Symbol of Freedom: ATSA and International Efforts to increase Security

Valerie Kraml
I. Introduction

Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy... we should champion privacy even when we have nothing to hide.

Bruce Schneier The Eternal Value of Privacy, 2006

On September 11, 2001, foreign terrorists hijacked and flew American jetliners into buildings in New York and Washington D.C., causing widespread destruction. In the aftermath, the U.S. experienced an aviation security awakening, marked by a drastic shift in how the U.S. approach and negotiate security issues within the modern aviation system. As the world becomes more technologically and socially connected, security has become an increasingly complex domestic concern. In particular, domestic efforts to ensure security require some modification or reduction of individual rights. Following the September 11th ("9-11") terrorist attacks, the U.S. has struggled with balancing differing standards of individual rights with domestic security in an increasingly international airline industry.

As the world becomes more interdependent, and threats to
security grow, there is a rising need for international cooperation to battle security threats.¹ Efforts to build international agreements, however, are balanced against domestic laws protecting individual rights. Notwithstanding their shared emphasis on individual rights, the U.S. and the EU have taken very different approaches to the protection of individual rights within the context of international and domestic security. ²

The U.S. and EU share a similar need for state security and both maintain strong protections for individual privacy. However, this note argues that in the dichotomy between state security and data privacy rights, the U.S. and EU maintain opposing views. In the U.S., state security acts as a catch-all: Once the government claims the need for state security, it will trump domestic privacy rights. By contrast, in the EU, the privacy rights are given more protection and the government has a higher burden to meet in order to trump individual rights. This note argues that the relative importance and protections afforded to privacy rights impacts the ability of domestic governments to negotiate successful international agreements that increase domestic and global state security.

This note will explore and address these different approaches within the context of the 2001 Aviation and Transportation Security Act ("ATSA"),³ which requires the collection and transfer of airline passenger personal data. First, this note analyzes the history and the extent of U.S. and EU privacy laws as they relate to airline passenger data transfers and collection. Second, it examines efforts by the U.S. and EU to come to an agreement for the transfer of passenger data within the context of differing domestic privacy requirements and laws. Finally, it explores the tensions between U.S. and EU legal values and how different concepts of individual rights, as they relate to personal privacy, affect international treaty creation.

---


To that end, Part II of this note will briefly detail the evolution of the ATSA with a focus on U.S. and EU efforts to comply. Part III addresses the theory of conflict and how states balance between individual privacy rights and efforts to increase state security. Part IV will focus on EU privacy laws, as detailed in EU Directive 95/46/ED ("the Directive"), which the EU ratified in 1995. Also known as the Data Protection Directive, the Directive outlines the nature and the extent of individual data privacy rights within the EU and limitations on data transfer to third-party countries. Part V will examine U.S. privacy laws as they relate to individual passenger data privacy, with a special focus on the post 9-11 reduction of passenger privacy rights and the emergence of class action lawsuits against airlines. Part VI will compare U.S. and EU approaches to privacy laws and security. Part VII applies these different approaches and details efforts made by both the U.S. and the EU to come to an ATSA agreement, including some of the political problems that both sides faced. The focus will be on the tension between the U.S. and EU regarding the conceptualization of individual rights and how it affected the parties' acceptance/rejection of this international agreement. In Part VIII, this note will explore how domestic politics are able to undermine valid international treaties and laws and explore possible avenues for effective negotiations.

II. ATSA: Basic Overview of Law and Conflict

Believing that stronger intelligence, agency communication, and shared data collection would have provided adequate notice of the 9-11 attacks, the U.S. legislature passed the Aviation and Transportation Security Act in 2001. The ATSA created and empowered the Transportation Security Administration ("TSA") to

---


5. ATSA, supra note 3.
make numerous industry changes to maximize domestic security. 6
In particular, the TSA is charged with evaluating all passengers
boarding an aircraft using a computer-assisted passenger
prescreening system ("CAPPS").7 Using its broad authority, the
TSA requires that all domestic airlines provide Passenger Name
Records ("PNR") prior to boarding.8 PNRs are the "reservation
information contained in an air carrier's electronic reservation
system and/or departure control system that sets forth the identity
and travel plans of each passenger."9

