorities to ensure consistent data protection (EDPS website).

Finally, the national Data Protection Authorities are responsible for the protection of privacy and data in their respective countries.

All of these institutions have an independent character, but are based on legal basis and still remain fully part of the European and national institutions. As a result, they have official recognition that a simple advocacy group could not obtain. In this sense, why did they not manage to provide a counterweight to those agencies pushing for policies that favor security over privacy?

Dorothee Heisenberg makes the same comments (2005) in the introduction of her book: “Although the Article 29 Working Party is an institutionalized committee established in the European Data Protection Directive, in this book it is often characterized as an “interest”, leading some to wonder why it would be classified with other groups that have to fight for government recognition; one significant difference between institutions and interests is that institutions have some legal rights leading
them to structure and participate in decision-making more officially, and (usually) more effectively than interests. Since, as was pointed out above, this is not true of the Article 29 Working Party, it functionally resembles an interest more than an institution.” (Heisenber, 2005, p17)

First of all, it is important to discuss the issue of the European pillars, already addressed in the previous chapter. Indeed, in the case of PNR, the decision was made under the third pillar, which cut off any power from the Data Protection Authorities. As well as the European Parliament and the European Commission, the privacy representatives do not have any role to play in the decision making of third pillar debates. Although the members of the Article 29 Working Party gave their opinion on the PNR issue, they were not allowed to do so in the name of the Working Party, as such entity only has legal status in the first pillar.

In the case of data retention, the decision was made under the first pillar, which granted the European Parliament co-decision powers and legalized the involvement of the Data Protection Authorities. Even if the Directive was actually passed, one could argue that the influence of the Working Party and EDPS has managed to limit the civil liberties damages and obtain greater concessions than for PNR. As a result, in cases where the Data Protection Authorities are involved, the decisions made include better privacy safeguards.
Another issue faced by the Data Protection Authorities is that their status does not require the European institutions to involve them in discussions and debate held under the third pillar. Indeed, this limitation means that the privacy representatives were not even invited to all of the critical decision-making meetings. For instance, while negotiating the Data Retention Directive, the U.K. organized on September 8 and 9, 2005, a JHA Council informal two-day-meeting. Although the privacy issue was strongly linked to the discussions, the Data Protection Authorities were not invited (EDRI-gram - Number 3.18, 2005).

During the PNR debate, the Working Party issued several opinions, consistently emphasizing the lack of data protection and the unsatisfactory character of the several agreements. The October 11, 2007 press release25 pointed out the same weaknesses, which they’d criticized in the very first agreement proposals. But the Working Party did not have the power to force the European institutions to take its recommendations into account.

The EDPS recommendations received the same treatment. Peter Hustinx, the European Data Protection Supervisor, wrote in July 2007 to the European Commission to express his “grave concern” for the PNR Agreement, describing it as “without legal precedent” and warning that “Data on EU citizens will be readily accessible to a broad

range of US agencies and there is no limitation to what US authorities are allowed to do with the data. Once more, these concerns were ignored by the European Commission. According to The Observer (2007), which reported on Hustinx’s letter, neither EDPS nor the European Parliament saw the final draft of the agreement. This emphasizes again the limited recognition granted to their authority by the European Commission.

The European Parliament was the most critical of the agreements, regularly underlining their weaknesses. The MEPs also denounced the fact that these accords were concluded without the involvement of any members of Parliaments from the European or the American side and emphasized the lack of democratic oversight (European Parliament News, 2007). The MEPs took the opportunity of the PNR debate to express their desire to have joint decision-making rights with the Council of Ministers to protect better European privacy, if a European PNR agreement was to be implemented.

These findings can also be applied to the Data Retention debate as the European Parliament, the Working Party and the EDPS openly opposed the legislation. Their

unfavorable opinions and critical recommendations did not have more effect than during the PNR debate. Interestingly, even if the final draft was taken under the first pillar basis and thus in co-decision with the Parliament, the MEPs gave in under the pressure from the Council and the Commission and accepted to sign the Directive. The final agreement closely resembled the previous proposals that the Parliament had strongly criticized, but the MEPs still validated it.

