Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State

VALSAMIS MITSILEGAS*

ABSTRACT

In stark contrast to the field of legislation on the rights of third-country nationals or to the requirements and conditions for access to the territory of states, the field of the enforcement of immigration control has been increasingly subject to legal harmonization: either by the adoption of global law on immigration control or by the convergence of domestic law and policy in the field. This convergence is particularly marked when one compares legal responses to immigration control in the United States and the European Union, where globalization has been used to justify the extension of state power—by proclaiming state action necessary in order to address perceived global security threats—and the use of key features of globalization that may facilitate free movement—such as the use of technology—in order to enhance immigration control. Globalization has led to the strengthening, rather than the weakening, of the state. This strengthening of the state has significant consequences not only for immigration but also for citizenship as expressed by both relations between individuals and between citizens and the state. By examining the global and transatlantic policy and legislative consensus on immigration control, this Article will cast light on the challenges the extension of state power that globalized immigration control entails for fundamental rights and the rule of law.

INTRODUCTION: GLOBALIZATION AND THE LAW OF IMMIGRATION CONTROL

The aim of this Article is to explore how the law of immigration control has been transformed in a globalized world. While immigration control has traditionally been perceived as the prerogative of the state

* Professor of European Criminal Law and Director of the Criminal Justice Centre at Queen Mary University of London.

Indiana Journal of Global Legal Studies Vol. 19 #1 (Winter 2012)

and as a prime example of the exercise of state sovereignty via state power, globalization has challenged this assumption by questioning territorial borders and facilitating the movement of people around the world. This perception of globalization as a facilitator of immigration—including undesired mobility on the part of the receiving states—has led to the development of a series of legislative measures aimed at enhancing border controls. In stark contrast to the field of legislation on the rights of third-country nationals or to the requirements and conditions for access to the territory of states, the field of the enforcement of immigration control has been increasingly subject to legal harmonization: either by the adoption of global law on immigration control or by the convergence of domestic law and policy in the field. This convergence is particularly marked when one compares legal responses to immigration control in the United States and the European Union and is based on a transatlantic consensus on the need to extend the powers of the state—both in terms of capacity and in terms of territorial reach—in order to address global flows of people. A key element of this strategy is the use of globalization to justify the extension of state power—by proclaiming state action necessary in order to address perceived global security threats—and the use of key features of globalization that may facilitate movement—such as the use of technology—in order to enhance immigration control. In this manner, globalization has led to the strengthening, rather than the weakening, of the state.

This Article will attempt to demonstrate that this strengthening of the state has significant consequences not only for immigration, but also for citizenship as expressed by both relations between individuals and between citizens and the state. By examining the global and transatlantic policy and legislative consensus on immigration control, this Article will cast light on the challenges the extension of state power that globalized immigration control entails for fundamental rights and the rule of law.

I. GLOBALIZATION, IMMIGRATION CONTROL, AND SECURITY

Writing on the link between "illegal" immigration and globalization, Catherine Dauvergne has noted that

> [t]he impression that the problem of illegal migration is a global one, and the fact that those who seek to migrate outside the law have access to a geographically broader range of options than in earlier eras, contribute to the

> construction of an identity category of people named by the new noun "illegal."[1]

This link between globalization and the perceived facilitation of unwanted movement it entails has justified the enhancement of immigration control in the West. Going a step further and looking beyond the debate over illegality in immigration law, this part will demonstrate how immigration control has been transformed by shaping state responses to counter perceived global security threats. Rather than focusing only on countering "illegal" movement (or, as Dauvergne puts it, "migration outside the law"), immigration control here focuses more generally on countering movement which is considered "dangerous" or a security threat. This securitized approach, which links migration and movement to evils such as transnational organized crime and terrorism, has enabled the development of a global enforcement consensus. The translation of this consensus into legislation has signified a considerable extension of state power at the expense of rights not only of foreigners but also of citizens: as will be demonstrated below, in particular in the case of counterterrorism, securitized immigration controls have shifted the focus from immigration control of third-country nationals at the physical border to the generalized surveillance of third-country nationals and citizens alike.

A. Immigration Control as a Response to the Threat of Transnational Organized Crime

The securitization of immigration control in a global context is evident in the first major multilateral convention aiming to develop global legal norms to counter the threat of transnational organized crime. Reflecting the post-Cold War framing of transnational organized crime as a global security threat in need of urgent countermeasures,[2] the response of the international community has been the adoption of the United Nations Convention on Transnational Organized Crime, symbolically signed in Palermo in 2000 (Palermo Convention). Negotiated throughout the 1990s, the Palmero Convention is an ambitious and comprehensive multilateral instrument aiming at combating and preventing organized crime. It contains provisions ranging from the criminalization of participation in an organized crime

---

1. CATHERINE DAUVERGNE, MAKING PEOPLE ILLEGAL: WHAT GLOBALISATION MEANS FOR MIGRATION AND LAW 19 (2008).

2. *See generally* VALSAMIS MITSILEGAS ET AL., THE EUROPEAN UNION AND INTERNAL SECURITY: GUARDIAN OF THE PEOPLE? 42-59 (2003) (discussing the securitization of organized crime).

group, money laundering, and corruption to provisions on judicial cooperation with regard to organized crime, police cooperation, and the law of criminal procedure. The Convention is complemented by three protocols on human trafficking, human smuggling, and the illicit manufacturing and trafficking in firearms. Following the model of the Convention, the Protocols also contain provisions on criminalization and enforcement.[3]

It is by no coincidence that the first major global legal instrument adopted by the international community on immigration control was prompted by security considerations. As Anne Gallagher has noted, "[w]hile human rights concerns may have provided some impetus (or cover) for collective action, it was clearly the sovereignty/security issues surrounding trafficking and migrant smuggling, as well as the perceived link with organized criminal groups operating across national borders, that provided the true driving force behind such efforts."[4] Rather than focusing on the immigrant, the Trafficking and Smuggling Protocols were justified primarily on the basis of the need to protect states from transnational criminality. This "securitized" approach has been criticized heavily for effectively criminalizing migration and extending the reach of the state, with James Hathaway arguing that "the focus of the transnational effort against human trafficking on the prevention of cross-border movements created a legal slippery slope in which it proved possible to set a transnational duty to criminalize not only 'human trafficking' . . . but also the much broader phenomenon of human smuggling,"[5] and that the U.N. intervention is really a pretext for the globalization of border control.[6]

1. The Case of Trafficking in Human Beings

To a great extent, a close examination of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (Trafficking Protocol) does justice to the above claims. While it is true that the Protocol focuses on the criminalization of trafficking and

---

3. *See, e.g.*, DAVID MCCLEAN, TRANSNATIONAL ORGANIZED CRIME: A COMMENTARY ON THE UN CONVENTION AND ITS PROTOCOLS (2007) (providing legal analysis on the text of the UN Convention Against Transnational Organized Crime); *see also* Dimitri Vlassis, *Drafting the United Nations Convention against Transnational Organized Crime*, *in* COMBATING TRANSNATIONAL CRIME: CONCEPTS, ACTIVITIES AND RESPONSES 356, 356-62 (Phil Williams & Dimitri Vlassis eds., 2001) (discussing the adoption of the convention).

4. ANNE T. GALLAGHER, THE INTERNATIONAL LAW OF HUMAN TRAFFICKING 71 (2010).

5. James C. Hathaway, *The Human Rights Quagmire of "Human Trafficking,"* 49 VA. J. INT'L L. 1, 5 (2008). *But see* Anne T. Gallagher, *Human Rights and Human Trafficking: Quagmire or Firm Ground? A Response to James Hathaway*, 49 VA. J. INT'L L. 789 (2009).

6. Hathaway, *supra* note 5, at 25-35.

the prosecution and punishment of the traffickers and not the trafficked persons,[7] the Protocol does trigger a raft of enforcement measures[8] and the provisions on the rights of trafficked persons have been drafted with the interests of the state firmly in mind. While the Trafficking Protocol does contain a separate part on the protection of victims,[9] the latter includes a provision on repatriation[10] and the two provisions aiming at granting rights to victims in the receiving state render these rights largely conditional upon the discretion of the signatory states. Article 6 of the Protocol on Assistance to and Protection of Victims of Trafficking obliges states to inter alia, "*[i]n appropriate cases and to the extent possible* under its domestic law. . . protect the privacy and identity of victims of trafficking in persons, including, inter alia, by making legal proceedings relating to such trafficking confidential" (emphasis added);[11] to introduce measures to "provide to victims. . . *in appropriate cases*: (a) Information on relevant court and administrative proceedings; (b) Assistance to enable their views and concerns to be presented and considered at appropriate stages of criminal proceedings" (emphasis added);[12] and "to *consider* implementing measures to provide for the physical, psychological and social recovery of victims of trafficking" (emphasis added).[13] On the other hand, Article 7(1) of the Protocol on the Status of Victims of Trafficking in Persons in Receiving States calls upon states to "*consider* adopting legislative or other appropriate measures that permit victims of trafficking in persons to remain in its territory, temporarily or permanently, in appropriate cases" (emphasis added).[14] In implementing the above provision, states must "give appropriate consideration to humanitarian and compassionate factors."[15]

The Trafficking Protocol thus links the rights of victims of trafficking with security of residence under the immigration law in the receiving state. This approach has been criticized by Elspeth Guild, who points out that "[b]y focusing on the foreignness of the victim, which is determined by the fact of the border crossing and the lack of a right of

---

7. See Article 5 on Criminalization, in conjunction with the use of terms as defined in Article 3, in Trafficking Protocol, G.A. Res. 55/25, Annex II, U.N. Doc. A/RES/55/25, at 32-33 (Jan. 8, 2001).

8. See Articles 9-13, *id.* at 35-37. Note, however, the human rights and nondiscrimination saving clause in Article 14, *id.* at 37.

9. See Articles 6-8, *id.* at 33-35.

10. See Article 8, *id.* at 34-35.

11. *Id.* at 33.

12. *Id.*

13. *Id.*

14. *Id.* at 34.

15. *Id.*

residence, the issue is moved from one about working conditions to one about immigration," adding that "[t]he central issue about security within the labour force is exchanged for the issue of the security of border controls and foreigners."[16] This shift of focus from labor exploitation to security may also lead to rendering any rights granted to victims of trafficking under immigration law conditional upon the perceived "usefulness" of the victim to the state. Under this functionalist logic, the state has the discretion to provide security of residence to victims only if the latter prove to be useful in the prosecution of trafficking cases.

This trend has been prevalent in the European Union, where a number of EU initiatives related to the position of the victim have been framed and justified under a functionalist, prosecutorial logic. This trend is particularly visible in the 2004 Directive on the Residence Permit to Victims of Trafficking,[17] which was adopted with the specific purpose "to define the conditions for granting residence permits of limited duration, linked to the length of the relevant national proceedings, to third-country nationals *who cooperate in the fight against trafficking in human beings or against action to facilitate illegal immigration*" (emphasis added).[18] Following this logic, the directive places a duty on Member States to consider issuing a residence permit for victims of trafficking if the following conditions are met: the opportunity presented for the victim to prolong his or her stay on its territory for the investigations or the judicial proceedings; the demonstration by the victim of a clear intention to cooperate; and the victim having severed all relations with those suspected of human trafficking.[19] Residence permits may thus be provided to victims only if they facilitate the prosecution of suspected traffickers. Not only that, but the residence permit provided is entirely conditional upon the progress of the criminal proceedings—it will not be renewed if the above conditions cease to be satisfied or if a decision adopted by the competent authorities has terminated the relevant proceedings.[20] This approach is also echoed in the recently adopted Directive on Trafficking in Human Beings,[21] whose protective provision placing Member States under the duty to allow their national authorities "not to prosecute or impose penalties on victims" for their involvement in criminal activities that they have been compelled to commit as a direct consequence of being

16. ELSPETH GUILD, SECURITY AND MIGRATION IN THE 21ST CENTURY 174 (2009).
17. Council Directive 2004/81, 2004 O.J. (L 261) 19 (EC).
18. See Article 1, *id.* at 20.
19. See Article 8, *id.* at 22.
20. See Article 13(1), *id.* at 23.
21. Council Directive 2011/36, 2011 O.J. (L 101) 1 (EU).

subjected to trafficking (Article 8) has also been justified partly under a prosecutorial logic.[22]

2. The Case of Human Smuggling

Similar concerns regarding the consequences of the securitization of migration for the individual arise from the provisions of the Protocol on the Smuggling of Migrants. While it is true that criminal liability for human smuggling does not extend to the smuggled migrants themselves, with the Protocol expressly stating that migrants will not become liable to criminal prosecution for the fact of having been the object of smuggling,[23] the provision on the criminalization of smuggling expressly states that it does not prevent states from taking measures against a person whose conduct constitutes an offense under their domestic law.[24] The Smuggling Protocol thus does not prevent states from treating illegal entry, stay, or residence as such as criminal offenses under their domestic law.[25] Moreover, the Smuggling Protocol does not expressly exclude the criminalization of individuals or organizations that provide assistance to individuals for the purposes of them accessing or remaining in the territory of states in order to lodge an application for asylum.

Such criminalization is very likely implicitly excluded by the requirement in the Protocol for the smuggling offenses to be instituted only when committed intentionally and in order to obtain financial gain,[26] and, as in the case of the Trafficking Protocol, concerns with regard to the rights of asylum seekers have led to the inclusion of a human rights saving clause in the Protocol.[27] However, this may not be sufficient to limit the consequences stemming from a broad

---

22. *Id.* at 7. According to the Preamble to the Directive, "[t]he aim of such protection is to safeguard the human rights of victims, to avoid further victimisation *and to encourage them to act as witnesses in criminal proceedings against the perpetrators*" (emphasis added). *Id.* at 3.

23. *Id.* at 7.

24. Protocol Against the Smuggling of Migrants by Land, Sea and Air, Supplementing the Convention Against Transnational Organized Crime art. 6(4), Nov. 15, 2000, *available at* http://www.unhcr.org/refworld/docid/479dee062.html [hereinafter Smuggling Protocol].

25. *Id.* The recent Italian legislation constitutes a prime example of such criminalization. However, the use of criminal law sanctions in the context of failing to leave the country was ruled as contrary to EU law by the Court of Justice of the European Union in the recent ruling. *See* Case C-61/11, Corte d'appello di Trento v. El Dridi, O.J. (C 113) (2011).

26. Smuggling Protocol, *supra* note 24, art. 6(1).

27. *Id.* art. 19. For background to the negotiations, see Anne Gallagher, *Human Rights and the New UN Protocols on Trafficking and Migrant Smuggling: A Preliminary Analysis*, 23 HUM. RTS. Q. 975, 994 (2001).

criminalization approach. This is evident when one examines the definition and criminalization of human smuggling at the EU level. The directive defining what is called in EU law the "facilitation of unauthorized entry, transit and residence"[28] goes further than the Smuggling Protocol in that it does not require one to obtain a financial or other material benefit for the smuggling offense to be established.[29] The Directive calls upon member states to adopt criminal sanctions for "any person who intentionally assists a person who is not a national of a Member State to enter, or transit across, the territory of a Member State in breach of the laws of the State concerned on the entry or transit of aliens. . . ."[30] The scope of criminalization is very broad as it can cover any form of assistance to enter or transit the territory of an EU Member State in breach of what is essentially administrative law (such as cases where the migrant is traveling without travel documents).