Of particular importance within the international realm was the
ATSA's amendment to §44909,10 which required that all foreign
airlines flying to or over American territory to electronically provide
PNRs to the U.S. Commissioner of Customs.11

Under the ATSA, all foreign crew and passenger manifests
must contain:

- The full name of each passenger and crew member;12
- The date of birth and citizenship of each passenger and
  crew member;13
- The sex of each passenger and crew member;14

6. The ATSA heightened domestic security measures by: 1) requiring federal
agencies to increase screening of airport perimeters, planes, passengers, and
baggage; 2) requiring that secure doors be installed in all aircrafts between the
flight deck and passenger compartments (§ 44903); 3) requiring crew training in
terrorism identification and security measures (§ 44918); 4) limiting the ability of
foreign nationals and/or aliens or other designated individuals to obtain flight
training for crafts exceeding the 12,500-pound take-off weight (§ 44939).

7. See ATSA, supra note 3, § 44903(j)(2).

8. 19 C.F.R. 122.49b(c) (2004). In addition to ATSA requirements, Air carriers
must disclose thirty-four items including: date of reservation, date(s) of intended
travel, passenger name, number of travelers, seat information, address, payment
information, billing address, telephone numbers, frequent flyer information, travel
agency, travel status of passenger, one-way ticket or free ticket identifiers, email
address, ticket number, date of issuance, no show history, number of bags, bag tag
numbers, voluntary/involuntary upgrades, and date of birth. Undertakings of the
United States Bureau of Customs and Border Protection and the United States

10. ATSA, supra note 3, § 115(c)(5).
11. Id. § 115(c)(1).
12. Id. § 115(c)(2)(A).
13. Id. § 115(c)(2)(B).
14. Id. § 115(c)(2)(C).
The passport number and country of issuance for each passenger and crew member, if required for travel;¹⁵

The U.S. visa number or resident alien card number for each passenger and crew member, as applicable;¹⁶

Any "other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to secure aviation safety."¹⁷

As with domestic PNRs, the ATSA requires that all foreign air carriers entering or leaving the U.S. provide the Bureau of Customs and Border Protection ("CBP") and the U.S. Department of Homeland Security ("DHS") with electronic access to PNRs.¹⁸

Specifically, CBP may electronically access the PNR data from air carriers' reservation systems located within the territory of the Member States of the EU.

III. Rights vs. Security: the Theory of Conflict

Compliance with the ATSA requirements is a contentious issue between the U.S. and EU members primarily due to differences in how the U.S. and EU balance individual rights versus state security. Compared to the U.S., EU countries have stronger enumerated individual data privacy rights. Thus, it was questionable whether the European airlines could comply with ATSA requirements without violating EU's own privacy laws. Within the EU, data privacy and transfers are governed by the Directive, which mandates strong protection of individual privacy rights and limited governmental access. European airlines were in a dilemma: either they could transfer passenger data in compliance with U.S. law and be subjected to EU penalties,¹⁹ or they could refuse to transfer

¹⁵. Id. § 115(c)(2)(D).

¹⁶. Id. § 115(c)(2)(E).

¹⁷. Id. § 115(c)(2)(F).


¹⁹. Council Directive, supra note 4, art. 2. Directive 95/46 allows member states to set their own conditions, minimum requirements, and penalties against those who are "the natural or legal person, public authority, agency or any other body which alone or jointly . . . determines the purposes and means of the processing of personal data." See also Arnulf S. Gubitz, The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the EU Data Protection Laws: How Much Access to
passenger data per the ATSA and face U.S. imposed fines or the revocation of landing rights within the U.S.\textsuperscript{20}

Maintenance of national security, especially in the face of global threats, is an essential element of state preservation and sovereignty. Tensions often exist between respecting individual rights and freedoms and ensuring the preservation of the state. State efforts to ensure sovereignty and security require the implementation of measures - in terms of laws, regulations, and sanctions - that necessarily restrict the rights and freedoms of individuals. Finding the balance between individual rights and state security is often difficult; restrictive state actions are often criticized as violating the rule of law, lacking sufficient checks and balances, and encompassing unnecessary or dangerous restrictions on constitutional rights.\textsuperscript{21} Thus, increases in state security usually result in a reduction or limitation of individual liberties.\textsuperscript{22}

Following the passage of the ATSA, questions arose regarding the role of state encroachment onto individual rights, especially as they relate to privacy. These questions are whether individual rights and freedoms should be restricted, and whether the restrictions can be justified for the sake of national security.