The national Data Protection Authorities also seem to have a limited influence with their own governments. Indeed, they often do not have a budget corresponding to their needs and are understaffed. In some countries, the Data Protection Authority is only represented by one person. In other, the tasks they are responsible for are so great, that they just cannot carry out their action effectively, if at all. This is the case of the CNIL (Commission National d’Informatique et des Libertés), the French Data Protection Authority, whose activity keeps growing and its budget remains extremely limited\(^{27}\). Indeed, since his appointment as president in 2004, Alex Turk has been asking the government for more funds, just like his predecessors had done. In 2006, he compared the CNIL to a company in a situation of bankruptcy. Following these complaints, the government granted an increase in budget of a €300,000. The

following year, this rise was of €400 000. This seems to be an improvement of the situation and a sign that the CNIL still managed to get heard. However, the activity of the CNIL has grown so much that these increases in funds appear insignificant. For instance, in 2005, the number of controls supposed to be carried out by the CNIL increased by 235%, in comparison from the previous year and the number of controls actually realized rose by 113% (still not representing the total amount planned). The sum of decisions taken in 2005 also rose by 200%. Alex Turk pointed out that for certain types of complaints, the CNIL has sometimes several years of delay. In 2005, he also asked for the doubling of its staff, as a necessity to carry out the CNIL mission, but only half of the 20 jobs required were granted. Finally, the 1978 legislation was amended in April 2004 expanded the roles and tasks of the CNIL. The Figaro even stressed that in these circumstances, the tasks of the CNIL were almost impossible to carry out (2007).

Moreover, the actual influence of the CNIL is also controversial, as many criticized its lack of opposition to the government. In December 2007, the CNIL offices were even invaded by civil liberty groups which wanted the dissolution of the Commission, arguing that it was not standing up for the citizens’ privacy but instead simply sided with the government.
Finally, the Data Protection Authorities do not necessarily have representatives working within the domestic key institutions. For instance, in the United States, privacy officers work in most significant federal agencies, such as the Department of Homeland Security, the Department of Justice (Office of Information and Privacy) or the Department of Health and Human Services. As such, they are more able to influence debates. Particularly, the Privacy Chief Officer of the Office of Management and Budget benefits from real leverage, as he/she works in the agency responsible for overseeing the budget of Federal agencies and reviewing their IT projects.

This situation is similar at the European Union level since Data Protection Officers are employed in the main agencies such as the European Central Bank, the European Agency for the Management of Operational Cooperation at the External Border (FRONTEX) or the Court of Justice of the European Communities. However, at the domestic level, national governments have not always appointed privacy representatives in their key agencies. Since some European security decisions are made under the third pillar and only based on the Member States’ preferences, the privacy issue will not ensure representation at the European level if the national Data Protection Authorities have no means of influencing their own government.

The limited influence of the national Data Protection Authorities can also be assessed by the little awareness the population has in their existence. In December
2005, 63% of the French population did not know the CNIL and in 2006 only 15% of the British population had heard of the Information Commissioner’s Office (ICO).

The Data Protection Authorities only have the leverage provided by the 1995 European Data Protection Directive and the fact that they can reach out to the population to denounce privacy infringement. In the case of PNR and data retention, they have been actively criticizing the European Commission’s decisions, but without success. Because they have limited leverage on the Member States due to its bureaucratic structure, the European countries just did not pay attention to these recommendations. The leverage left was the public opinion rallying in support of the Privacy authorities. However, the European citizens did not side with these critics, as they may consider security as the most important priority.

Because Privacy authorities are constrained by the weakening European bureaucratic structure, they do not benefit from a significant power to influence the outcome of the negotiations. As a result, they were not players in the signing of the PNR, had limited impact on the data retention agreements and have not slowed the shift in the position of the European Union towards a more security-oriented approach.

However, by looking at the reasons why these authorities have such a limited power, one could argue that the national governments are responsible. Indeed, the choice of granting little funds and recognition to the Privacy authorities stems from the
Member States themselves, and thus one could wonder if the European countries do not reduce the Data Protection Authorities’ influence on purpose, as it goes against their preferences. Finally, the Article 29 Working Party and EDPS follow the same logic, as the Union did not decide to grant them more authority and recognition. Siding with the Data Protection Authorities thus did not seem to be in the general interest of the European Union, demonstrating a preference for security measures.