The negative impact this provision has on third-country nationals who wish to apply for asylum and gain access to the European Union is evident. The directive does attempt to address this issue by granting Member States the discretion not to impose sanctions for human smuggling by applying their national law and practice for cases where the aim of the behavior is to provide humanitarian assistance to the person concerned.[31] However, this provision is discretionary, so its value in redressing the balance set out by the broad definition and criminalization of human smuggling under EU law is questionable. By using the threat of criminal sanctions, the EU measures on human smuggling essentially aim at deterring individuals and organizations from coming into contact and assisting any third-country national wishing to enter the territory of EU Member States. As has been noted in an issue paper published by the Council of Europe Commissioner for Human Rights, "the message which is sent is that contact with foreigners can be risky as it may result in criminal charges."[32]

In addition to the criminalization provisions, the protocol includes a series of provisions on enforcement. A specific part of the protocol is devoted to smuggling of migrants by sea.[33] This contains detailed provisions on state cooperation to suppress the smuggling of migrants at

---

28. Council Directive 2002/90, 2002 O.J. (L 328) 19 (EC).

29. *See* art. 1(1)(a), *id.*

30. *Id.*; *accord* Council Directive 2002/946, art. 1(1), 2002 O.J. (L 328) 2 (EC) ("Each Member State shall take the measures necessary to ensure that the infringements defined in Articles 1 and 2 of Directive 2002/90/EC are punishable by effective, proportionate and dissuasive criminal penalties which may entail extradition.").

31. See Article 1(2), Council Directive 2002/90, *supra* note 28.

32. Elspeth Guild, *Criminalisation of Migration in Europe: Human Rights Implications*, COUNCIL OF EUR., COMM'R HUM. RTS. 39 (2009).

33. Smuggling Protocol, *supra* note 24, arts. 7-9.

sea, a number of which have been inspired by similar provisions on enforcement included in the UN Narcotics Convention.[34] Of particular importance is a provision allowing states to board and search vessels suspected of being engaged in human smuggling and are without nationality[35]—with the aim presumably being to cover smaller vessels carrying migrants such as the *cayucos* and the *pateras*.[36] This provision has formed the basis of quite extensive EU rules allowing for extensive enforcement measures at sea.[37] According to the rules for sea border operations coordinated by the European Border Agency, enforcement measures (which include both boarding and searching the ship and seizing the ship and apprehending persons on board) will be taken "if the suspicions that the ship is without nationality prove to be founded and that there are reasonable grounds to suspect that the ship is engaged in the smuggling of migrants by sea" in accordance with the Protocol Against Smuggling.[38] Part III of the protocol on "prevention, cooperation and other measures" includes an extensive set of further enforcement provisions including provisions on information, on border measures, on travel documents, and on return.[39] The detail of these provisions and the focus on enforcement do justice to Hathaway's claim that the treatment of human smuggling in a convention on organized crime serves to trigger the globalization of border control, with the powers and reach of the state being substantially extended.

B. Immigration Control as Counterterrorism

September 11, 2001 has been a watershed moment for the securitization of immigration control. The immediate U.S. response—

---

34. *See* DOUGLAS GUILFOYLE, SHIPPING INTERDICTION AND THE LAW OF THE SEA, 184-85 (2009); MCCLEAN, *supra* note 3, at 399-414.

35. According to Article 8(7) of the Smuggling Protocol,

> [a] State Party that has reasonable grounds to suspect that a vessel is engaged in the smuggling of migrants by sea and is without nationality or may be assimilated to a vessel without nationality may board and search this vessel. If evidence confirming the suspicion is found, that State Party shall take appropriate measures in accordance with relevant domestic and international law.

Smuggling Protocol, *supra* note 24.

36. Article 3(d) of the Smuggling Protocol defines a "vessel" broadly as "any type of water craft, including non-displacement craft and seaplanes, used or capable of being used as a means of transportation on water, except a warship, naval auxiliary or other vessel owned or operated by a Government and used, for the time being, only on government non-commercial service." *Id.*

37. Council Decision 2010/252, 2010 O.J. (L 111) 20 (EU).

38. See annex I, 2.5.2.5., *id.* at 23.

39. Smuggling Protocol, *supra* note 24, arts. 10-18.

which was heavily influenced by the manner in which the 9/11 attacks occurred—has led to the development of a remarkable transatlantic convergence regarding border security. The main elements of this securitized model of immigration control are as follows: immigration checks and controls do not serve only immigration but also security purposes—"it is all about security"; there is an emphasis on preventing movement, and thus a shift from controls at the physical border to extraterritorial immigration controls aiming to screen those planning to travel in advance of traveling anywhere in the globe; and this preventative approach is based on risk assessment and aims to identify "dangerous" individuals in advance. In this light, there is a shift from immigration control in a narrow sense to the control of mobility more broadly: it is not only third-country nationals wishing to enter the territory who are monitored, but all travelers and passengers. In this process, there is a widening of surveillance, with a wide range of personal data being collected for the purposes of securitized immigration control and a wide range of government agencies (and not only immigration agencies) having access to such data, as well as a deepening of surveillance (via the collection of extremely sensitive categories of personal data, including biometrics). The securitization of immigration control in this manner has served to strengthen the state by leading to a proliferation of state power. At the same time, it poses significant challenges to fundamental rights, in particular nondiscrimination, privacy, and data protection. By focusing on the United States and the European Union, the following Sections will cast light on the emergence of a transatlantic convergence on border security in a globalized world.

1. Immigration Control and Security in U.S. Law

The manner in which the 9/11 attacks took place signaled an emphasis on border security, and prompted discussions on the issue of entry to the United States of those who could execute such attacks. The 9/11 Commission Report devoted a section on "terrorist travel."[40] In this context, the report stressed the shortcomings of the pre-9/11 U.S. system, asserting that "targeting travel is at least as powerful a weapon against terrorists as targeting their money," and recommended that the United States "should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist

40. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 383-85 (2004) [hereinafter 9/11 COMMISSION REPORT].

travel facilitators, and constrain terrorist mobility."[41] This approach was also reflected in the U.S. strategy for "homeland security." The latter, put forward by the Bush Administration in 2002, included a whole chapter on "border and transportation security," and another on information sharing for homeland security. Great emphasis was placed on the widening and deepening of information collection and sharing (including of biometrics) from a variety of sources.[42] It is indicative that the wording of both the chapters on border security and information sharing converges in this respect. The strategy calls for the establishment of a "border of the future" (smart borders)[43] and of a "system of systems" which will provide "the right information to the right people at all times."[44]

This strategy was translated into a series of legislative and executive measures aiming, on the one hand, at monitoring the movement of passengers into and through the United States (by the establishment of prescreening systems) and, on the other, at promoting interagency cooperation and the interoperability of databases with regard to "homeland" and "border" security. The latter appears as a term in the title of the 2002 Enhanced Border Security and Visa Entry Reform Act, which placed emphasis on another element of "border security" linked to both aspects described above: the identification of individuals wishing to enter the United States, in particular, by introducing requirements that travel documents contain machine-readable data, such as fingerprints. Subsequent measures expressly required the taking of biometric identifiers from individuals entering the United States, emphasizing again the prevention element in border control.[45]

The emphasis of U.S. law on preventative immigration control via the use of biometric identification for third-country nationals is evident in the US-VISIT program, a key component of the new U.S. system of

---

41. *Id.* at 385.

42. OFFICE FOR HOMELAND SECURITY, NATIONAL STRATEGY FOR HOMELAND SECURITY 22 (2002).

43. *Id.* at 22.

44. *Id.* at 56; *see also* Reg Whitaker, *A Faustian Bargain? America and the Dream of Total Information Awareness*, *in* THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY 14, 155-68 (Kevin D. Haggerty & Richard V. Ericson eds., 2006) (discussing the now-aborted scheme by the Bush Administration for the establishment of a Total Information Awareness [TIA] system).

45. For a general analysis of "border security" in the U.S. context, see Valsamis Mitsilegas, *Borders, Security and Transatlantic Cooperation in the Twenty-First Century: Identity and Privacy in an Era of Globalized Surveillance*, *in* IMMIGRATION POLICY AND SECURITY 148, 148-60 (Terri E. Givens et al. eds., 2009) [hereinafter *Borders, Security and Transatlantic Cooperation in the Twenty-First Century*].

extraterritorial immigration control aimed at "border security." Entitled "The U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program," it has been designed to use biometric and biographic information to control and monitor the preentry, entry, status and exit of foreign visitors and is deemed to be "intended to enhance the security of U.S. citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the U.S. immigration system, and protect the privacy of visitors to the United States."[46] As the Department of Homeland Security (DHS) noted, it is "*part of a continuum of security measures* that begins overseas, when a person applies for a visa to travel to the United States, and continues on through entry and exit at U.S. air and seaports and, eventually, at land border crossings" (emphasis added).[47] The features of US-VISIT were designed to include reliance on biometrics, integration of arrival and departure data on foreign nationals (including commercial carrier passenger manifests), and integration with other law enforcement and security systems.[48] The system initially applied to select nationalities, but, notwithstanding privacy concerns,[49] has now been rolled out for all foreign visitors.[50] In this context, it has been noted

> that the US VISIT Program now applies to *all* foreign bodies, not merely those that have been identified as potentially "risky" or even "guilty" . . . is all the more significant. In the new border protection practices, each visitor to the US features as a foreign body tagged with an individual calculated level of risk.[51]

These concerns are intensified in the light of the development of a new US-VISIT:

---

46. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-316, HOMELAND SECURITY: STRATEGIC SOLUTION FOR US-VISIT PROGRAM NEEDS TO BE BETTER DEFINED, JUSTIFIED AND COORDINATED 1 (2008) [hereinafter STRATEGIC SOLUTION FOR US-VISIT PROGRAM NEEDS TO BE BETTER].

47. Colin J. Bennett, *What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11*, *in* GLOBAL SURVEILLANCE AND POLICING: BORDERS, SECURITY, IDENTITY 113, 127 (Elia Zureik & Mark B. Salter eds., 2005).

48. *See* U.S. DEP'T OF HOMELAND SEC., US-VISIT PROGRAM, INCREMENT 1: PRIVACY IMPACT ASSESSMENT (2003).

49. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-202, HOMELAND SECURITY: SOME PROGRESS MADE BUT MANY CHALLENGES REMAIN ON U.S. VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY PROGRAM (2005).

50. *See* Mark B. Salter, *Passports, Mobility, and Security: How Smart Can the Border Be?*, 5 INT'L STUD. PERSP. 71, 78 (2004).

51. Charlotte Epstein, *Embodying Risk: Using Biometrics to Protect the Borders*, *in* RISK AND THE WAR ON TERROR 178, 185 (Louise Amoore & Marieke de Goede eds., 2008).

> capability known as "Unique Identity," which is to establish a single identity for all individuals who interact with any immigration and border management organisation by capturing the individual's biometrics, including 10 fingerprints and a digital image, *at the earliest possible interaction* (emphasis added).[52]

The ambition of U.S. law and policy has been to extend the net of securitized immigration control globally. Not only has U.S. law required biometrics from third-country nationals wishing to enter the United States, but it has moved further to require third *states* to introduce biometric identity documents to their citizens if they wished to receive preferential treatment from the United States as part of the U.S. Visa Waiver Program. Under the latter, "the Secretary of Homeland Security, in consultation with the Secretary of State, may waive the 'B' nonimmigrant visa requirement for aliens traveling from certain countries as temporary visitors for business or pleasure."[53] The biometrics requirement to the existing Visa Waiver Program introduced by the Enhanced Border Security and Visa Entry Reform Act of 2002[54] mandated that, by October 26, 2004, the government of each Visa Waiver Program country needed to certify that it has established a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate a biometric identifier. The Intelligence Reform and Terrorism Prevention Act of 2004[55] "added the requirement that by October 26, 2006, as a condition of being in the VWP [Visa Waiver Program], each country must certify that it is developing a program to issue tamper-resistant, machine-readable visa documents that incorporate biometric identifiers which are verifiable at the country's port of entry."[56]

Visa facilitation, on the condition of the deepening of surveillance via the introduction of biometrics, has thus become a U.S. foreign policy tool aiming to create a global intensification of surveillance. As will be seen below, the U.S. requirements have had significant impact on the development of the EU policy in the field, with the related issue of visa reciprocity also arising.[57] At the same time, the collection of biometric

---

52. STRATEGIC SOLUTION FOR US-VISIT PROGRAM NEEDS TO BE BETTER, *supra* note 46, at 2.

53. ALLISON SISKIN, CONG. RESEARCH SERV., RL32221, VISA WAIVER PROGRAM (2004), http://www.fas.org/sgp/crs/homesec/RL32221.pdf.

54. Pub. L. No. 107-173, 116 Stat. 543 (2002).

55. Pub. L. No. 108-458, 118 Stat. 3638 (2004).

56. SISKIN, *supra* note 53, at 19-20.

57. The European Commission reports regularly on visa reciprocity. For the latest Report at the time of writing, see *Report from the Commission to the European Parliament*

data under the Visa Waiver Program has been linked with the development by the United States of an automated entry-exit system. The 9/11 Commission Recommendations Act[58] mandated that "the Secretary of [the DHS], in consultation with the Secretary of State . . . develop and implement a[n] . . . electronic travel authorization system" (ESTA), through which each alien electronically provides, in advance of travel, the biographical information necessary to determine whether the alien is eligible to travel to the United States and enter under the VWP. It also required the Secretary of the DHS "to establish an exit system that records the departure of every alien who entered under the VWP and left the United States by air."[59] This system is not yet fully in place. However, according to the DHS:

> [o]nce ESTA is mandatory, all nationals or citizens of Visa Waiver Program (VWP) countries who plan to travel to the United States for temporary business or pleasure will require an approved ESTA prior to boarding a carrier to travel by air or sea to the United States under the VWP.[60]

In addition to requiring biometrics from third-country nationals and using biometrics as a foreign policy tool to export U.S. requirements at the global level, the next step towards the intensification of surveillance has been the U.S. legislature's move to internalize this security paradigm by introducing a requirement for the inclusion of biometrics in U.S. passports. According to the State Department, since 2007, only e-passports are issued—they contain a computer chip with a digital photograph, in addition to the data visually displayed on the photo page of the passport.[61] As Ayelet Shachar has noted writing on U.S. immigration law, "the increased post 9/11 regulation of the non-citizen has become a precursor for adopting unprecedented immigration control measures affecting the quintessential member: the American citizen."[62] This is only one of a number of instances where, as will be seen below,

---

and the Council on Certain Third Countries' Maintenance of Visa Requirements in Breach of the Principle of Reciprocity, COM (2010) 620 final (May 11, 2010).

58. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 711 (2007).

59. SISKIN, *supra* note 53, at 21.

60. *Fact Sheet: Electronic System for Travel Authorization (ESTA)*, HOMELAND SEC. (June 3, 2008), http://www.dhs.gov/xnews/releases/pr_1212498415724.shtm.

61. *The U.S. Electronic Passport*, TRAVEL.STATE.GOV, http://travel.state.gov/passport/passport_2498.html (last visited Jan. 10, 2012).

62. Ayelet Shachar, *The Shifting Border of Immigration Regulation*, 3 STAN. J. C.R. & C.L. 165, 183 (2007).

the link between security and the generalized monitoring of movement has led to the expansion of control from the foreigner to the citizen.