Following the 9-11 terrorist attacks, the U.S. "awoke to the growing threat posed by terrorist organizations with global reach and the probability of additional terrorist attacks on U.S. soil."\textsuperscript{23} It


21. For instance, violations of individual privacy such as censorship, mass surveillance, and wiretapping can be justified as necessary for national security purposes. See, e.g., Electronic Privacy Information Center, The USA PATRIOT Act, http://epic.org/privacy/terrorism/usapatriot (last visited Feb. 17, 2009).

22. See e.g., Security and Human Rights (Benjamin J. Goold & Liora Lazarus eds., Hart Publishing 2007). There has been a new wave of research and discourse arguing that the state security/human right dichotomy is both inaccurate and unhelpful. Researchers, NGOs and non-profits have been arguing that state security can exist within the confines of both protecting and promoting human rights. The theory is that human security [which combines state security and human elements] is something that can be promoted by the state, within the confines of state security, and while maximizing human liberties. For more information, see Asia-Pacific Politics: Hegemony vs. Human Security (Joseph Camilleri et al. eds., Edward Elgar, Cheltenham 2007).

was quickly realized that national security required broad and effective engagement in the international arena:

No longer an abstract concept about conflicts fought in far-away lands, [U.S.] national security now includes safeguarding our public spaces, our economic infrastructure, our transportation and information networks and our public confidences. Because American infrastructure interconnects industry, public services and private citizens, an attack on a single point causes a ripple effect for all Americans ... [thus making] our government's central role... the collective security of the American people at home.

With this, a "domestic/global security state" has begun to emerge to "reduce the vulnerability of people and complex systems to catastrophic disruption and destruction through intentional and accidental acts." The "domestic/global security state" evolved with the increase in international interdependency and events that impact the domestic state. The domestic security state, which developed out of both real and perceived internal threats to the nation, is evolutionary in that it is rooted in the American system of government, which emphasizes and responds to changes in constitutionalism, liberty, separation of power, due process, equal protection, and individual rights. However, regardless of its evolutionary ability, the domestic security state is unable to combat the threats of terrorism that are increasingly rooted in other countries. As the world becomes more globally interconnected through economies, technology, and culture, the fight for domestic security must necessarily include global security concerns.

25. Howard et al., supra note 23.
27. Id. at 73.
29. See generally PETER BERGER & SAMUEL HUNTING, MANY GLOBALIZATIONS (Oxford Press 2002). See also Audrey Cronin, Behind the Curve: Globalization and
The "domestic/global security state" depends largely on improved and advanced intelligence gathering, which impacts domestic individual rights. It has been generally recognized that defense, foreign policy intelligence, and domestic intelligence are governed by different cultures, principles, laws, regulations, and processes. But, to address international terrorism, there must be a convergence of defense and domestic intelligence. Defense intelligence can be of "crucial significance for domestic action and vice versa." Consequently, new rules, principles, and methods of information gathering and sharing need to be developed to facilitate information sharing. The "domestic/global security state" engages in information gathering that must be balanced against domestic individual rights, such as privacy rights, which often come into conflict with domestic and international efforts to ensure security. As a result, through differences in case law and statutes, the U.S. and EU have taken very different approaches to the protection of individual privacy rights within the collection, storage, and transfer of personal data. The following sections highlight these differences.