**Conclusion**

The theories discussed above represent five significant explanations as why the European Union security policy has become more aligned on their American counterparts’ strategy. But a general trend seems to appear. Indeed, whether they are domestic preferences, economic interdependence, security dependence, or linked to bureaucratic structure, the reasons why the EU is moving towards a more security-oriented society stems from European interests. It now seems that the Members States want such changes to happen, influencing decisions at the domestic and European levels.

The assumption expressed earlier that the E.U. is using American coercion as a justification appears even more relevant. Instead of openly facing a conflict with Data
Protection Authorities and civil liberty groups whose influence has been limited anyway, the E.U. puts the blame on the United States for forcing them to adjust to their security preferences.

Finally, some Members States have implemented security measures that have not been introduced in the United States, such as national identity cards. The European Union had also agreed to introduce biometrics components in passports even before the United States required it as a condition of entry on their territory. As Gus Hosein (2005) argues, “when you compare the surveillance laws in Europe and the U.S. you find that the EU always goes further.” Finally, the fact that European Union is now discussing the implementation of a European PNR transfer system similar to the E.U.-U.S. agreement reinforced the assumption that the Member States approved of the data exchange at the first place. As Sophie In't Veld, a Dutch Liberal MEP, put it, “It is disingenuous of the Commission to tell us in July that they fought to resist US demands for an intrusive system only to propose a similar system themselves four months later” (Financial Times, 2007). The shift in balance between privacy and security thus seems to be only partially based on the coercive actions of the United States, but more on the emergence of a general European interest in prioritizing security over privacy.
Chapter Six: Conclusion

Since September 11, European law enforcement and judiciary agencies have been granted more and more power and means to ensure citizens’ safety. In this regard, the European Union is clearly shifting its position to reflect the general perception that security has become a priority, even if it requires trading off some privacy protections. Despite vehement protests from the Data Protection Authorities and the European Parliament, the E.U. signed several data sharing agreements with the United States, introduced biometric components in its passports and plans on setting up a fingerprint database by the end of 2008. These examples only illustrate the dynamics at the European Union level. Domestic priorities have followed the same trend and several Member States even implemented further-reaching security policies, in the name of fighting terrorism.

Throughout this thesis, I have examined the drivers of the European policy change, arguing that coercion, often used as the sole excuse for Europe’s shift in position, is not sufficient to fully understand the forces at play. Domestic preferences, interdependence with the United States in terms of national security and economics and the limited power of Data Protection Authorities have all shaped European Union policies regarding privacy and security. These four factors are based on European
characteristics and it is the evolution of such European internal dynamics that has led to a shift in the general interests of the E.U.

The five policy diffusion theories discussed at length in the previous chapters bolster the argument advanced in this thesis, as each of them offer a complementary hypothesis explaining the reasons why the European Union is more closely aligning its privacy and security polices with those of the United States.

The coercion statement, claiming that the U.S. forced the E.U. into becoming more security-oriented, is commonly put forth both by national governments and representatives of European institutions. The influence of the United States clearly impacted the European shift in position, as the U.S. threatened to use sanctions against the E.U. But some European governments found it politically useful to explain their domestic change in policy as being due to U.S. pressure. Indeed, they were now able to pass policies that had previously failed adoption at the national level, presenting them as obligations forced upon by international forces, especially by the U.S.

However, this thesis has argued that other important factors have pushed the Member States towards adopting the U.S. policies. Indeed, I have demonstrated that domestic preferences played an important role in the shift of European position, as several Member States strongly influenced the debates. The study of the British, French and German policies has pointed out their support for additional security
measures, even if it reflects negatively on privacy rights. Because these three countries have substantial power within the E.U., they were able to push their national preferences at the European level.

Economic interdependence between the United States and the European Union, as well as their dependence on each other in terms of security, also represents two substantial complementary explanations as to why the E.U. is adopting policies aligned with the U.S. preferences. Because several American “incentives” would have strongly affected the E.U. economy, which is closely interrelated to the American’s, the Member States had to take into consideration the priorities of the United States and were convinced to follow its security and privacy approach.