2. Immigration Control and Security in EU Law

The link between immigration control and security was clearly articulated in the five-year Program for EU Justice and Home Affairs law and policy agreed by the European Council in 2004 (the Hague Program). According to the latter,

> The management of migration flows, including the fight against illegal immigration should be strengthened by establishing *a continuum of security measures* that effectively links visa application procedures and entry and exit procedures at external border crossings. Such measures are also of importance for the prevention and control of crime, in particular terrorism. In order to achieve this, a coherent approach and harmonised solutions in the EU on biometric identifiers and data are necessary (emphasis added).[63]

This is a clear reflection of the concept of "border security" as developed in the United States, with controls on immigration and movement being prioritized and linked with counterterrorism. In this manner, the wording of the Hague Program represents the creation of what scholars have already identified in the 1990s as the so-called "(in)security continuum," which consists of linking, in law and policy discourse, the disparate aims of controlling immigration on the one hand and fighting "security threats" such as crime and terrorism on the other.[64] Intervention *before* entry, prevention and the collection and exchange of personal data (including biometrics) are all key in this context.

As with the United States, the renewal of such an (in)security continuum emerged at the EU level following attacks in Madrid, a European capital. In the Declaration on Combating Terrorism of March 25, 2004, following these attacks, the European Council linked the monitoring of the movement of people with counterterrorism by stressing that "[i]mproved border controls and document security play an important role in combating terrorism."[65] There were two elements

---

63. The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, 2005 O.J. (C 53) 1, 7.

64. *See* DIDIER BIGO, POLICES EN RÉSEAUX: L'EXPÉRIENCE EUROPÉENNE (1996).

65. Declaration on Combating Terrorism, Brussels European Council 7 (Mar. 25, 2004), *available at* http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.

in this approach: the inclusion of biometrics in EU visas and passports, which were to be prioritized and relevant measures adopted by the end of 2004, and the enhancement of the interoperability between EU databases and the creation of "synergies" between existing and future information systems (such as the Schengen Information System II, the Visa Information System and Eurodac) in order to exploit their added value within their respective legal and technical frameworks in the prevention and fight against terrorism.[66] Unlike the United States, where, as seen above, the introduction of biometrics in identity documents of third-country nationals preceded the introduction of biometrics in the passports of U.S. citizens, in the European Union moves to include biometrics were pursued simultaneously under a banner of security.

Political pressure towards the insertion of biometrics into identity and travel documents in EU Member States led to the adoption, in December 2004, of a Regulation introducing biometric identifiers (in the form of facial images and fingerprints) in EU passports.[67] The Commission justified the introduction of biometrics in EU passports as being necessary to meet U.S. requirements on document security and thus prolong the U.S. Visa Waiver Program that a number of EU Member States enjoy and extend it to EU Member States that are not members.[68] The legal basis of the Regulation was the then Article 62(2)(a) of the EC Treaty on External Border Controls, although the Regulation was deemed by Member States such as the United Kingdom to be a security measure.[69] The Regulation was finally adopted notwithstanding serious legality objections related to the appropriateness of a Title IV (immigration) legal basis in regards to measures affecting EU citizens and doubts over the existence of Community competence to adopt binding legislation on the content of identity documents.[70] Notwithstanding these concerns, negotiations on the measure went ahead. A second biometric identifier—fingerprints—was added and the biometrics regulation was adopted swiftly thereafter

66. *See* Valsamis Mitsilegas, *Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme*, 60 CULTURES ET CONFLITS, Hiver [Winter] 2005, at 185 (Fr.), *available at* http://conflits.revues.org/index1829.html.

67. Council Regulation 2252/2004, 2004 O.J. (L 385) 1 (EC).

68. Mitsilegas, *supra* note 66, at 172.

69. *See* Letter from Caroline Flint MP, Parliamentary Under Secretary of State, Home Office to Lord Julian Grenfell, Chairman (July 15, 2004), http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/16/16208.htm (stating that "[o]ur view is that the current proposal is first and foremost a security measure").

70. Mitsilegas, *supra* note 66.

in December 2004.[71] EU immigration law was thus used to adopt a measure deemed by some as primarily concerned with security and applicable not to third-country nationals, but to EU citizens. As I noted back in 2005, in this manner and under a questionable legal basis[72] EU Member States unanimously adopted a measure facilitating the surveillance not of foreigners but of their own citizens.[73]

Biometrics are also playing a central role in EU immigration control, in particular via their use in the EU Visa Information System (VIS).[74] The development of the VIS is a clear example of the trend to securitize migration and blur the boundary between immigration and police databases. The Council on Justice and Home Affairs adopted detailed conclusions on the development of VIS in February 2004, stating clearly that one of the purposes of the system would be to "contribute towards improving the administration of the common visa policy and towards internal security and combating terrorism."[75] It also

---

71. The need for the swift adoption of the proposal has also been justified on the grounds that the United States would abandon its visa-waiver program with those EU Member States that had not introduced biometrics in their passports by a certain date. The EU has managed to obtain an extension to the U.S. deadline for the insertion of biometrics, but this new U.S. deadline will not be met and it is unlikely to be extended by the United States. *See US Says Deadline for Biometric "Passports" Cannot be Extended*, STATEWATCH, http://www.statewatch.org/ news/2005/apr/01eu-us-passports.htm (last visited Jan. 19, 2012) (reproducing the March 25, 2005 letter from the Chairman of the U.S. House Judiciary Committee to the Commission and the Council).

72. It is noteworthy in this context that the Lisbon Treaty, in force since December 1, 2009, now includes an express legal basis that may enable the adoption of EU measures on "passports, identity cards, residence permits or any other such document." Consolidated Version of the Treaty on the Functioning of the European Union art. 77(3), Sept. 30, 2010, 2010 O.J. (C 83) 47 [hereinafter TFEU]. Although this power is linked with the facilitation of free movement and residence rights for EU citizens, Article 77(3) is included in the part of the Treaty dealing with policies on border checks, immigration, and asylum. See Chapter 2 of Title V on the Area of Freedom, Security and Justice*, id.* at 73.

73. *See* Mitsilegas, *supra* note 66. For an articulation of this argument in an English-language publication, see Valsamis Mitsilegas, *Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance*, *in* WHOSE FREEDOM, SECURITY AND JUSTICE? 359 (Anneliese Baldaccini et al. eds., 2007) [hereinafter *Border Security in the European Union*].

74. On the use of biometrics in EU databases, with emphasis on the immigration databases, see Anneliese Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 10 EUR. J. MIGRATION & L. 31 (2008). *See also* Evelien Brouwer, *The Use of Biometrics in EU Databases and Identity Documents: Keeping Track of Foreigners' Movements and Rights*, *in* ARE YOU WHO YOU SAY YOU ARE? THE EU AND BIOMETRIC BORDERS 45, 48-50 (Juliet Lodge ed., 2007).

75. Press Release, Justice and Home Affairs, Council of the European Union, at 16 (Feb. 19, 2004), *available at* http://www.consilium.europa.eu/press/press-releases/latest-pressreleases/newsroomrelated.aspx?bid=86&grp=6802&lang=en&id=.

called for access to VIS to be granted to border guards and "other national authorities to be authorised by each Member State such as police departments, immigration departments and services responsible for internal security."[76] In June 2004, the Council adopted a Decision forming the legal basis for the establishment of VIS[77] and negotiations began to define its purpose and functions and formulate rules on access and exchange of data. The Commission subsequently tabled a draft Regulation aiming to take VIS further by defining its aims and rules on data access and exchange.[78] The Council on Justice and Home Affairs of 24 February 2005 called for access to VIS to be given to national authorities responsible for "internal security" when exercising their powers in "investigating, preventing and detecting criminal offences, including terrorist acts . . . [or] threats" and invited the Commission to present a separate, third-pillar (national security) proposal to this end.[79] The Commission tabled such a proposal in November 2005.[80] The two texts were linked and thus negotiated in parallel (codecision was formally required for the first-pillar regulation, while for the third-pillar decision the European Parliament had a consultation role).[81] Agreement on both proposals was confirmed at the Council on Justice and Home Affairs of 12-13 June 2007,[82] and they were published in the Official Journal with considerable delay in August 2008.[83] Reflecting the logic of the Conclusions of the 2005 Council on Justice and Home Affairs, the VIS Regulation expressly states that one of the purposes of the Visa Information System is to "contribute to the prevention of threats to

76. *Id*. at 19.

77. Council Decision 2004/512, 2004 O.J. (L 213) 5 (EC).

78. *Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System (VIS) and the Exchange of Data Between Member States on Short Stay-Visas*, at 2, COM (2004) 835 final (Dec. 28, 2004).

79. Press Release, Council of the European Union, Council Meeting on Justice and Home Affairs, at 16 (Feb. 24, 2005), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/83980.pdf.

80. *Proposal for a Council Decision Concerning Access for Consultation of the Visa Information System (VIS) by the Authorities of Member States Responsible for Internal Security and by Europol for the Purpose of the Prevention, Detection and Investigation of Terrorist Offenses and of Other Serious Criminal Offenses*, COM (2005) 600 final (Nov. 24, 2005).

81. For details, see Valsamis Mitsilegas, *Human Rights, Terrorism and the Quest for "Border Security"*, *in* INDIVIDUAL GUARANTEES IN THE EUROPEAN JUDICIAL AREA IN CRIMINAL MATTERS 85 (Marco Pederazzi et al. eds., 2011).

82. Press Release, Council of the European Union, Council Meeting on Justice and Home Affairs (June 12-13, 2007).

83. Council Regulation 767/2008, 2008 O.J. (L 218) 60 (EC); Council Decision 2008/633, 2008 O.J. (L 218) 129 (EU).

internal security of . . . the Member States."[84] The Regulation also contains a bridging clause to the third-pillar decision that gives Europol access to VIS by Europol "within the limits of its mandate and when necessary for the performance of its tasks," and gives the relevant national authorities access to VIS "if there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences."[85] The terms of access of internal security authorities and Europol to the VIS are set out in detail in the third-pillar decision.[86] The VIS will also include biometric data.[87] Some detail with regard to the introduction of biometrics to EU visas can be found in a recently adopted Regulation amending the Common Consular Instructions.[88] The link between the collection and use of biometrics on the one hand and the identification of the visa holder on the other is made clear already in the Preamble to the Regulation.[89] In a clear convergence with the U.S. system, the Regulation calls upon Member States to collect biometric identifiers comprising the facial image and ten fingerprints from the applicant.[90]

Another example of the new generalized surveillance based on monitoring movement, applying to both EU and third-country nationals, is the collection of sensitive personal data. The new move by the European Commission to propose the creation of an entry-exit system at the external borders of the European Union, coupled with facilitation of border crossings for bona fide travelers and the creation of an electronic travel authorization system.[91] The entry-exit system would be a new database, applying to third-country nationals admitted for a short stay; bona fide travelers would be "low risk" third-country nationals, but also EU citizens—both would cross external borders via "automated gates." The Electronic Travel Authorization System (ETAS) would apply to third-country nationals not subject to a visa requirement who would be required to make an electronic application in advance of traveling.

---

84. The Regulation also enables the recording of biometric data into VIS in Article 5(1). Council Regulation 767/2008, *supra* note 83, at 64-65.

85. *Id*. at 63.

86. In particular, see Articles 5-7, *id*. at 64-65.

87. *Id.* at 61, 64-66.

88. *See* Regulation 390/2009, 2009 O.J. (L 131) 1, 1 (EC).

89. "The integration of biometric identifiers in the VIS is an important step towards the use of new elements, which establish a more reliable link between the visa holder and the passport in order to avoid the use of false identities." *Id.*

90. *Id.* at 4. For exceptions, see *id.* at 5.

91. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, at 5, COM (2008) 69 final (Feb. 13, 2008).

These proposals are similar to the U.S. model of border security, and are reminiscent of the recommendation by the 9/11 Commission to "balance" the collection of biometrics of U.S. citizens with measures aimed at speeding "known travelers." Both interoperability and the use of biometrics are central to these proposals, in particular to the proposals for the establishment of a system of border crossings via automated gates. The Commission notes that:

> In the run-up to *full introduction of biometric passports*, the current legal framework allows for schemes based on voluntary enrolment to be deployed by Member States, under the condition that the criteria for enrolment correspond to those for minimum checks at the borders *and that the schemes are open for all persons enjoying the Community right to free movement*. Such schemes should be *interoperable* within the EU, based on common technical standards, which should be defined to support the *widespread and coherent use of automated border control systems* (emphasis added).[92]

However, the added value of a new database on an entry-exit system for third-country nationals is not evident, especially in light of the recent establishment of the VIS. Moreover and along with the evident proportionality concerns, there have been serious legality concerns with regard to the extension of legislation on the management of the EU external border to EU citizens.[93] However, the momentum for the establishment of an entry-exit system along these lines is currently high. The European Council invited the Commission to present proposals for an entry-exit and registered traveler system by the beginning of 2010,[94] and agreed in the European Pact on Immigration and Asylum (endorsed by the European Council in October 2008) to deploy "modern technological means to ensure that systems are interoperable" and stated that from 2012 the focus should be "on establishing electronic recording of entry and exit, together with a fast-track procedure for European citizens and other travellers."[95] The

92. *Id*. at 7.

93. For further details on this point, see Valsamis Mitsilegas, *The Borders Paradox: The Surveillance of Movement in a Union Without Internal Frontiers*, *in* A RIGHT TO INCLUSION AND EXCLUSION? NORMATIVE FAULT LINES OF THE EU'S AREA OF FREEDOM, SECURITY AND JUSTICE 33 (Hans Lindahl ed., 2009) [hereinafter *The Borders Paradox*].

94. Presidency Conclusions, Brussels European Council, ¶ 10 (June 20, 2008).

95. Memorandum, European Pact on Immigration and Asylum to the Council of the EU, pt. 3(e), at 10 (Sep. 24, 2008).

political prioritization of the establishment of an entry-exit system has been reaffirmed in the Stockholm Program, the five-year plan succeeding the Hague Program, which emphasized once more the link between security, mobility, and technology.[96]

The opening sentence of the Stockholm Program chapter entitled "access to Europe in a globalised world" states that "[t]he Union must continue to facilitate legal access to the territory of its Member States while in parallel taking measures to counteract illegal immigration *and cross-border crime* and maintaining a high level of security" (emphasis added).[97] Noting that the possibilities of "new and interoperable technologies hold great potential for rendering border management more efficient as well as more secure but should not lead to discrimination or unequal treatment of passengers," the European Council invited the Commission to present proposals for an entry-exit system alongside a fast track registered traveler program with a view to such a system becoming operational as soon as possible; to prepare a study on the possibility and usefulness of developing a European system of travel authorization and, where appropriate, to make the necessary proposals; and to continue to examine the issue of automated border controls and other issues connected to rendering border management more efficient.[98] The Commission Action Plan on the implementation of the Stockholm Program envisaged the tabling of legislative proposals setting up an Entry Exit System and a Registered Traveller Program in 2011.[99] No such proposals have been tabled yet at the time of writing, but the development of EU border control along these lines is clearly a live issue.[100]

By establishing an entry-exit system—which is remarkably similar to developments in U.S. law analyzed above—the EU introduces a system of surveillance of movement based on automaticity, interoperability, and the collection and consultation of sensitive personal data, such as biometrics. As I have noted elsewhere, merging the logic of risk prevention with the logic of border security, this model has far-reaching consequences for the protection of fundamental rights

96. The Stockholm Programme, 2010 O.J. (C 115) 1, 1 (EC).

97. *Id.* at 26.

98. *Id.* at 27.

99. *Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Programme*, at 44, COM (2010) 171 final (Apr. 20, 2010).