IV. EU Data Privacy Laws

The EU has a rich history of protecting and respecting individual's data privacy rights. On December 10, 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights. These rights were formulated in response to the horrors of World War II, where among other things personal

---

30. Carroll, supra note 26, at 78.
31. Id.
32. This need has been recognized by the government. See generally US General Accounting Office, Testimony of David M. Walker to the Senate Committed on Intelligence, Homeland Security Information Sharing Activities Face Continued Management Challenges (Sept. 23, 2002).
33. Carroll, supra note 26, at n. 4. See generally statements of Robert S. Mueller, FBI Director, projecting that the FBI will become "part of an official international terrorism alliance similar to NATO." Furthermore, he "envisioned the FBI of tomorrow as a highly trained, electronically sophisticated, internationally networked organization that has terrorism as its principal target... Soon all counterterrorism functions will be intelligence-driven operations with law enforcement sanctions as an ancillary aspect."
information, which was initially collected for innocent purposes, became a "tool of oppression in the hands of a powerful government." Under Article 12 of the Declaration, individual privacy was protected against "arbitrary interference" by the government.

Over the next thirty years, the need for regional guidelines to harmonize amongst national data protection legislations became increasingly necessary. Efforts to harmonize domestic laws, and thereby reduce trade disputes throughout Europe, began with the Organization for Economic Cooperation and Development ("OECD") (formerly the Organization for European Economic Cooperation (OEEC) under the Marshall Plan). The focus of the OECD was to "develop Guidelines which would help to harmonize national privacy legislation and, while upholding such human rights, at the same time prevent interruptions in international flows of data."

Efforts to further protect individual data privacy, especially following the OECD Guidelines, was furthered by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("APPD"). Under the APPD, individual data was protected from arbitrary and indiscriminate collection and third-party or transborder transfer.

As mentioned above, the EU ratified the Directive in 1995. The main goals of the Directive were to ensure the unrestricted movement of personal data among member states while


36. Id.


40. Id. arts. 5, 6, and 8.
simultaneously protecting individual rights via a high level of protection of personal data within the EU. Because directives provide only guidelines and are not binding, the Commission remained concerned about data security due to differences in domestic laws within EU member states. Since the Directive was subject to member state review, some states took a very strict approach to third party data transfers, while others were more relaxed.

A. Requirements and Protections under the Directive

The Directive provides ground rules for individual data privacy and applies to both electronic and paper filing systems. It begins by laying down basic privacy principles, starting with the idea that data information should be collected for specific, legitimate purposes, stored no longer than necessary, and further protected upon transfer to third party countries. The goal is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" while also bolstering the "free flow of personal data."

Under Section 6 of the Directive, member states - and the controller specifically - are required to ensure the fair, accurate, lawful, and legitimate storage and transfer of individual data. Specifically, all personal data must be 1) "processed fairly and lawfully"; 2) collected for "specified, explicit, and legitimate purpose" and not processed in ways incompatible with this purpose unless "appropriate" domestic safeguards are utilized; 3) "adequate, relevant, and not excessive in relation to the purpose for which [it] was collected/processed"; 4) accurate (with inaccurate or incomplete data being erased or rectified); and 5) kept and stored in a manner that permits identification of individuals for "no longer

42. Id. at 10 (stating that "the implementation of a Directive of this kind, that is a Directive leaving a considerable latitude to the Member States, but also requiring them to fill in a significant amount of detail, is undoubtedly a complex task.").
43. Id. at 11.
45. Id. arts. 1 & 2.
46. See supra text accompanying note 19.
than necessary for the purposes for which the data was collected." 47

Any collection of private data requires unambiguous individual consent unless the data falls within one of several explicit exceptions. 48 Although the controller does not need consent, they do need to provide disclosure to the individual whose information is being collected when data processing is necessary for the following reasons: 1) the performance or entrance of a contract; 2) the controller to comply with their legal obligation; 3) protecting the vital interests of the data subject; 4) the performance of a task carried out in the public interest or within the exercise of official authority vested in either the controller or designated third party; 5) legitimate interests pursued by the controller or third party. 49 Even within these narrow exceptions, the individual retains the right to contest the collection and the transmission of their private information for any legitimate reason. 50

Under Section 3, Article 8, special safeguards are instituted for the collection and transmission of sensitive passenger data, such as race or ethnic origins and religious or political affiliations. Overall, member states are prohibited from "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." 51 The Directive made an explicit exception for the processing of personal data obtained and used to further "public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law." 52 However, even within this exception, any collected data must be narrowly-related to the reason collected and strict retention guidelines are ensured. 53 As such, the collection and transmission of personal data can only occur on a case-by-case basis when supported by informed and legitimate suspicion. 54