Likewise, the need to cooperate in order to ensure the safety of the citizens has arisen as an indispensable condition of success against transnational terrorism. Because the security of the population represents an ultimate priority, the E.U. adjusted its policies to this increasing need and adopted American measures.

Finally, the bureaucratic structure of the European Union plays an important role in the adoption of foreign policies. Because the Data Protection Authorities do not benefit from powerful means of influence and were often kept out of key decision-making meetings, they were not able to efficiently counter the European policy shift.
The two case studies analyzed in this thesis have substantially demonstrated my argument. They complement each other as they point to the same finding: the important role of changing European interests as a force pushing the E.U. to align its security strategy with American policies. Both PNR and data retention reinforce the fact that Europe is becoming more security-focused and that European governments use American coercion as an excuse to adopt stricter policies. For instance, the European Commissioners declared that they disapproved of the PNR Agreement and that they had no choice but to accept the conditions of the United States. However, a couple of days before the signing of the U.S-E.U. treaty, Justice Commissioner Franco Frattini proposed a similar PNR system to be implemented at the E.U. level. This underlines the fact that the European Commission actually wanted the E.U.-U.S. Agreement in the first place but tried to avoid facing the privacy advocates’ opposition. In the case of data retention, the Directive was debated at the European level without significant participation by the United States government. The resulting agreement, favoring security over privacy safeguards was reached by European Member States only, which emphasized the fact that the pressures for security came from within the Union.
This thesis adds to the existing literature, as it brings a different perspective to the privacy and security debate by using policy diffusion theories. While writing this paper, I have sought to approach the issue in a new way by expanding the theoretical lens through which it has previously been viewed. While the few writers analyzing this topic have focused on coercion, examining all the drivers of European policy change is a critical element to understanding how and why decisions are made at the national and transnational levels.

Limitations

Nonetheless, this thesis does have several limitations. First, the European debate surrounding privacy and security has taken on a new significance since September 11 and has gained intensity over the years. As a result, it is difficult to get a complete perspective of the major events and find many in-depth studies relevant to this issue. In addition, because this paper addresses national security, some key information is classified and thus unavailable. This makes it hard to find comprehensive analyses of the situation, to fully grasp the power of each actor and to assess the impact of each decision made. Moreover, the scope of this issue is wide and complex as it involves numerous players and several levels of influence. In this thesis,
I have addressed the privacy and security issues particularly at the European and Member State levels. Analyzing more in depth the internal dynamics driving a country decision-making process would bring additional insights to the general issue. Finally, there is a difference between implementing a law and actually applying and respecting it. Indeed, the fact that numerous decisions are made at the European level but partially or not at all transposed into national legislation is hard to take into account and challenges the basis of my analysis.

**Policy recommendations**

With the European Data Protection Directive of 1995, the Member States set international standards for privacy. Even if only few countries have a level of protection considered by the E.U. as adequate, many states have adopted policies reflecting the European model. Because the Member States prided themselves on their respect of civil liberties, they represented a counterweight for the strict security measures increasingly implemented in the United States. Even in the aftermath of the World Trade Center attacks, the European Union criticized American practices as
being overreactive. However, as argued in this thesis, this position has changed. It is important here to remember that the European Data Protection Directive of 1995 is still in effect and strongly regulates general privacy issues. The Directive was only loosened for law enforcement and police matters, which still is a substantial weakening of privacy safeguards. This shift in European policies will have global repercussions because opponents of security measures that reduce civil liberties protections will be less able to use the European model as a counter-argument.

Evidently, the preference for counter-terrorism strategies over privacy is not shared by every player within the Union. However, what matters is that the deciders are the proponents of increasing security. Nonetheless, as mentioned earlier, improving privacy is crucial to enhance security. Both the European Union and the United States should keep this in mind since they argue that citizens’ safety is their most important priority. In this case, the best way for them to achieve this primary goal is to implement privacy safeguards, in addition to security measures.