100. A document setting out the provisional agendas for Council meetings during the Polish Presidency (second semester of 2011) indicates the possibility of the Commission tabling a (nonlegally binding) Communication on Smart Borders (Entry-Exit System and Registered Traveller System) during the Presidency. *See* Memorandum, Provisional Agendas for Council Meetings, at 30 (June 30, 2011).

and the relationship between the individual and the state.[101] Movement is monitored on the basis of profiling and individual, subjective assessments of each traveler. Both third-country nationals and EU citizens can be deemed "suspects" under these assessments, and their freedom of movement curtailed accordingly. The introduction of the concept of "bona fide" traveler is extremely worrying in this context. As the European Data Protection Supervisor has noted in his preliminary comments on the Commission proposals:

> The underlying assumption in the communications (especially in the entry/exit proposal) is worrying: all travellers are put under surveillance and are considered a priori as potential law breakers. For instance in the Registered Travellers system, only the travellers taking specific steps, through ad hoc registration and provision of detailed personal information, will be considered "bona fide" travellers. The vast amount of travellers, who do not travel frequently enough to undergo such a registration, are thus, by implication, de facto in the "mala fide" category of those suspected of intentions of overstay.[102]

II. GLOBALIZATION, IMMIGRATION CONTROL, AND DELEGATION

Another way by which state power has proliferated in an era of globalized immigration control has been via the delegation of powers and tasks related to such control. This article has already mentioned how the securitization of immigration control has been promoted via the reliance of the state on technology (via the creation and interconnection of a series of databases establishing wide-ranging systems of surveillance of movement). This Section will expand on the recourse of the state to technology as a way of delegating power. It will also focus on two other forms of delegation that are relevant to globalized immigration control: the establishment and use of government agencies to control movement, especially in the context of securitized immigration control; and the recourse of the state to the private sector to assist with monitoring global flows of people. In terms of the use of agencies, the (in)security continuum linking immigration and security has been expressed via border control powers being assigned to security

101. *See The Borders Paradox*, *supra* note 93.

102. *Preliminary Comments of the European Data Protection Supervisor*, at 5-6 (Mar. 3, 2008), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

agencies (as in the case of the United States) or immigration agencies being entrusted with security responsibilities (as in the case of the European Union and the European Borders Agency-FRONTEX). There is further transatlantic convergence in enabling maximum interagency cooperation between immigration agencies and other law enforcement agencies. In terms of the privatization of immigration control, the transatlantic convergence on the use of the private sector (especially carriers) to cooperate with the state has also now been translated, to some extent, in global instruments such as the Palermo Convention. This Section will analyze this three-pronged delegation process in greater detail and attempt to highlight how such delegation expands the powers of the state while at the same time creates gaps in state responsibility and accountability for immigration control.

A. The Privatization of Immigration Control

In one of his many important writings on globalization, Fred Aman explains that the trend toward privatization now involves services, not regulation, and private parties now perform the functions involved: "[I]n effect, the government delegates responsibility for services to private actors."[103] This statement is increasingly applicable in the field of immigration law. Issues surrounding delegation from the state to the private sector in the context of carriers' liability have been analyzed extensively in the literature,[104] but also arise in the context of the extension of the privatization of immigration control to include actors such as employers. This Section will examine both of these instances of privatization and attempt to demonstrate that, rather than asking the private sector *to replace* state functions in the field, privatization in the field of immigration control means that the state delegates *additional* tasks (such as the examination and assessment of identity documents) to the private sector. In this manner, the involvement of the private sector serves to add an extra layer of immigration control, on top of the exercise of the expanding state powers in the field.

---

103. Alfred C. Aman, Jr., *Globalization, Democracy, and the Need for a New Administrative Law*, 10 IND. J. GLOBAL LEGAL STUD. 125, 128-29 (2003).

104. *See, e.g.*, Virginie Guiraudon, *De-Nationalizing Control: Analyzing State Responses to Constraints on Migration Control*, *in* CONTROLLING A NEW MIGRATION WORLD 29 (Virginie Guiraudon & Christian Joppke eds., 2001). *See, e.g.*, Gallya Lahav, *Immigration and the State: The Devolution and Privatisation of Immigration Control in the EU*, 24 J. ETHNIC MIGRATION STUD. 675 (1998); Frances Nicholson, *Implementation of the Immigration (Carriers' Liability) Act 1987: Privatising Immigration Functions at the Expenses of International Obligations?*, 46 INT'L & COMP. L. Q. 586 (1997) (providing U.K. context).

There has been a long tradition in Europe of using carriers as an extra layer of immigration control. Both the United Kingdom and the Schengen countries introduced carriers' liability legislation in the late 1980s, with the Schengen carriers' liability requirements incorporated in an expanded version in EU law in 2001.[105] The Carriers liability Directive[106] takes forward the provisions of Article 26 of the Schengen Implementing Convention and imposes two main duties on carriers: "to take all the necessary measures to ensure that an alien carried out by air or sea is in possession of the travel documents required for entry into the territories"[107] and to assume responsibility for third-country nationals who have been refused entry into the territory, including their return or assuming the cost of their return.[108] If carriers transport third-country nationals who do not possess the necessary travel documents, they face a series of financial sanctions.[109] In this manner, carriers are asked to provide an extra layer of immigration control in identifying passengers and checking travel documents. EU law also privatizes immigration control at the level of enforcement, by requiring carriers to take charge or bear the cost of the return of third-country nationals whom they have transported into EU territory.

The privatization of immigration control via the imposition of duties on carriers has expanded the scope of the duties, as well as the global reach of those duties. As will be seen in detail later in the Article, carriers are now further required to collect and transmit passenger data to state authorities.[110] As far as the global reach of privatization, it is noteworthy that both the trafficking and smuggling Protocols of the Palermo Convention include specific provisions on carriers' liability. According to the provisions on border measures, parties must "adopt legislative or other appropriate measures to prevent, to the extent possible, means of transport operated by commercial carriers from being used in the commission of" human smuggling or trafficking.

> [W]here appropriate, and without prejudice to applicable international conventions such measures shall include establishing the obligation of commercial carriers,

105. *See* Nicholson, *supra* note 104 (discussing the United Kingdom); MITSILEGAS ET AL., *supra* note 2, at 109-11.

106. Council Directive 2001/51, 2001 O.J. (L 187) 45, 45 (EC).

107. Convention Implementing the Schengen Agreement, art. 26(1)(b), 1990 O.J. (L 239) 19.

108. *See* Council Directive 2001/51, *supra* note 106, at 46; Convention Implementing the Schengen Agreement, *supra* note 107, art. 26(1)(a).

109. *See* Council Directive 2001/51, *supra* note 106, art. 4-5; Convention Implementing the Schengen Agreement, *supra* note 107, art. 26(2).

110. *See infra* Part V.

> including any transportation company or the owner or operator of any means of transport, to ascertain that all passengers are in possession of the travel documents required for entry into the receiving State.[111]

The Protocols call for the imposition of sanctions in cases of the carriers' violation of the duty to ascertain whether passengers are in possession of the required travel documents.[112] They also call upon states to consider taking measures that permit the denial of entry or revocation of visas of persons implicated in the commission of trafficking or smuggling.[113] Prevention of movement is thus key to the carriers' provisions of the Palermo Protocols, with the latter focusing expressly on carriers' duties to check passengers in order to ascertain the validity of their travel documents (with the implicit consequence that not possessing the required travel documents will result in not being accepted for travel by the carrier).

The preventative aspect of the privatization of immigration control via the imposition of duties on carriers has been increasingly coupled with calls upon the private sector to cooperate with the state regarding the enforcement of immigration law within the territory. This ex post immigration control, occurring after the entry into the territory, is evident in the case of imposition of duties on private companies in their capacity as employers. The latter are increasingly required to assist immigration control by checking the validity of the documents of those to be employed in their organization. Involving employers in immigration control has been a common policy on both sides of the Atlantic. In the United States, the E-Verify System allows employers to check, on a voluntary basis, work eligibility by verifying workers' names and identity data against federal databases.[114] E-Verify was launched in 2007,[115] following successive pilot projects implementing the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.[116] The

---

111. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime, G.A. Res. 55/25, annex II, U.N. GAOR, 55th Sess., Supp. No. 49, at 60, U.N. Doc. A/55/383, at art. 11 (Nov. 15, 2000); Protocol Against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention Against Transnational Organized Crime, art. 11, G.A. Res. 25, annex II, U.N. GAOR, 55th Sess., Supp. No. 49, at 60, U.N. Doc. A/55/383 (Nov. 15, 2000).

112. See Articles 11(4), contained in both Protocols, *id.*

113. See Articles 11(5), *id.*

114. Marc R. Rosenblum, *E-Verify: Strengths, Weaknesses, and Proposals for Reform*, 2011 MIGRATION POLICY INST. 1.

115. *Id.* at 2.

116. Pub. L. No. 104-208, 110 Stat. 3009-546 (2003).

system is widely applied but has been criticized "for high error rates and other adverse effects, and some have argued that to be effective it should be linked to a new biometric identity system."[117] The privatization of immigration control may thus lead to the widening and deepening of surveillance of both third-country nationals and U.S. citizens. Marc Rosenblum has noted that "[i]mplementing a national biometric ID system would require the US government to capture fingerprints (or some other biometric data) for 160 million US workers," adding that "[p]erhaps the most important question about a biometric card is whether Americans are ready to be fingerprinted as a precondition for eligibility to work."[118]

A less generalized but more far-reaching system as to the duties imposed and their enforcement has been established at the EU level. The recently adopted Directive on employers' sanctions[119] prohibits the employment of third-country nationals staying illegally.[120] Sanctions for the infringement of this prohibition are mainly financial,[121] but there are also alternatives, such as exclusion from public procurement.[122] The Directive also provides for the imposition of criminal penalties to employers if a series of aggravating circumstances occur.[123] The Directive imposes a series of identification, record-keeping, and reporting duties on employers. Employers must require that before taking up the employment a third-country national hold and present to the employer a valid residence permit or other authorization for his or her stay; "keep for at least the duration of the employment a copy or record of the residence permit or other authori[z]ation for stay available for possible inspection by the competent authorities of the Member States"; and "notify the competent authorities designated by Member States of the start of [the] employment of third-country nationals within a period laid down by each Member State."[124] If employers fulfill these obligations, they will not be held liable for an infringement of the prohibition of illegal employment unless the employers knew that the document was presented as a valid residence permit or another authorization for stay was a forgery.[125] EU law thus imposes extensive immigration enforcement duties on employers, including duties of cooperation with the state.

---

117. Rosenblum, *supra* note 114, at 1-2.
118. *Id.* at 13.
119. Council Directive 2009/52, 2009 O.J. (L 168) 24 (EC).
120. See Article 3(1), *id.* at 28.
121. See Articles 5-6, *id.* at 28-29.
122. See Article 7, *id.* at 29.
123. See Articles 9-10, *id.* at 30.
124. See Article 4(1), *id.* at 28.
125. See Article 4(3), *id.* at 28.

In addition to the extension of state power by imposing immigration control duties to the private sector, privatization enhances state power via the involvement of the private sector in developing state capabilities on immigration control. As has been noted by Gina Clayton, private companies are now increasingly involved in the process of issuing U.K. visas, with the line between private and state responsibility being at times difficult to draw.[126] In an era where immigration control is increasingly based on the use of technology, databases, and biometrics, private commercial interests are inextricably linked with state interests, with private companies involved in building new databases, automated gates, and biometric capabilities.[127] In this context, the state may rely on new policies in the field to boost economic activity, while commercially driven initiatives may be adopted as government policy without adequate scrutiny or justification.[128] The confluence of commercial and state interests in this context may lead to the depoliticization of immigration control, with the development of additional state capabilities in the field being viewed narrowly as a factor of economic growth or as a consequence of technological developments.[129]

Similar to the criminalization of the facilitation of unauthorized entry (or human smuggling) discussed above, the private sector is thus urged to pay particular attention when coming into contact with foreigners—even if such contact is in the normal course of ordinary commercial life. In addition to the prohibition and criminalization of contact with undesired foreigners, the privatization of immigration control signifies the imposition of specific duties on the private sector, in particular duties to identify passengers and check the validity of identity documents. The private sector is held responsible for dealing with individuals deemed not to be eligible under immigration law and is under a duty to detect such ineligibility and report it to the state. This

---

126. *See* Gina Clayton, *The UK and Extraterritorial Immigration Control: Entry Clearance and Juxtaposed Control*, *in* EXTRATERRITORIAL IMMIGRATION CONTROL: LEGAL CHALLENGES (Valsamis Mitsilegas & Bernard Ryan eds., 2010).

127. For the discussion of the issue of privatization in the development of the U.S. Homeland Security Strategy, see PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY: WHY PRIVATISATION OF GOVERNMENT FUNCTIONS THREATENS DEMOCRACY AND WHAT WE CAN DO ABOUT IT (2007).

128. *See generally* Valsamis Mitsilegas, *Extraterritorial Immigration Control in the 21st Century: The Individual and the State Transformed*, *in* EXTRATERRITORIAL IMMIGRATION CONTROL: LEGAL CHALLENGES 39, *supra* note 126 [hereinafter *Extraterritorial Immigration Control in the 21st Century*] (discussing the changes and growing securitization in extraterritorial immigration control exercised in the West post-9/11 and its consequences).

129. On the link between immigration control and technology see, *infra* Part III.C.

"responsibilization" strategy[130] mirrors the strategy to involve the private sector in cooperating with the state in the field of crime control and security governance.[131] In the field of immigration control, responsibilization via privatization leads to the strengthening of the state by introducing additional layers of checks on third-country nationals.

While extending immigration control and enhancing state power, the responsibilization of the private sector weakens the position of the affected individuals in a number of ways: (1) it challenges the right to asylum and the respect for the principle of nonrefoulement by potentially preventing the individual's access to the territory for the purposes of lodging an asylum claim; (2) it challenges the principle of nondiscrimination by requiring the private sector to evaluate third-country nationals on the basis of risk assessment; and (3) as seen above in the Section on the collection of biometrics and as will be seen further below in the part on the requirements for the transmission of Passenger Name Data, it challenges the right to private life and data protection via the collection and transmission to the state of a wide range of personal data. The latter two challenges become more acute in light of the extension of checks from third-country nationals to citizens. The human rights challenges also become rule of law challenges as responsibilization in the form of the privatization of immigration control may lead to gaps in the legal responsibility of the state for preventing access and infringing fundamental rights, as the state can hide behind the acts of the private sector. These rule of law challenges will be explored further below.

B. Immigration Control via Delegation to Agencies

Another example of delegation of state power in the field of immigration control is the establishment of new and extension of the mandate of existing agencies. In both the European Union and the United States, the focus on the role of agencies has been highly symbolic politically and justified on the grounds of the need to provide better

130. *See generally* David Garland, *The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society*, 36 BRIT. J. CRIMINOLOGY 445 (1996) (introducing the term "responsibilization").

131. For an analysis of privatization in this context, see VALSAMIS MITSILEGAS, MONEY LAUNDERING COUNTER-MEASURES IN THE EUROPEAN UNION: A NEW PARADIGM OF SECURITY GOVERNANCE VERSUS FUNDAMENTAL LEGAL PRINCIPLES (2003).

coordination to state practices of border control.[132] Transatlantic convergence of law and practice has seen the establishment of new agencies, the extension of agency powers—in line with the securitization of immigration control discussed above—to cover not only immigration control stricto sensu, but also security matters, the prioritization of interagency cooperation (in particular cooperation between immigration control agencies and security agencies) and the establishment of transatlantic cooperation channels between these agencies. As with the privatization of immigration control, delegation of power to agencies has potentially significant fundamental rights and rule of law implications.