47. Id. art. 6
48. Id. art. 7 (a).
49. Id. art. 7 (b)-(f)
50. Id. arts. 7 (f) & 14.
51. Id. art. 8(1).
52. Id. art. 3(2).
54. "Member States shall provide that personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Id. art. 6(1)(b).
B. Data Transfers to Third-Party Countries

Article 25 of the Directive enables EU member countries and controllers, such as airlines, to transfer individual data to third party countries. However, data can only be transferred once it is determined that the third-party has an "adequate level of protection" of the private information. This requires a case-by-case determination of the nature of the data, the purpose and duration of the operation, the country of origin/destination, utilized rules of law and profession, and security measures employed within the third country. Similar to Article 7, Article 25 of the Directive makes an express exception, even without an adequate level of protection, that allows data transfers to a third country to fulfill a contract in which the data subject is a party.

If a third country fails to meet an adequate level of protection, member states will act to prevent any transfer of that type of data to the third party. The European Commission and member countries then have the ability to negotiate with the third country to remedy any breach of privacy and work to reinstate the flow of information upon the showing of adequate protection of "the private lives and basic freedoms and rights of individuals." Negotiations are undertaken either to bring the third country into an agreement to comply with the Directive or to convince the third country to modify their domestic laws.

In order to better identify and negotiate with third countries, the European Commission set up the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party." The Working Party has the "power to determine, on the basis of Article 25(6) of the Directive whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into." The Working

55. Id. art. 25.
56. Id. art. 25(1).
57. Id. art. 25(2).
58. Id. art. 25.
59. Id. art. 25(4).
60. Id. art. 25(5)-(6).
61. Id. art. 25(4)-(5).
Party has determined that "personal data can flow from the twenty-five EU member states and three EEA member countries (Norway, Liechtenstein and Iceland) to a third country without any further safeguard being necessary." In addition, limited data has been approved for third party transfer to the U.S. as long as the data falls under the safeguards of the U.S. Department of Commerce's Safe Harbor Privacy Principles.

V. U.S. Data Privacy Laws

Unlike the EU, the U.S. has no comprehensive privacy law. Although courts have interpreted the U.S. Constitution as providing unenumerated privacy rights, the scope and extent of these rights are unclear and are explored on a case-by-case basis. The basic right to privacy received explicit discussion in Griswold v. Connecticut, where the U.S. Supreme Court first recognized that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance" which give individuals a right to privacy. The right to privacy has been explored in a number of other cases following Griswold.

However, the strongest indicator of U.S. privacy rights is found not in case law, but in statutes. Generally, American personal data collection and transfers are regulated by the Privacy Act of 1974, the Electronic Communications Privacy Act of 1986 ("ECPA"), and the 2002 Freedom of Information Act ("FOIA"). These laws have been interpreted as limiting actions of the government, but not

---

63. Id.
64. Id.
68. It should be noted that other privacy bills, such as the Personal Information Privacy Act of 2001 and Defense of Privacy Act, were introduced in Congress with the goal of strengthening personal privacy rights, but they were never enacted into law.
necessarily those of private industries or businesses.\(^69\)

\section*{A. Privacy Case Law}

Although the U.S. Supreme Court has not addressed the dichotomy between state security and individual privacy law, lower courts have recognized broad powers of the state to maintain security in the face of global threats.\(^70\) To the same degree, courts have recognized a strong individual right to privacy. There is a dearth of case law examining the intersection between state security measures and individual privacy rights.

Courts have interpreted the U.S. Constitution and case law to grant individual protection from governmental intrusion. However, in terms of privacy, the strongest protections have been toward individual rights enumerated in the Bill of Rights.\(^71\) The foremost case addressing the scope of individual privacy is \textit{Griswold v. Connecticut}, where the court held that the "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance [and these] [v]arious guarantees create zones of privacy."\(^72\) Moreover, \textit{Griswold} explained:

Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his

\(^69\) See, e.g., Drew Shenkman, Comment, \textit{Flying the Not-So-Private Skies: How Passengers' Personal Information Privacy Stopped at the Airplane Door, and What (If Anything) May Be Done to Get It Back}, 17 Alb. L.J. Sci. & Tech. 667 (2007) (outlining class action attempts against airlines for privacy violations and the inability of class action claims to succeed).