The current situation of favoring security policies that neglect privacy rights has been emerging in Europe for several years and one could think that this trend will continue into the next decades. Because security has become a clear trade-off for civil

---

liberties, there is a need to reestablish a better balance in favor of privacy. The first thing coming to mind would be to increase the power of Data Protection Authorities and their involvement in security matters. Indeed, the major concern is that often, the privacy representatives are not included in crucial discussions, either because these debates are introduced on the third pillar basis where the Article 29 Working Party does not have authority, or simply because the leaders of the meetings can chose not to invite them.

This thesis has already addressed the weak influence of the Data Protection Authorities due to the E.U. bureaucratic structure. In the European model, privacy representatives – whether EDPS, the Article 29 Working Party or the Data Protection Authorities – benefit from an independent status, but only receive little consideration from the European institutions, which limits their influence in debates. On the other side, the United States has set up Chief Privacy Officers in a number of key federal agencies, to ensure that privacy issues are considered during policy discussions. However, since these Officers report to the head of their agency, there are limits to how critical they can be of their agencies’ policies and how public they can with their criticism.

A way of ensuring that privacy representatives are involved in the security debates would thus be to adopt a structure for the Data Protection Authorities that
reflects the advantages of both U.S. and E.U. systems. Even if the European Union has set up a network of Data Protection Officers represented in the main European institutions, it is not always the case at the domestic level. Since some of the European directives are adopted in the third pillar, the agreement is made between the European governments only. If the Data Protection Authorities do not have representatives in key domestic agencies and have only limited power at home, they will not be able to influence their own governments and the privacy issue will not be represented at the European level.

In addition to this change in status, the powers of the Article 29 Working Party should be expanded to the third pillar issues, as security matters and agreements have also been signed within this field. Because the Data Protection Authorities did not have the authority to express their opinion, the issue of privacy was not represented in the debates.

By making sure Privacy Authorities are not left out of the discussions, the European institutions would be more strongly inclined to listen to their recommendations. The Data Protection Authorities are already condemning some security measures but do not have the leverage to force the Member States to listen to them. By making their presence mandatory in each security debate, they would gain considerable influence.
Finally, improving privacy representation could be done by ensuring that the security measures proposed and accepted do not go against any existing privacy laws. In addition to this, there is also a difference between implementing a privacy policy and actually applying it. As a result, setting up better oversight mechanisms would ensure that Member States are complying with the existing privacy legislation and do not discreetly circumvent them.

However, this general perspective on how to improve privacy representation seems too simplistic as the Data Protection Authorities can only do so much. Indeed, particularly in the third pillar, the European governments are in control of the decisions. Regarding privacy, they don’t want to increase the power of the Data Protection Authorities, since it would interfere with their own interests. Since they are the ones making the rules of the European Union functions, how could the governments be pushed towards accepting such compromise?

Gus Hosein (2005) argues that Europe is becoming more aligned with American policies and more security-oriented because there is little public discussion, since decisions are made within the E.U. institutions and not at the Member State level. He also demonstrates that the more a policy is publicly discussed, the greater the chance it will be criticized and modified. Because the privacy and security matters are
debated behind closed doors at the E.U. level and the governments have politicized these issues, the European citizens do not get the opportunity to be involved. By increasing awareness of their privacy rights through the media, national Data Protection Authorities or civil liberties advocates and by involving the public opinion to a greater extent, the governments would be obliged to give privacy defenders a stronger consideration.

As mentioned among other policy diffusion theories, a change in public opinion can influence a government to adopt a certain policy. In this case, it would not be that much of a change in European perspective but the emergence of a preference and concern for privacy. As a result, if the European citizens were more involved in the privacy and security debate, they could ask the governments to reconsider privacy as a priority. Since the governments are the ones enacting rules limiting the power of the Data Protection Authorities, pressure from the public could represent a significant way to ensure that privacy is brought back into the debates.