In the United States, delegation of immigration control to agencies has become particularly prominent post-9/11, where U.S. law and policy in the field was marked by a shift from immigration control to border security more broadly. With border security becoming a central element of the post-9/11 national security strategy, specific divisions within the DHS have been allocated a number of responsibilities for various aspects of immigration control.[133] A recent book by a policy expert on U.S. counterterrorism and border security enumerates no less than thirty-five agencies with roles in "securing human mobility."[134] These are split between the White House and four other government departments: the DHS, the State Department, the Department of Justice, and the Department of Defense. The proliferation of agencies dealing with immigration control—and beyond that, "human mobility" (see below)—is clearly illustrated when one looks at the relevant agencies within the DHS: along with the DHS senior leadership, responsibility lies, inter alia, with Offices of Intelligence and Analysis, Policy, U.S. Visitor and Immigrant Status Indicator Technology Program (US-VISIT), U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, U.S. Coast Guard, and the Transportation Security Administration.[135] This architecture clearly represents an extension of state power as well as a strongly securitized approach to immigration control.

In the European Union, efforts to address the impact of globalization and the geopolitical and legal changes in Europe resulting

---

132. *See generally* HOUSE OF LORDS EUROPEAN UNION COMMITTEE, FRONTEX: THE EU EXTERNAL BORDERS AGENCY, 9TH REPORT, HL PAPER 60 (SESSION 2007-08); *Border Security in the European Union*, *supra* note 72; 9/11 COMMISSION REPORT, *supra* note 40.

133. On the development of the DHS in the context of border security, see *Borders, Security and Transatlantic Cooperation in the Twenty-First Century*, *supra* note 45.

134. SUSAN GINSBURG, SECURING HUMAN MOBILITY IN THE AGE OF RISK: NEW CHALLENGES FOR TRAVEL, MIGRATION AND BORDERS (2010).

135. *Id.* at 124.

in the abolition of internal border controls within the European Union, on the one hand, and the extension of EU territory via the successive enlargements of the European Union (in particular the eastward enlargements) on the other, have led to the establishment of a European agency responsible for border controls (FRONTEX).[136] The latter has been established as a Community Agency with specific responsibilities for border management.[137] Creating a border management agency at the EU level has posed a number of significant challenges for the reconfiguration of immigration control in Europe. First of all, the discussion of delegation of powers from the state to agencies must be viewed in the specific light of EU law, where the additional layer of the contested relationship between the competence of the European Union (and its agencies) and the Member States exists. This aspect is particularly relevant in the field of immigration control, traditionally linked to state sovereignty. In this context, a key question as regards the delegation of immigration control powers at the EU level is who has the power, and thus the legal responsibility, for immigration control: is it the Member States of the European Union, or the EU Agency (FRONTEX)? As will be demonstrated below, the lines between national and European Union competence in the field are blurred on many occasions, resulting in gaps in the legal protection of those affected by immigration control at the EU level.

The difficult task of establishing a European agency for immigration control, while respecting state sovereignty in the field, is reflected in the careful articulation of the FRONTEX's powers. The opening article to the FRONTEX Regulation states that the aim of the Agency is to improve "the integrated management of the external borders of the Member States of the European Union."[138] While the responsibility for the control and surveillance of external borders lies with Member States, the provision continues, the Agency will facilitate and render more effective the application of European Community measures by coordinating Member States' implementation of these measures, thereby contributing to "an efficient, high and uniform level of control on persons and surveillance of the external borders of the Member States."[139] To achieve this, the main tasks of the Agency are to coordinate operational cooperation between Member States, including

136. For the background to the establishment of FRONTEX, see *Border Security in the European Union*, *supra* note 73.

137. Council Regulation 2007/2004, Establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, 2004 O.J. (L 349) 1 (EC).

138. See Article 1, *id.* at 3.

139. *Id.*

the evaluation, approval, and coordination of proposals for joint operations and pilot projects and launching, in agreement with Member States concerned, of initiatives for such operations and projects;[140] to assist Member States with training of border guards;[141] to carry out risk analysis by developing a common risk analysis model;[142] to follow up research development on border control;[143] to assist Member States in circumstances requiring increased technical and operational assistance at external borders;[144] and to provide Member States with the necessary support in organizing joint return operations.[145]

The key to the question of the extent to which FRONTEX has replaced national border controls is to determine the extent of the Agency's coordination powers.[146] Two main questions arise in this context: first, whether Agency staff will have enforcement powers in the territory of Member States (and consequently which rules will apply to them); and second, whether the Agency has coercive powers over Member States when organizing joint operations. As to the first question, Article 10 of the FRONTEX Regulation states that the "exercise of executive powers by the agency's staff and the Member States' experts acting on the territory of another Member State shall be subject to the national law of that Member State."[147] What constitutes "executive power" in this context is not defined in the regulation. The latter however avoids explicitly excluding operational powers of Agency staff from its scope, a view that is reinforced by the similar treatment of Agency staff with experts from Member States. There is less ambiguity with regard to the second question—i.e., whether the Agency can compel Member States to participate in joint operations without their agreement. Article 3(1) states that "the Agency may itself, and *in agreement with the Member State(s) concerned*, launch initiatives for

140. See Articles 2(1) and 3(1), *id.* at 4.

141. See Articles 2(1) and 5, *id.* In this context, developments such as the Community Borders Code are particularly relevant. Regulation (EC) No. 562/2006, 2006 O.J. (L 105) 1.

142. Council Regulation 2007/2004, *supra* note 137, at 4.

143. See Articles 2(1)(d) and 6, *id.*

144. *Id.* Article 8(b) specifically calls for the deployment of the Agency's experts to support national authorities. *Id.* at 5.

145. See Articles 2(1)(f) and 9, *id.* at 4, 5.

146. The preamble further confirms that the development of policy and legislation on external border control and surveillance remains a responsibility of the EU institutions, in particular the Council. *Id*. at 2.

147. *Id.* at 5. It is noteworthy and indicative of the sensitivity of the issue that in his evidence before the House of Lords EU Committee on the role of the Agency on returns of irregular immigrants, the Director, Mr. Laitinen, stated that they "do not have executive powers." *See* House of Lords E.U. Select Comm., *Illegal Migrants: Proposals for a Common EU Returns Policy*, 32d Report, Sess. 2005-06, HL Paper 166 (2006).

joint operations and pilot projects . . . ." (emphasis added).[148] Thus, Member States cannot be made to participate in joint projects without their agreement. Article 20(3) of the Regulation provides an additional safeguard by stating that proposals for decisions on specific activities to be carried out at, or in the immediate vicinity of, the external border of any particular Member State require a vote by the Member of the Management Board representing that Member State in favor of their adoption.

The powers of FRONTEX were further developed via the amendment of its legal basis to allow for the deployment of so-called Rapid Border Intervention Teams Regulation (RABITs).[149] There is a greater pooling of state sovereignty and a greater clarity and detail as to the tasks of these teams, which are deployed for the purposes of providing rapid operational assistance for a limited period to a requesting EU Member State facing a situation of urgent and exceptional pressure.[150] The tasks and powers of these teams, the first of which was deployed at the request of Greece in the autumn of 2010 on the Greek-Turkish land border,[151] are described in Article 6 of the RABITs Regulation. This article states that "Members of the teams shall have the capacity to perform all tasks and exercise all powers for border checks or border surveillance" in accordance with the Schengen Borders Code and "that are necessary for the realisation of the objectives of that Regulation."[152] Article 6 also states that they may only perform tasks and exercise powers under instructions from and, as a general rule in the presence of border guards of the host Member State.[153] The RABITs Regulation further contributes to the militarization of the EU external border, as they are allowed to carry weapons[154] and use force, including weapons.[155] According to the

148. Council Regulation 2007/2004, *supra* note 137, at 4.

149. Regulation (EC) No. 863/2007, 2007 O.J. (L 199) 30 (establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers).

150. *Id.*

151. *See* General Report: European Agency for the Mgmt. of Operational Cooperation at the External Borders of the Member States of the E.U., FRONTEX, at 40 (2011).

152. Regulation (EC) No. 863/2007, *supra* note 149, at 33.

153. *Id.*

154. According to Article 6(5) of the RABITs Regulation,

> [w]hile performing their tasks and exercising their powers, members of the teams may carry service weapons, ammunition and equipment as authorised according to the home Member State's national law. However, the host Member State may prohibit the carrying of certain service weapons, ammunition and equipment, provided that its own legislation applies the same prohibition to its own border guards.

Id.

provision on applicable law, while performing the tasks and exercising the powers, the members of the teams shall comply with EC law and the national law of the host Member State.[156]

The RABITs Regulation has added detail on the legal framework of some aspects of FRONTEX operations,[157] and represents a clear shift from purely national to EU border control involving executive measures and coercive powers. However, the legal framework of FRONTEX still creates a number of concerns with regard to gaps in the accountability and legal responsibility of the Agency. Delegation of immigration control to an EU agency increases enforcement powers by providing an additional layer of immigration control and the Agency's actions may have significant consequences for the individuals affected, with FRONTEX already actively coordinating Member State action in the field.[158] However, the extent of the powers and accountability of the agency are unclear. FRONTEX has been established as a management agency, and its annual reports are dominated by management-speak and management-style targets. This may lead to a depoliticization of border controls at the EU level, as well as fundamental decisions on EU border strategy being made on the basis of the FRONTEX operational plan and the decisions of its management board rather than on the basis of a more open debate.[159] Thus far, decisions on FRONTEX operations have been shrouded in secrecy,[160] with transparency as to its operational plans lacking.[161] Moreover, while its parent regulation has

155. According to Article 6(6),

> [w]hile performing their tasks and exercising their powers, members of the teams shall be authorised to use force, including service weapons, ammunition and equipment, with the consent of the home Member State and the host Member Sate, in the presence of border guards of the host Member State and in accordance with the national law of the host Member State.

Id. However, Article 6(7) allows the use of weapons, ammunition, and equipment "in legitimate self-defence and in legitimate defence of members of the teams or of other persons, in accordance with the national law of the host Member State." *Id.*

156. See Article 9, *id.* at 34.

157. As has the 2010 Decision on the surveillance of the sea external borders, discussed in part, see Council Decision 2010/252, *supra* note 37, at 20.

158. For details of FRONTEX planning and coordinating of joint border control operations contained in its annual reports, see *Annual Reports*, FRONTEX, www.frontex.europa.edu/annual_report (last visited Jan. 20, 2012).

159. For more on FRONTEX and depoliticization, see *Border Security in the European Union*, *supra* note 73.

160. *See* Violeta Moreno-Lax, *Seeking Asylum in the Mediterranean: Against a Fragmentary Reading of EU Member States' Obligations Accruing at Sea*, 23 INT'L. J. REFUGEE L. 174, 184 (2011).

161. The recent amendment to the FRONTEX Regulation calls for the drawing up of an operational plan by the Executive Director of FRONTEX for the joint operations organized by the Agency. *See* Regulation (EU) No. 1168/2011, 2011 O.J. (L 304) 7.

emphasized coordination as a key FRONTEX task, it is not clear whether such coordination of national responses leads to FRONTEX responsibility. FRONTEX is officially a "management" agency but cannot easily fit in with the various typologies of EU agencies[162] that have been established primarily in a market regulation context.[163] The emphasis on management in the FRONTEX Regulation cannot mask the fact that FRONTEX is essentially an operational agency, involved in actions with a significant impact on the relationship between the individual and the state.[164]

Notwithstanding the growth in FRONTEX activities in recent years, it has been increasingly difficult to pin down its responsibilities when it comes to its action. FRONTEX may be operational in practice, yet it may also claim that it has no legal responsibility for border controls, as it has merely a "coordinating" role. This may lead to a situation in which FRONTEX denies any responsibility claiming that the exercise of border controls are for Member States,[165] while Member States frame controls at their external borders as controls by FRONTEX—with Member States increasingly viewing FRONTEX as an answer to their expectations with regard to their border control responsibilities.[166] The potential for the creation of gaps in the legal responsibility of actors in FRONTEX operations is magnified if one looks at the legal framework underpinning the relations between FRONTEX on the one hand and other bodies and agencies (in particular law enforcement agencies) and

---

162. For attempts at categorization of EU agencies, see Edoardo Chiti, *The Emergence of a Community Administration: The Case of European Agencies*, 37 COMMON MKT. L. REV. 309 (2000); Alexander Kreher, *Agencies in the European Community: A Step Towards Administrative Integration in Europe*, 4 J. EUR. PUB. POL'Y 225 (1997); Ellen Vos, *Reforming the European Commission: What Role to Play for EU Agencies?*, 37 COMMON MKT. L. REV. 1113 (2000).

163. *See* Giandominico Majone, *The New European Agencies: Regulation by Information*, J. EUR. PUB. POL'Y 262 (1997) (arguing that networking between agencies can help enhance their reputation and independence, increasing the development of information-based modes of regulation).

164. *See Extraterritorial Immigration Control*, *supra* note 128. As Curtin notes, it can be argued that in the case of FRONTEX the Council did not delegate its own existing executive powers but rather the tasks in question had been exercised by Member States. DEIDRE CURTIN, EXECUTIVE POWER OF THE EUROPEAN UNION: LAW, PRACTICES, AND THE LIVING CONSTITUTION 164 (2009).

165. See, in this context, the striking FRONTEX news release in which FRONTEX "would like to state categorically that the agency has not been involved in diversion activities to Libya," the latter being based on a bilateral agreement between Italy and Libya. *Commissioner Malmström visits Frontex*, FRONTEX (Feb. 18, 2010), http://www.frontex.europa.eu/newsroom/news_releases/art70.htm.

166. *Area of Justice, Freedom, and Security*, HELLENIC REPUB. MIN. FOREIGN AFF. (Feb. 3, 2012), http://www1.mfa.gr/en/foreign-policy/greece-in-the-eu/area-of-justice-freedom-and-security.html?page=4.

third countries on the other. The FRONTEX Regulation provides for cooperation between the Agency and international organizations (including Europol) and third countries on the basis of "working arrangements."[167] FRONTEX has already entered into a number of such "working arrangements" with security and law enforcement agencies both within[168] and outside the European Union,[169] as well as with a number of third states.[170] The ambiguity regarding the legal force of working arrangements and the lack of transparency with regard to their negotiation and content may lead to the emergence of FRONTEX as an actor in a securitized, global system of immigration control without being accompanied by clearly defined standards of legal responsibility, either for itself or for its interlocutors. The implications of these lacunae in legal responsibility will be further explored in the section on extraterritorial immigration control below.[171]

C. Immigration Control and Technology

The growing recourse to technology for border controls has been discussed in this Article in the section on the securitization of immigration control. The latter is based largely on the establishment and development of databases, the collection and checking of biometrics, and the use of automated gates in entry and exit points. The state has relied on technology in developing further layers of control and surveillance of individuals on the move. However, this recourse to technology has significant consequences for the affected individuals. It leads to the dehumanization of individuals via the instrumentalization of the human body, with sensitive pieces of personal data being provided to the state and checked on a regular basis at various instances of

---

167. *See* Articles 13-14, Council Regulation 2007/2004, *supra* note 137, at 5-6.

168. *See* EUROPOL & FRONTEX, Strategic Co-operation Agreement Between the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union and the European Police Office (2011), *available at* https://www.europol.europa.eu/sites/default/files/flags/frontex.pdf.