\(^71\) See supra note 66. (Griswold as constitutionally protecting individual privacy rights).

\(^72\) Griswold, 381 U.S. at 481.
detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." 73

The Court went on to argue that each of these Bill of Rights guarantees had an underlying theme of individual privacy 74 that ensured an unenumerated privacy right against the state's need for safety and security. Accordingly, the Court has stated that [e]ven though the governmental purpose is legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved." 75

This discussion was furthered in Roe v. Wade, where the Supreme Court extended the right to privacy to protect against encroachment, not only by the federal government, 76 but also by state governments. 77 In Roe, the Court stated that the Due Process Clause of the Fourteenth Amendment protects against state actions that violate an individual right to privacy. 78 Although the Roe Court does not recognize an unfettered right to privacy, 79 they did recognize that the "right of personal privacy, or a guarantee of certain areas or zones of privacy, exists under the Constitution." 80

In order for the state to validly infringe on these zones of privacy, the state must have a "compelling" interest in the regulated activity that is narrowly tailored to achieving a legitimate state end. 81 The

73. Griswold at 484.

74. Id. (stating "The right of association contained in the penumbra of the First Amendment is one. The Third Amendment in its prohibition against the quartering of soldiers in any house in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. The Fifth Amendment in its self-incrimination clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides that the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.")


76. See supra note 66. (Griswold which only addressed the right to privacy against the federal government and did not address the role of states or the Fourteenth Amendment).

77. Roe, 410 U.S. at 147-67.

78. Id. at 153.

79. Id. at 155.

80. Id. at 152.

81. Id. at 155-56. See also Kramer v. Union Free School Dist., 395 U.S. 621, 627
state interest is necessarily balanced against the individual right.\textsuperscript{82} This standard places a high burden on the state to show that its reason for limiting individual privacy is based on more than a slight or even important reason.

\textit{Roe} identifies a strong individual right to privacy that is protected from overarching or expansive regulations, by either the federal or state government, that are not narrowly tailored and based on a compelling state interest. In applying this standard to the ATSA, it is clear that state security and protecting society against terrorism is a compelling governmental interest. However, there are questions as to whether the ATSA, which requires a broad and unfettered access to \textit{all} passenger data as opposed to limiting data collection to some of the more high-risk passengers, is narrowly tailored enough to justify governmental intrusion on individual privacy rights.

B. Privacy Statutes

In accordance with the Supreme Court’s constitutional recognition of individual privacy rights, Congress has enacted statutes that guide and limit the ability of the government to collect, store, and transfer personal data. As mentioned above, the Privacy Act of 1974, the ECPA, and the FOIA\textsuperscript{83} have been the main U.S. laws governing the use, collection, and transfer of data by third parties. Although these laws intended to strengthen personal data privacy rights, in actuality, they have provided lenient access to a great number of governmental and private agencies. As a result, individual passenger privacy rights in the U.S. are weaker than those in the EU

C. The Privacy Act of 1974

The Privacy Act of 1974 was instituted because “[t]he Bill of Rights guarantees to each American protections which we equate with specific rights of citizenship in a free society [and] [t]his legislation is a major first step in a continuing effort to define the ‘penumbra’ of privacy which emanates from specific guarantees in

\textsuperscript{82} \textit{Roe}, 410 U.S. at 155-56.

the Bill of Rights and which helps to give them life and substance as recognized in *Griswold.*"  

The purpose of the Privacy Act was two-fold. First, it was intended to protect personal information from government agency access and to enable individuals to review and correct agency information. Under the Act, governmental agencies were prohibited from transferring personal and private information to third parties without the individual's consent, except for twelve explicit exceptions. These exceptions, however, were quite broad and allowed many different agencies and people to access a person's data without their consent. For instance, private data could be transferred for census and statistical data keeping, upon the request of law enforcement or any other agency on a "need to know" basis, for debt collection, and individual "health and safety." The most controversial exception is that for "routine uses," which under subsection (a)(7) is defined as any use "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." Congress intended that "routine uses" would "permit other than intra-agency disclosures" and that therefore "[i]t is not necessary . . . to include intra-agency transfers in the portion of the system notice covering routine uses." As such, Congress provided no strong prohibitions or limitations on the transfer of personal data under the Privacy Act and many different agencies and people are able to gain access to a person's data without their consent.