Some of these recommendations could also apply on the American side of the Atlantic. The current Presidential election has witnessed an increase in the recognition of the privacy issue, as Barack Obama and especially Hillary Clinton addressed this matter in their campaigns. The U.S. already has the advantage of having Chief Privacy
Officers within the key federal agencies, but their effectiveness depends largely upon their agency’s leadership. For instance, internationally recognized privacy expert Peter Swire strongly improved the appreciation of the privacy issue while serving as the Clinton Administration's Chief Counselor for privacy in the U.S. Office of Management and Budget. However, he was not reappointed or replaced when President Georges W. Bush took office in 2001. An efficient way to ensure that the Chief Privacy Officers’ position remains in effect, without consideration of the Administration in charge, would be to grant these privacy representatives a status comparable to the one of Inspector Generals, auditors of the government activities. Alternatively, the Chief Privacy Officers of key agencies could be required by legislation and subject to greater Congressional oversight. This could also give them the opportunity to express their opinion freely without fearing repercussions from the government, a position enjoyed by independent European Data Protection Authorities.

The terrorist attacks in New York City, Madrid and London, which had huge repercussions worldwide because of their spectacular aspects, have created momentum for the proponents of increased security measures. Since then, governments have emphasized the risk of threats, advocating for better safety measures even if their costs and implications were high. As Schneier (2005) explains, security always has trade-
offs, be they financial, logistical or privacy-related. Were the terrorism threat to diminish, the public might start to reconsider whether the security trade-offs are worth the inconvenience and governments may find it harder to demand further expansion of their powers. This is a paradox in that the reduction of the threat of terrorism implies the construction of better counter terrorism, intelligence and security tools, which brings us back to the central debate: how to balance security and privacy to ensure the improvement of both. In the meantime, European and American governments should remember: “They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety” (Benjamin Franklin, 1759).
References


Booth, Jenny. Clarke threatens MEPs over EU terror laws. *The Times*, October 12, 2005


Commission of the European Communities Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final, November 6, 2007


Council Decision on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security 2006/729/CFSP/JHA. October 16 2006


Données des passagers - Berlin accepte les demandes américaines. *Agence France Presse*. March 13, 2004


Foucart, S. (2004, 14 juillet). A l'heure du passeport biométrique, le contrôle des fichiers internationaux est plus sensible que jamais ; FRANCE SOCIÉTÉ les pouvoirs de la CNIL devraient être considérablement amoindris. Le Monde,


German Ministers at Odds Over EU Passenger Data Plan, Deutsche Welle. January 29, 2008


Give us those data; airline security.(2006, June 3). The Economist


Hustinx Peter. EDPS. *New PNR agreement with the United States of America*. June 27, 2007,. Letter to Wolfgang Schauble


178
Kerr, M. (2003, July 19). You won't have noticed, but Uncle Sam is watching you. The Daily Telegraph (London)


http://www.nytimes.com/2005/06/16/national/16privacy.html?_r=1&oref=slogin


O'brien, K. J. (2005, September 22). EU sets new plan on data retention ; A bid to harmonize 'diversity in our laws'. The International Herald Tribune, pp. 1.


Oceans apart. (2006, December 1) The Guardian


Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes MEMO/07/449. November 6, 2007


Pinson, G. (2005, 4 mai). L'industrie de la communication S'inquiète des projets de bruxelles. La Tribune,


Rasmussen Reports. Is the following country an ally or enemy of the U.S.? Retrieved in March 2008 from: http://www.rasmussenreports.com/public_content/politics/ally_enemy/ally_or_enemy


REMID. Religionen in Deutschland: Mitgliederzahlen; Retrieved in March 2008 from : http://www.remid.de/remid_info_zahlen.htm)


Rennie, D. (2006, June 10). The truth is that europe is america's poodle; The Spectator, 20 21.

Research and Documentation Centre of the Dutch Ministry of Justice, (2006). First inventory of policy on counterterrorism: Germany, France, Italy, Spain, the United Kingdom and the United States – ‘research in progress’


The fight within; Counterterrorism in Europe.(2005, July 23). *The Economist*


U.S., Britain to increase joint anti-terrorism efforts.(2003). *CongressDaily, , 13.*

U.S. Customs Service. Passenger Name Record Information Required for Passenger on Flights in Foreign Air Transportation to or from the United States. Interim Rules.19 CFR Part 122. June 19, 2002


Vital-Durand Brigitte. La Cnil affiche les fichiers qui fâchent. *Libération.* June 23, 2004


Wright, Lawrence (January 21, 2008) The Spymaster; A Reporter at Large. *The New Yorker*