169. *See Frontex Signs Working Arrangement with Interpol*, FRONTEX (May 29, 2009), http://www.frontex.europa.eu/newsroom/news_releases/art63.html.

170. As of February 2011, FRONTEX had concluded working arrangements with the competent authorities of fourteen third countries: Russia, Ukraine, Croatia, Moldova, Georgia, the Former Yugoslav Republic of Macedonia, Serbia, Albania, Bosnia and Herzegovina, Montenegro, Belarus, Canada, Cape Verde, and the United States. Negotiations for eight further working arrangements had been taking place at the time with the following countries: Turkey, Libya, Morocco, Senegal, Mauritania, Egypt, Brazil, and Nigeria. *See External Relations*, FRONTEX, http://www.frontex.europa.eu/external_relations/ (last visited Jan. 20, 2012).

171. *See infra* Part IV.

travel.[172] It is based on the continuous risk assessment of passengers at various entry and exit points, as well as in advance of travel, and such risk assessment is based on automaticity, with a negative assessment potentially leading to failure to be accepted for travel or to pass an automated gate. Along with its contribution to the extension of state surveillance, the use of technology may thus lead to the prevention of entry and challenge the rule of law by restricting the avenues for a legal remedy in cases of denial of entry. The growing emphasis on the use of technology for immigration control and the need for related issues to be addressed as technical, rather than legal issues, further constitute another level of depoliticization. In addition to the aspects of immigration control discussed in the securitization section of this Article, this section will highlight the above challenges by discussing two further examples of technological immigration control: one in the United States and one in the European Union.

As Rey Koslowski has noted, technology has been used by the DHS as a "force multiplier" to increase border control capacity.[173] In this context, in 2005 the DHS launched a new technology project designed to monitor the border: the Secure Border Initiative (SBI). SBI is a comprehensive, multiyear plan that, among other things, involves a "systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of unmanned aerial vehicles (UAVs), and next-generation detection technology."[174] SBInet had a bumpy ride, facing continued and repeated technical problems, cost overruns and schedule delays,[175] and was eventually cancelled in January 2011. "In cancelling the program, [DHS Secretary, Janet] Napolitano made clear that border enforcement would continue, with continued 'boots on the ground' and more intensive 'point defense'—deploying existing technology, such as surveillance drones, radar, and sensors, in strategic locations."[176] Notwithstanding the challenges the use of technology for immigration control presented in

172. *See also* Huub Dijstelbloem, *Europe's New Technological Gatekeepers: Debating the Deployment of Technology in Migration Policy*, 1 AMSTERDAM L. F., no. 4, 2009 at 11, 13 (arguing that "[b]iometry can violate the integrity of the person or lead to the personal body being regarded as an instrument").

173. Rey Koslowski, *The Evolution of Border Controls as a Mechanism to Prevent Illegal Immigration*, MIGRATION POL'Y INST. 3 (2011).

174. *Id.* at 9.

175. *See* Koslowski, *supra* note 173; DEP'T HOMELAND SEC., *Southwest Border Security Technology: New Path Forward*, *available at* http://www.bizjournals.com/washington/pdf/technologyPlan.pdf (last visited Jan. 26, 2012) (evaluating the results of the department-wide assessment of the SBInet program).

176. Demetrios G. Papademetriou & Elizabeth Collett, *A New Architecture for Border Management*, MIGRATION POL'Y INST., 10 (2011).

the implementation of the program, the emphasis on the use of technology for surveillance purposes remains.

At the EU level, the emphasis on technology is clearly reflected in a Commission Communication on the "interoperability" of databases.[177] The purpose of the Communication was to highlight how, beyond their present purposes, databases "can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime."[178] On the basis of this approach, the Commission argued strongly in favor of granting "authorities responsible for internal security" access to immigration databases including the VIS.[179] The communication provided a definition of "interoperability," which is the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge."[180] According to the Commission, interoperability is a technical rather than a legal or political concept.[181] This attempt to treat interoperability, which is a term now increasingly used by EU institutions,[182] as a merely technical concept, while at the same time using the concept to enable maximum access to databases containing a wide range of personal data (which become even more sensitive with the sustained emphasis on biometrics) is a striking attempt to depoliticize the issue and shield developments from the enhanced scrutiny that the adoption of legislation in the field would provide.[183]

The challenges of emphasizing technology as a tool for immigration control in the European Union are further evident in recent proposals to

177. *See Communication from the Commission to the Council and the European Parliament on Improved Effectiveness, Enhanced Interoperability and Synergies Among European Databases in the Area of Justice and Home Affairs*, COM (2005) 597 final, (Nov. 24, 2005).

178. *Id.* at 2.

179. *Id.* at 8. The Commission also took the opportunity to float proposals for longer-term developments, including the creation of a European Criminal Automated Fingerprints Identification System, the creation of an entry-exit system and introduction of a border crossing facilitation scheme for frequent border crossers, and European registers for travel documents and identity cards. *Id.* at 8-9. On these developments, see *supra* Part III.A.

180. *Id.* at 3.

181. *Id.*

182. *See, e.g.*, Press Release, Justice and Home Affairs 2873d Council Meeting, ¶ 16 (June 5-6, 2008) (stating that pilot projects developing future EU border management measures should allow for "maximum interoperability").

183. *See Extraterritorial Immigration Control*, *supra* note 128.

develop a European Border Surveillance System (EUROSUR).[184] The development of such a system was floated by the Commission in a Communication published in 2008.[185] According to this document,

> It is necessary to envisage a common *technical* framework to support Member States' authorities to act efficiently at local level, command at national level, coordinate at European level and cooperate with third countries in order to *detect, identify, track and intercept* persons attempting to enter the EU illegally outside border crossing points (emphasis added).[186]

This passage expressly links technology, the intensification of surveillance on the basis of intelligence, and prevention in EU immigration control. This link is confirmed by subsequent Commission proposals on how to take EUROSUR forward.[187] The latter call for the establishment of an "information sharing and cooperation mechanism enabling Member States' authorities carrying out border surveillance activities and FRONTEX to collaborate at tactical, operational and strategic levels," (emphasis omitted)[188] including the development of "situational pictures" at the national and European level which will be partly based on a "Common Pre-Frontier Intelligence Picture" managed by FRONTEX.[189] The Commission envisages the development of EUROSUR in eight steps: (1) providing the essential border surveillance infrastructure at the national level; (2) establishing a communication network between the national coordination centers including FRONTEX (which will "provide communication tools and electronic data exchange in order to send, receive and process non-classified and classified information 24/7 close to real time"); (3) providing support to neighboring third countries for the establishment of border surveillance

184. *See generally* Julien Jeandesboz, *Beyond the Tartar Steppe: EUROSUR and the Ethics of European Border Control Practices*, *in* EUROPE UNDER THREAT? SECURITY, MIGRATION AND INTEGRATION (J. Peter Burgess & Serge Gutwirth eds., forthcoming 2012).

185. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the Creation of a European Border Surveillance System (EUROSUR)*, COM (2008) 68 final (Feb. 13, 2008).

186. *Id.* at 4.

187. *Commission Staff Working Paper: Determining the Technical and Operational Framework for the European Border Surveillance System (EUROSUR) and the Actions to be Taken for its Establishment*, at 3, SEC (2011) 145 final (Jan. 28, 2011).

188. *Id.* at 4.

189. *Id.*

infrastructure;[190] (4) focusing on research and development; (5) developing common application of surveillance tools;[191] (6) developing a common prefrontier intelligence picture;[192] (7) creating a common information sharing environment for border control and internal security purposes covering the Mediterranean Sea, the southern Atlantic Ocean (Canary Islands), and the Black Sea; and (8) ultimately creating "a common information sharing environment for the whole EU maritime domain."[193]

The emphasis on technology, intelligence, and extraterritoriality is evident in the Commission's vision of the development of EUROSUR. Technology is to be used to establish a system of European border surveillance that will be extended, in effect, to third countries.[194] Key elements of this system are the interconnection and interoperability of databases and maximum information exchange, including between civilian and military authorities. Extensive surveillance is thus to be enabled by technology, with the aim of producing intelligence and preventing entry into the European Union. Technology is thus used to extend the reach and powers of the state with significant consequences for the individuals affected by EUROSUR, both in terms of privacy and data protection, and access to the territory of the European Union. Notwithstanding these consequences, in the development of EUROSUR

190. According to the Commission,

> [a] concrete example of how such support, leading to closer cooperation, could be given is the SEASHORE network which is operational between Spain, Portugal, Mauretania, Senegal and Cape Verde. Gambia, Guinea Bissau and Morocco joined the SEAHORSE network in November 2010. SEAHORSE could be used as a model for setting up a similar network between Member States and neighbouring third countries in the Mediterranean sea.

Id. at 7.

191. These surveillance tools consist of three components: "[t]racking of vessels on the high seas"; "[p]unctual monitoring of selected neighbouring third-country ports and coasts"; and "[m]onitoring external land borders and the pre-frontier area." *Id.* at 8.

192. This prefrontier intelligence picture consists of four components: "[o]perational information, e.g. on detected targets and alerts"; "[s]trategic key information, e.g. on routes and methods used by traffickers"; "[k]nowledge base, i.e. a formalised description of vocabulary and methods"; and "[b]asic geodata, e.g. topographic and thematic maps and nautical charts." *Id.* at 8.

193. The Common Information Sharing Environment's guiding principles are: "[a]n approach interlinking all user communities"; "[b]uilding a technical framework for interoperability and future integration"; "[i]nformation exchange between civilian and military authorities"; and finally, "[s]pecific legal provisions." *Id.* at 9.

194. Cooperation with third countries has also been emphasized by the governments of EU Member States. *See* Press Release, Justice and Home Affairs, (Feb. 25-26, 2008) (noting five specific conclusions concerning the development of EUROSUR).

the establishment of a legal framework to regulate the use of technology is merely an afterthought.[195]

III. GLOBALIZATION AND EXTRATERRITORIALITY

The development of extraterritorial immigration control practices has been a key tool for states to address perceived pressures from global migration flows. Extraterritoriality in this context has a number of advantages for states. On the one hand, it extends the reach of the state outside its territory with the aim of preventing access; on the other hand, it may create gaps in the legal responsibility of states, as states may claim that their domestic law or international obligations do not apply outside their territory.[196] Extraterritoriality in immigration control has thus far been addressed in this Article on a number of occasions: in examining prevention in the context of securitized immigration control; in analyzing privatization, and in particular the role of carriers; and, in the case of the European Union, in examining the evolution of agencies and systems such as FRONTEX and EUROSUR.

Extraterritorial immigration control practices are not uniform in these examples. They can be differentiated using criteria such as their territorial reach and their actual effect. In regards to territorial reach, one can distinguish between extraterritorial immigration control on the high seas (in international waters) and extraterritorial immigration control taking place in agreement with (and in the territory of) third countries. In regards to effect, one can distinguish between actual operational intervention (e.g., by boarding a ship) and prevention of access to the territory (e.g., by deflecting a boat or preventing boarding in the territory of a third state on the basis of tracking of individuals with intelligence obtained via surveillance). The challenges with regard to determining the legal responsibility of states when exercising extraterritorial immigration control are exacerbated in the case of the European Union, where the division of power between FRONTEX and Member States is not always clear.

In determining state responsibility for extraterritorial immigration control, useful lessons can be drawn from the case law of the European Court of Human Rights in Strasbourg. On a number of occasions, the Strasbourg Court has attempted to clarify the extent of state

195. As seen above, a vague reference to "legal provisions" comes last on the list of the guiding principles for a Common Information sharing environment for the whole EU maritime domain.

196. For an overview of these challenges, see generally EXTRATERRITORIAL IMMIGRATION CONTROL: LEGAL CHALLENGES, *supra* note 126.

responsibility for complying with the European Convention on Human Rights when acting extraterritorially. In its recent ruling in *Al-Skeini*, the court confirmed that in certain circumstances, the use of force by a state's agents operating outside its territory may bring the individual under the control of the state's authorities into the state's jurisdiction under Article 1 of the Convention.[197] Reiterating its earlier case law, the court added that "[w]hat is decisive in such cases is *the exercise of physical power and control over the person in question*" (emphasis added).[198]

A case cited in *Al-Skeini* which is of particular relevance to the issue of extraterritorial immigration control is *Medvedyev*.[199] The court ruled that the Convention applied extraterritorially in enforcement actions by France in a case of suspected drug trafficking on the high seas. As this was a case of France having exercised "full and effective control" over the boat in question and its crew, "at least de facto, from the time of its interception, in a continuous and uninterrupted manner until they were tried in France, the applicants were effectively within France's jurisdiction for the purposes of Article 1 of the Convention" (emphasis omitted).[200] The case is of relevance for extraterritorial immigration control not only because it involved the use of force and actual interception at sea, but also because this happened in a relative legal vacuum with few developed international law rules in the field. The court recognized this vacuum by stating that "it is regrettable . . . that the international effort to combat drug trafficking on the high seas is not better coordinated bearing in mind the increasingly global dimension of the problem" (emphasis omitted)[201] and found "that the deprivation of liberty" in this case "was not 'lawful' . . . for lack of a legal basis of the requisite quality to satisfy the general principle of legal certainty" (emphasis omitted).[202] The court rejected the French Government's claim that interception on the high seas is a special case, stating that

> The special nature of the maritime environment relied upon by the Government in the instant case cannot justify an area outside the law where ships' crews are covered by no legal system capable of affording them enjoyment of the rights and guarantees protected by the

197. *See* Al-Skeini v. United Kingdom, App. No. 55721/07, Eur. Ct. H.R. 1 (2011).
198. *Id.* at 58-59.
199. Medvedyev v. France, App. No. 3394/03 Eur. Ct. H.R. (2010).
200. *Id.* ¶ 67.
201. *Id.* ¶ 101.
202. *Id.* ¶ 102.

> Convention which the States have undertaken to secure to everyone within their jurisdiction, any more than it can provide offenders with a "safe haven" (emphasis omitted).[203]

The European Court of Human Rights (ECHR) has thus attempted to address the rule of law and fundamental rights issues arising from the existence of gaps in legal protection in extraterritorial state acts by expanding state jurisdiction under the Convention. The jurisprudence of the court is particularly relevant in cases of extraterritorial immigration control, as the court's approach, in effect, exports the border to places and instances where the state exercises enforcement action. This approach has been characterized as "functional." What matters is not a generalized test of personal or geographical control, but rather the specific power or authority assumed by the state acting extraterritorially in a given capacity.[204] In this manner, extraterritorial state action, either on the high seas and in international waters or in the territory of a third state, is subject to human rights norms. In the case of the European Union, this extension is of particular importance in view of the prospective post-Lisbon accession of the European Union to the European Convention on Human Rights. EU accession to the ECHR will mean, inter alia, that EU institutions (including bodies and agencies like FRONTEX) will be bound by the Convention.

What is less evident from this approach is whether these norms apply in cases where there is no actual state enforcement action taking place, but where there are attempts to deflect movement via the use of surveillance extraterritorially (for instance via the use of EUROSUR) or in cases where the attribution of responsibility is difficult because multiple authorities are involved (particularly in cases of FRONTEX operations, including cooperation with third states). An expansive interpretation of jurisdiction will address these issues and remedy the legal uncertainty stemming from gaps in legal responsibility. Such expansive interpretation, broadening the causal link between state intervention and the effect on the individuals concerned, has been put forward by scholars such as Thomas Gammeltolft-Hansen, who has argued that in the human rights context, jurisdiction in this sense flows from the de facto relationship established between the individual and the state through the very act itself, *or the potential of acting* (emphasis added).[205] In a similar vein (but focusing more specifically on the

---

203. *Id.* ¶ 81.

204. THOMAS GAMMELTOFT-HANSEN, ACCESS TO ASYLUM INTERNATIONAL REFUGEE LAW AND THE GLOBALISATION OF MIGRATION CONTROL 124 (2011).

205. *Id.* at 125.

operation of FRONTEX and its relationship with Member States), Guy Goodwin-Gill notes that:

> Interception operations are initiated and coordinated by the EU agency, Frontex, and collaboratively or individually by EU Member States. Directly *or indirectly*, they affect the rights of individuals, some or many of whom may be in need of international protection. Within the terms of the ILC articles on state responsibility, particularly Article 4 and 6, interceptions continue to be carried out in the exercise of governmental authority by the state, or in the equivalent exercise of its executive competence by the EU's agency (emphasis added).[206]

Nothing in the evidence of practice to date reveals any break in the chain of liability. Neither the on-board presence of a third-state official, nor the use of joint patrols in which actual interception is undertaken by a third state, disengage the primary actor from responsibility for setting the scene that allows the result, if nothing more. In each case, the EU agency or Member States exercise a sufficient degree of effective control; it may not be solely liable for what follows, but it is liable nonetheless.[207]

IV. THE NEXUS BETWEEN SECURITY, DELEGATION AND EXTRATERRITORIALITY: FROM IMMIGRATION CONTROL TO THE SURVEILLANCE OF MOVEMENT IN A GLOBALIZED WORLD

The analysis thus far has attempted to demonstrate how immigration control is being transformed in an era of globalization following three major trends: the securitization of immigration and mobility; the delegation of state power to the private sector, government agencies, or databases; and the emphasis on extraterritorial immigration control. This section will cast light on the nexus between these trends by examining in detail the development of a global legislative framework aimed at monitoring movement by the collection and transmission of Passenger Name Record (PNR) data to state authorities. Devoting a separate part specifically to PNR is necessary for a number of reasons: it highlights the interconnections between the

206 Guy S. Goodwin-Gill, *The Right to Seek Asylum: Interception at Sea and the Principle of Non-Refoulement,* 23 INT'L J. REFUGEE L. 443, 453 (2011).

207 *Id.*

various immigration control trends analyzed above; it highlights how a global paradigm of immigration control has emerged following unilateral U.S. action and subsequent transatlantic convergence; it demonstrates the more general shift from immigration control on the physical border focusing only on foreigners to generalized extraterritorial surveillance aimed at citizens and foreigners alike; and, in the light of all of the above, it demonstrates how globalized immigration controls have strengthened the state at the expense of human rights. To highlight the above issues, the analysis in this Section will follow the various legal and policy steps from the introduction of PNR requirements in U.S. law to the reaction of the European Union, the achievement of transatlantic convergence, and the push toward global standards.

A. U.S. Law Post-9/11

As seen above, the surveillance of movement and passenger flows has been a key component of U.S. counterterrorism strategy post-9/11. Globalization and extraterritoriality have been central in the development of U.S. law and policy in the field. In a DHS strategy document, it was stated expressly that "the increasing mobility and destructive potential of modern terrorism has required the United States to rethink and rearrange fundamentally its systems for border and transportation security" and that border security must be conceived as "fully integrated requirements because our domestic transportation systems are intertwined inextricably with the global transport infrastructure."[208] This focus on globalization was reaffirmed by the then-U.S. DHS Secretary, Tom Ridge, who noted that "[a]s the world community has become more connected through the globalization of technology, transportation, commerce and communication . . . the benefits of globalization available to peace loving, freedom loving people are available to the terrorists as well."[209] Not only immigration, but also mobility and movement via globalization have thus been securitized.

In this light, the United States passed legislation in November 2001 requiring air carriers operating flights to, from, or through the United States to provide U.S. Customs with electronic access to data contained in their automatic reservation and departure control systems.[210] This data, known as Passenger Name Records (PNR), constitutes a record of

208. OFFICE FOR HOMELAND SECURITY, supra note 42, at 21.

209. Louise Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 25 POL. GEOGRAPHY 336, 339 (2006).

210. *See* 49 U.S.C.A. § 44909 (2004); Correction of Air Cargo Manifest or Air Waybill, 19 C.F.R. § 122.49 (2005).

each passenger's travel requirements and contains all the information necessary to enable reservations to be processed and controlled by the booking and participating airlines. Transfer of such information to the U.S. authorities *before* departure has been a key element of the U.S. border security strategy, focusing on identification and prevention. PNR data can include a wide range of details, from the passenger's name and address to their email address, credit card details, and on-flight dietary requirements. The transfer of PNR data was deemed to be key to the operation of the U.S. Automated Targeting System (ATS), which uses a wide range of databases, including law enforcement and FBI databases to assess and identify "travelers that may pose a greater risk of terrorist or criminal activity and therefore should be subject to further scrutiny or examination."[211]

B. The Response of the European Commission

The U.S. legislation mentioned above was applicable to all flights to the United States, including flights from the European Union. European airlines would thus have to comply with the legislation if they did not want to be subject to heavy fines or even to the cancellation of landing rights at U.S. airports. EU Member States did eventually agree in 2003 on a directive requiring carriers to transmit passenger data, but this directive covered the transmission of data for journeys to the European Union and required the transmission of much more limited categories of personal data (API data, namely data that can be found primarily on the passport).[212] Notwithstanding the fact that the API Directive was adopted under Title IV and its stated aim was to combat illegal immigration, there have been attempts by the U.K. government during negotiations to frame it also as a national security and counterterrorism matter (and thus align it with its domestic approach on border security and e-borders).[213] However, in spite of the adoption of the API Directive, concerns were voiced in the European Union that U.S. PNR legislation

---

211. *See generally* DEP'T OF HOMELAND SEC., *A Report Concerning Passenger Name Record Information Derived from Flights Between the U.S. and the European Union*, 38 (Dec. 18, 2008). It has been noted that the ATS generates a risk assessment score for each traveler. *See* Shachar, *supra* note 62.

212. Council Directive 2004/82, 2004 O.J. (L 261) 24 (EC); *see also* Mitsilegas, *supra* note 66 (analyzing the directive).

213. Caroline Flint, then a Home Office Minister, argued that the proposal "is all about border control, whether it is illegal immigration or criminals coming in, or people who are a threat to national security." House of Lords E.U. Select Comm., *Fighting Illegal Immigration: Should Carriers Carry the Burden?*, 5th Report, Sess. 2003-04, HL Paper 29, at ¶ 9 (2004).

was too invasive of privacy and could be in conflict with the European Community's and Member States' data protection standards.[214]

The Commission informed the U.S. authorities of these concerns and this led to the entry into force of the U.S. legislation being postponed until March 5, 2003. Negotiations were protracted and lasted well beyond March 5, 2003, when U.S. law formally entered into force vis-à-vis EU airlines. They resulted in an agreement between the Commission and the U.S. authorities on December 16, 2003. Following a series of undertakings by the U.S. authorities, the Commission accepted that U.S. data protection standards in the context of PNR transfers were adequate. The Commission expressed this in a communication issued that day, justifying its decision by stating that

> [t]he option of insisting on the enforcement of the law on the EU side would have been politically justified, but . . . would have undermined the influence of more moderate and co-operative counsels in Washington and substituted a trial of strength for the genuine leverage we have as co-operative partners.[215]

The Commission called for a global EU approach to the sharing of PNR data. On the issue of transfers between the European Union and the United States, the Commission noted that the way forward was to establish a legal framework for existing PNR transfers to the United States. This would consist of an "adequacy" decision by the Commission, certifying that the U.S. data protection standards were adequate, followed by a "light" bilateral, international agreement between the European Community and the United States. Although the U.S. legislation was prompted by the 9/11 events and is viewed in the United States as a counterterrorism measure, in the European Union it was dealt with as a first-pillar internal market measure and not as a third-pillar counterterrorism measure. Making the most of its mandate, the Commission was arguably trying to consolidate its position as the European Union's and Member States' chief representative in negotiating standards in the field—it does not seem accidental that the communication on PNR also calls for a "global" EU approach in negotiating standards in international fora, such as the International Civil Aviation Organization (ICAO), where, presumably, it will be the

214. *See* Mitsilegas, *supra* note 66.

215. *Communication from the Commission to the Council and the Parliament Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*, at 5, COM (2003) 826 final (Dec. 16, 2003).

Commission and not the Council or Member States that will take the lead.

C. The EU-U.S. PNR Agreements

The Commission's handling of the PNR dossier revealed a two-fold agenda: to establish a first-pillar competence for external action in the field and, linked with this, to emerge as a global actor, acting on behalf of the Community, negotiating with the United States, and developing global standards and cooperation in the field. The saga following these negotiations is clear. A first-pillar EC-U.S. PNR Agreement allowing the transfer of PNR data to the United States was signed in the face of vocal opposition from the European Parliament, expert data protection bodies, and civil society. In the decision authorizing the conclusion of the agreement,[216] the Council invoked the urgency caused by the uncertainty for carriers and passengers.[217] The decision was preceded by the Commission's decision confirming the adequacy of U.S. data protection standards, which was finally adopted on May 14, 2004.[218] The terms of the Agreement and the U.S. undertakings have not changed from the draft that was so heavily criticized in the Article 29 Working Party on Data Protection and the European Parliament.[219]

The European Parliament brought an action before the European Court of Justice (ECJ), asking for annulment of the decision authorizing the conclusion of the EC-U.S. Agreement, on the grounds of infringement of the right to privacy and data protection, breach of the principle of proportionality, and legality grounds.[220] In November 2005, the Advocate-General expressed the view that, while the agreement and decision did not cause fundamental rights concerns, the adequacy decision of the Commission and the decision authorizing the signature of the agreement had to be annulled since the agreement dealt primarily with fighting terrorism (i.e., a third- and not a first-pillar

---

216. Council Decision 2004/496, 2004 O.J. (L 183) 83 (EC).

217. *Id.*

218. Commission Decision 2004/535, 2004 O.J. (L 235) 11. For Undertakings of the U.S. Department of Homeland Security, see *id.* at 15-21. For the annexed list of PNR, see *id.* at 22.

219. *See generally Border Security in the European Union*, *supra* note 73.

220. The European Parliament argued that the then Art. 95 EC Treaty (on the internal market) was not the right legal basis for the contested decision. It also argued that its assent should be required for the adoption of the decision authorizing the conclusion of the international agreement and not its mere consultation, as has happened. According to the Parliament, the agreement constituted an amendment of the 1995 data protection directive. *See* Council Document No. 11876/04 of 6 August 2004, ¶ 2, 2, www.statewatch.org/news/2004/aug/pnr-court.pdf.

matter).[221] The court issued its ruling in May 2006[222] and annulled the agreement on legality grounds. According to the court, the transfer of PNR constituted a security (third-pillar) matter and not an internal market (first-pillar) matter.

The annulment of the agreement resulted in the conclusion of an interim third-pillar agreement, and finally in 2007, of a third-pillar EU-U.S. PNR agreement.[223] This agreement[224] has done little to address concerns with regard to the adequacy of U.S. privacy standards. Like the earlier texts, the agreement includes an adequacy assessment—the United States is deemed to ensure an adequate level of PNR data protection for PNR data transferred from the European Union—that is linked with the issue of transmission of "EU" PNR data to third countries. The adequacy assessment means that the European Union "will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds."[225] Moreover, in a statement reminiscent of the one in the EU-U.S. Mutual Legal Assistance Agreement, the parties recognize that "US and European privacy law and policy share a common basis and that any differences in the implementation of these principles should not present an obstacle to cooperation between the U.S. and the EU."[226] The preservation of the U.S. standards is also ensured by a provision making clear that the agreement is not intended to derogate from or amend existing U.S. (and EU) law, and expressly states (as in earlier texts) that the agreement "does not create or confer any right or benefit on any other person or entity, private or public."[227] The agreement also seems to be creating, on the basis of reciprocity, a common level of data protection between the two parties: the DHS "expects that it is not being asked to undertake data protection

221. Opinion of the Advocate General, Case C-317/04, Parliament v. Council, 2006 E.C.R. I-4721.

222. The Parliament was supported by the European Data Protection Supervisor, while the Council was supported by the Commission and the United Kingdom. *Id.*

223. *See* Valsamis Mitsilegas, *The External Dimension of EU Action in Criminal Matters*, 12 EUR. FOREIGN AFF. REV. 457, 484-87 (2007) [hereinafter *The External Dimension of EU Action in Criminal Matters*].

224. 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 (DHS) (2007 PNR Agreement), 2007 O.J. (L 204) 18 [hereinafter 2007 PNR Agreement]; *see also* Council Decision 2007/551, 2007 O.J. (L 204) 16 (EU) (approving the 2007 PNR Agreement on the basis of Articles 24 and 38 of the Treaty of the European Union).

225. 2007 PNR Agreement, *supra* note 224, at 19.

226. *Id.*; *see also The External Dimension of EU Action in Criminal Matters*, *supra* note 222.

227. 2007 PNR Agreement, *supra* note 224, at 20.

measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems" and vice-versa.[228]

Widespread transfer of personal data to the United States is authorized. Although the text of the agreement itself does not include details of the PNR data transfer per se, these are set out in a separate "US letter to the EU," signed by the then-Secretary of Homeland Security, Michael Chertoff, which accompanies the agreement.[229] The letter enumerates nineteen types of PNR data covered by the Agreement (these are more or less similar to the broad categories in the earlier agreements and include data such as payment information, seat information, and "general remarks").[230] U.S. government authorities with law enforcement, public security, or counterterrorism functions can access this data and transfer it to government authorities in third countries.[231] The agreement also contains provisions regulating the move, under certain conditions, from a "pull" to a "push" system for PNR data transfer[232] and provisions defining its purpose as fighting terrorism and other serious crimes. The agreement leaves open the option of unilateral broadening by the United States of its scope.[233] The letter also extends the retention period of PNR data essentially to a minimum of fifteen years—seven years in an "active analytical database" and a further eight years in dormant status.[234] This provision has encountered a critical reaction in the European Parliament, which raised its concern that such databases lead to "a significant risk of massive profiling and data mining."[235] The European Data Protection

228. *Id.* at 19. See also the Letter from Michael Chertoff, US Secretary of Homeland Security, to Luis Amado, President of the Council of the European Union, discussing the reciprocity arrangements of the 2007 PNR Agreement, contained therein. *Id.* at 21.

229. *Id.* This is in turn followed by an "EU letter to the US" confirming that, on the basis of the assurances provided in the U.S. letter, the European Union deems that the United States ensure an adequate level of data protection and that, based on this finding, "the EU will take all the necessary steps to discourage international organizations or third countries from interfering with any transfers of EU PNR data to the United States." *Id.* at 25.

230. *Id.* at 21-22.

231. *Id.* at 21.

232. *Id.* at 23-24.

233. By stating that "DHS will advise the EU regarding the passage of any US legislation which materially affects the statements made in this letter." *Id.* at 21.

234. *Id.* at 23.

235. Resolution on the PNR Agreement with the USA, EUR. PARL. DOC. P6 0347, ¶ 20 (2007).

Supervisor has also raised concerns,[236] as has the Article 29 Working Party on Data Protection.[237]

D. The Internalization of the U.S. Model by the European Union

By insisting on concluding PNR Agreements with the United States on the terms described above, the European Union has made the first step toward the establishment of a global model of securitized extraterritorial immigration control based on the surveillance of movement via its compliance with the demands of foreign law. However, global convergence in PNR standards has not been limited to legal texts aiming to accommodate domestic demands. Notwithstanding sustained concerns raised by the European Parliament and specialist EU data-protection bodies with regard to the compatibility of the EU-U.S. PNR agreements with EU privacy and data protection law, there is ongoing political momentum for the development of an internal, EU PNR system, where EU law will require (as a minimum) airlines flying into the European Union to submit PNRs to the authorities of EU Member States.

1. EU PNR Before the Entry into Force of the Lisbon Treaty

The first Commission proposal for an EU PNR system dates back to 2007, when the Commission tabled a proposal for a Framework Decision establishing a similar system of transmission of PNR data by carriers flying into the European Union.[238] The Commission justified the proposal as a result of the "policy learning" from the existing PNR Agreements with the United States and Canada, as well as the development of pilot projects in the United Kingdom. According to the Commission, both of these developments (involving countries, in particular the United States and the United Kingdom, that have pushed forward a specific concept of "border security" linked with technology

---

236. *See Comment of the European Data Protection Supervisor on International Data Exchange Agreements* (Jan. 25, 2010), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-01-25_EU_US_data_exchange_EN.pdf.

237. *See Comment of the European Data Protection Supervisor on International Data Exchange Agreements* (Jan. 25, 2010), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-01-25_EU_US_data_exchange_EN.pdf.

238. *Commission Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes*, COM (2007) 654 final (Nov. 6 2007).

and the fight against terrorism) have demonstrated the potential of PNR data for law enforcement purposes.[239]

Along with the concerns raised in the context of the EU-U.S. PNR saga, one could question the necessity and added value of an essentially similar system at the EU level. After all, as mentioned above, there is recent legislation at the EU level on the transfer of API data adopted under an immigration legal basis. Mindful of this criticism, the Commission attempted, in the Explanatory Memorandum to the PNR proposal, to distinguish between the two initiatives. The Commission notes that

> [f]or the purposes of the fight against terrorism and organised crime, the information contained in the API data would be sufficient only for identifying known terrorists and criminals by using alert systems. API data are official data, as they stem from passports, and sufficiently accurate as to the identity of a person. On the other hand, PNR data contains more data elements and are available in advance of API data. Such data elements are a very important tool for carrying out risk assessments of the persons, for obtaining intelligence and for making associations between known and unknown people.[240]

From this passage, it is clear that the Commission has adopted an intelligence-led model of border controls very similar to the "border security" models in the United States. The emphasis is on risk assessment and profiling by collecting a wide range of personal data at the earliest possible stage in time. From the limited categories of passport data to be transmitted prior to departure under the API Directive, we are now moving to the transfer of a wide range of information related to air passengers at a considerably earlier stage. The transfer of PNR data is viewed as necessary not only for border controls and immigration, but also for broader counterterrorism and security purposes.[241]

---

239. *Id.* at 2.

240. *Id.* at 3.

241. *See* HOME OFFICE, EXPLANATORY MEMORANDUM ON EUROPEAN LEGISLATION, 6007/11 (Feb. 16, 2011), *available at* http://amberhawk.typepad.com/files/lords-home-office-memo_select-cttee-report-on-pnr.pdf (noting the need "to allow the processing and exchange of PNR data for wider border security and crime-fighting purposes"). The U.K. government further advocated a wider scope to the proposal than the one envisaged by the

2. Post-Lisbon Developments

Since agreement on the 2007 Commission proposal was not reached before the entry into force of the Lisbon Treaty, the Commission tabled a new text after the entry into force of the Lisbon Treaty, this time in the form of a directive.[242] The Commission again stresses the law enforcement use of PNR data, distinguishing between reactive use (use in investigations, prosecutions after the fact), real-time use (use prior to arrival or departure for crime prevention), and proactive use, stating:

> use of the data for analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers. In order to carry out such an analysis of relevance for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, a commensurate period of retention of the data by law enforcement authorities is necessary.[243]

The Commission adds that "PNR data enable law enforcement authorities to identify persons who were previously 'unknown'. i.e. persons previously unsuspected of involvement in serious crime and terrorism."[244] The link between the collection and transfer of PNR data and preventative risk assessment is further highlighted. As the Commission notes,

> The use of PNR data prior to arrival allows law enforcement authorities to conduct an assessment and perform a closer screening only of those persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security. This facilitates the travel of all other passengers and reduces the risk of passengers being subjected to examination upon entry into the EU on the basis of unlawful criteria

---

Commission. *See* EUROPEAN SCRUTINY COMMITTEE, SEVENTH REPORT, 2007-8, H.C. 16-vii, at 40-41 (U.K.).

242. *Commission Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation, and Prosecution of Terrorist Offences and Serious Crimes*, COM (2011) 32 final (Feb. 2, 2011).

243. *Id.* at 3-4.

244. *Id.* at 4.

> such as nationality or skin colour which may wrongly be associated with security risks by law enforcement authorities, including customs and border guards.[245]

Under this justification, the collection of passenger data serves to establish a system of generalized surveillance of movement for security purposes, with a wide range of passenger data being required (as in the case of U.S. law) to be communicated to state authorities.[246] This represents a clear shift from immigration control to the surveillance of foreigners and citizens alike. Border controls are thus disaggregated, with everyday passenger data being collected at various instances in time. The combination of these data, along with other categories of data collected in an era of securitized immigration control for risk assessment purposes, has profound consequences for the affected individuals, whose "dangerousness" is to be assessed regularly. Conscious of these implications, the Commission argues that this system will avoid racial profiling, while at the same time facilitating the movement of bona fide passengers. The Commission's argument as regards to profiling is questionable, as the PNR system is clearly established for the purpose of constant risk assessment.[247] The implications for privacy and nondiscrimination in this context are significant, as are the implications for citizenship. By prioritizing the convenience argument, the Commission is aiming at making increased surveillance of everyday life acceptable to citizens, as they believe that "it will not be them," but others who are controlled.[248]

---

245. *Id.* at 5.

246. Requested data includes all forms of payment information, including billing address, travel status of passenger (including confirmations), check-in status, no show or go show information, seat number and other seat information, number and other names of travelers on PNR, and "general remarks." *See id.* at 32.

247. *See Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*, at 4-5 (Mar. 25, 2011), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-03-25_PNR_EN.pdf (noting that "the 'assessment' of passengers (previously worded 'risk assessment') will be performed on the basis of constantly evolving and non transparent criteria").

248. *See generally* Valsamis Mitsilegas, *Security Versus Justice: The Individualisation of Security and the Erosion of Citizenship and Fundamental Rights*, *in* JUSTICE AND SECURITY IN THE 21ST CENTURY: LIBERTY, HUMAN RIGHTS AND THE RULE OF LAW (Synnove Ugelvik & Barbara Hudson eds., forthcoming Jan. 2012) (describing the impact of arguments of convenience for the reconfiguration of the relationship between the individual and the state on the one hand and between citizens on the other).

E. A Global Approach

The reaction of the European Union to U.S. law with regard to the collection and transmission of passenger data has evolved from finding a way to comply with U.S. requirements while respecting EU law to accepting the U.S. model in principle and attempting to contribute toward the development of a global system of passenger surveillance. The emphasis on the globalization of the surveillance of movement has been confirmed by the European Commission's publication of a communication on developing a global approach to PNR data transfers to third countries.[249] This subsection will focus on this gradual development of global standards in the field from an EU perspective.

1. From Unilateral U.S. Demands to Transatlantic Convergence

The internalization of the U.S. model of the surveillance of movement by the European Union via the establishment of a European PNR system may be seen as a significant political move by EU institutions to ensure real reciprocity with the United States (indeed, U.S. airlines would be subject to these standards, and the adoption of EU standards in the field will trigger the application of the various reciprocity clauses in the PNR Agreement). However, this move also means that the European Union is essentially importing the whole U.S. model of intelligence-led, generalized surveillance based on profiling via the gathering of a wide range of everyday information on *all* passengers for security purposes. While negotiations on the scope and content of the instrument are difficult and ongoing, it is noteworthy that one of the issues being discussed is extending the system to *intra-European Community* flights, leading thus to the generalized surveillance of air travel *within* the borderless Schengen area.[250] After the ECJ ruling, and in a clear convergence of EU with U.S. approaches, measures of monitoring movement via the collection and transmission of PNR data are directly justified on the grounds of counterterrorism. Immigration law thus becomes terrorism law and is used to regulate everyday legitimate mobility. Framing of the proposal as a counterterrorism measure not only results in the weakening of privacy protection *inside* the European Union (with the third-pillar privacy and data protection framework being fragmented and limited to say the least) but also sits uneasily with the proclaimed freedom of

249. *Commission Communication on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries*, COM (2010) 492 final (Sept. 21, 2010) [hereinafter *Transfers of PNR*].

250. *See* Press Release, Justice and Home Affairs Council, at 18 (Oct. 24, 2008).

movement within the European Union.[251] If adopted, the EU PNR system will signify a striking convergence of immigration control models between the European Union and the United States (and, as will be seen below, major industrialized Western countries such as Australia and Canada), a convergence based on the adoption of a model of a securitized control of movement emphasizing prevention on the basis of risk assessment.

2. Ongoing Bilateralism: Common Criteria for EU Negotiations with Third Countries

The development of a globalized model of passenger data transfer is further promoted by the continuation of EU negotiations for international agreements with third states in the field. In its communication on a "global approach," the Commission put forward a set of general criteria that should form the basis of future negotiations of PNR agreements with third countries. The development of a global approach in this context was justified, inter alia, on the basis of the need to fight terrorism while respecting fundamental rights: to provide legal certainty to carriers, to ensure coherence between the various EU external commitments, and to contribute in increasing passenger convenience.[252] This approach was confirmed by the EU Council on Justice and Home Affairs, which agreed that the mandates for the forthcoming negotiation of PNR agreements between the European Union and the United States, Canada, and Australia should be identical in content and adopted at the same time.[253] It remains to be seen whether the European Union will achieve coherence as regards to the content of these three agreements and coherence between the international agreements and internal EU law.[254] In this context, the adoption of internal EU PNR law may provide a benchmark, but this must always be viewed within the general constitutional and human rights framework of European Union law.

---

251. *See generally The Borders Paradox*, *supra* note 93.

252. *Transfers of PNR*, *supra* note 249, at 6.

253. *See* Press Release, Justice and Home Affairs Council, at 11 (Oct. 7-8, 2010).

254. At the time of writing, the European Union appears to be close to an agreement with Australia. *See Council Proposal for a Council Decision on the Conclusion of the Agreement between the European Union and Australia on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs and Border Protection Service*, COM (2011) 281 final (May 19, 2011).

3. The Goal of Multilateralism: The Development of Global PNR Instruments

The ultimate strategic aim of the European Commission is the move from the conclusion of bilateral PNR agreements between the European Union and third states to the adoption of global instruments in the field. The Commission in its communication invites the European Union to consider initiating discussions with international partners that use PNR data and those that are considering using such data, in order to explore whether there is common ground between them for dealing with PNR transfers on a multilateral level. The move towards multilateralism is justified as follows:

> As more and more countries in the world use PNR data, the issues arising from such use affect the international community. Even though the bilateral approach which has been adopted by the EU was the most appropriate one under the circumstances and seems to be the most appropriate one for the near future, it risks ceasing to be appropriate if many more countries become involved with PNR. The EU should therefore examine the possibility of setting standards for the transmission and use of PNR data on an international level. The Guidelines on PNR access that have been developed by ICAO in 2004 offer a solid basis for the harmonisation of the modalities of transmissions of PNR data. However, these guidelines are not binding and they deal insufficiently with data protection issues. They are therefore not sufficient in themselves, but should rather be used for guidance, especially on matters affecting the carriers.[255]

If the Commission's strategy bears fruit, we will have moved from a unilateral model of surveillance (the post-9/11 U.S. model) to a multilateral acceptance of this model in principle via the efforts of the European Union. In an era where PNR collection and transfers are a reality, the Commission's move towards multilateralism may have the advantage of strengthening the position of the European Union as a global actor in criminal and security matters, while at the same time promoting a global system of PNR collection, transfer and exchange that will be governed by a high level of fundamental rights safeguards—after

255. *Transfers of PNR*, *supra* note 249, at 10.

all, the European Union is under the duty, after Lisbon, to promote its internal values (including respect for the rule of law and fundamental rights) in external relations.[256] However, the move from the unilateral to the multilateral (via bilateral convergence) signifies that the heavily securitized post-9/11 approach consisting of maximum and generalized surveillance of everyday life via the monitoring of movement is here to stay.

CONCLUSION

Globalization has presented significant challenges to the state in terms of how to maintain the integrity of its border and control who enters its territory. As Saskia Sassen has noted, the border is now "embedded in the product, the person, and the instrument: a mobile agent endogenizes critical features of the border . . . there are multiple locations for the border, whether inside firms or in long transnational chains of locations that can move deep inside national territorial and institutional domains."[257]

This Article has attempted to demonstrate that this movement of the border in multiple locations (including both outside and inside of the physical territorial border) has resulted in the strengthening, rather than the weakening, of the state. The reach of the state has been extended considerably, both in terms of its powers over the individual and in terms of its territorial reach. The sphere of substantive criminal law has been expanded to include global, new offenses (such as trafficking and smuggling of human beings); state databases have been extended and interlinked, containing both more (and increasingly stemming from legitimate, everyday transactions) and more sensitive (in the form of biometrics) personal data; the securitization of movement has meant that state intervention has been extended from immigration control of third-country nationals to the generalized surveillance of foreigners and citizens alike; the state is supported in its control functions by both the private sector and specialized agencies and databases; it is also supported by third countries and exercises control beyond its physical border, extraterritorially. In this manner, state power is increasing while state responsibility is diminishing: enforcement action is not "state" action, but action by a private company, an agency, an IT system; enforcement action is not

256. *See* Valsamis Mitsilegas, *Transatlantic Counter-Terrorism Cooperation After Lisbon*, 2010 EUCRIM 111.

257. SASKIA SASSEN, TERRITORY, AUTHORITY, RIGHTS: FROM MEDIEVAL TO GLOBAL ASSEMBLAGES 416 (2008).

undertaken within the territory of the state, but outside its jurisdiction (on the high seas, in the territory of a third state).

The implications of this strengthening of the state for the affected individuals are considerable. Access to asylum is seriously impeded by making it extremely difficult for third-country nationals to reach the territory where they can lodge a claim; the emphasis on risk assessment increases the risk of discrimination; the collection, storage, and use of everyday, sensitive personal data challenges the rights to private life and data protection; immigration law is also used for citizens and criminal law to regulate immigrant flows; citizens and companies are asked to assume enforcement functions and to cooperate with the state to keep out undesired individuals; extensive and routine risk assessment of persons undertaking everyday, legitimate activity (i.e., travel or mobility) is justified on the grounds of convenience and inclusion (for the "trusted traveler"). In challenging fundamental rights and citizenship in this manner, immigration control in an era of globalization weakens the citizen. This weakening is exacerbated by the gaps in legal protection and accountability arising from the fact that the expansion of the reach of the state has not been accompanied by the development of detailed legal rules and safeguards regulating this expansion. Courts, most notably in Europe, have started to address this rule of law deficit. In the absence of detailed rules setting limits to the power of the state in this context, legal certainty and the protection of the individual leave much to be desired.