---

86. Id. § 552a(b).  
87. Id. § 552a(b)(4).  
88. Id. § 552a(b)(5).  
89. Id. § 552a(b)(7).  
90. Id. § 552a(b)(1).  
91. Id. § 552a(b)(12).  
92. Id. § 552a(b)(8).  
93. Id. § 552a(b)(3).  
95. "Of particular import with regard to interpretation of the Privacy Act is the absence of any formal conference report by a conference committee. Normally, after the conferees have reached an agreement on all proposed amendments, their recommendations are incorporated in a report which is signed by a majority of the
D. The ECPA

The ECPA was enacted in 1986\textsuperscript{96} in response to public concerns over electronic privacy. The ECPA was as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968\textsuperscript{97} (the "Wiretap Statute") in order to prevent unauthorized governmental access to private electronic communications.\textsuperscript{98} The ECPA regulated domestic surveillance and was separated into three areas: the Wiretap Act, the Pen Register Act,\textsuperscript{99} and the Stored Communications Act.\textsuperscript{100}

The Wiretap Act bars the intentional use, interception, or disclosure of electronic or wire communication without an applicable exception.\textsuperscript{101} It allows companies and the government to monitor communications in order to "combat fraud and theft of service."\textsuperscript{102} This monitoring must be reasonable, and not

\textsuperscript{96} ECPA, 18 U.S.C. § 2510 (Oct. 21, 1986).
\textsuperscript{97} 42 U.S.C. § 3711 (1968).
\textsuperscript{102} United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). See also U.S. Patriot Act, supra note 101, § 2511(2)(a)(i) (2006) (permitting "an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire
continuous,\textsuperscript{103} so that it balances the need for security with the protection of individual privacy rights in their communications.\textsuperscript{104} As a result, providers are unable to provide the government evidence of crimes that are unrelated to the provider's particular right or property.\textsuperscript{105}

The Stored Communications Act ("SCA") regulates the storage of electronic data and communications, such as emails and other transfers of data between private parties.\textsuperscript{106} The SCA was intended to prohibit a provider "from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient."\textsuperscript{107} Under the SCA, it is an offense for a governmental official to "intentionally access[] without authorization a facility through which an electronic communication service is provided" or to "intentionally exceed[] an authorization to access that facility; and thereby obtain [an] electronic communication while it is in electronic storage in such system."\textsuperscript{108} With the passage of the U.S. Patriot Act in 2001, some of the SCA provisions were expanded to allow the government to conduct domestic surveillance.\textsuperscript{109}

\textbf{E. The FOIA}

Under the FOIA, any individual, regardless of country of residence, had the right to request access to federal agency records or information unless protected from disclosure pursuant to an

\textsuperscript{103} United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976) ("This authority of the telephone company to intercept and disclose wire communications is not unlimited.").

\textsuperscript{104} See United States v. Harvey, 540 F.2d 1345, 1351 (8th Cir. 1976) ("The federal courts . . . have construed the statute to impose a standard of reasonableness upon the investigating communication carrier.").

\textsuperscript{105} Id. at 1352.


\textsuperscript{107} S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3591. See also Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003) (stating that SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility").

\textsuperscript{108} See supra note 106, § 2701(a)(1)-(2).

\textsuperscript{109} U.S. Patriot Act, supra note 101. See also ACLU v. Ashcroft, 542 U.S. 656, 666 (2004) (holding that it is constitutional under the First and Fourth Amendments for the FBI to compel certain service providers to disclose customer records).
exemption or exclusion. A federal agency can legally withhold an individual’s record or information where the information is authorized “to be kept secret in the interest of national defense or foreign policy.” This is especially true when the record contains trade secrets, commercial or financial information, personnel files, or medical files. In addition, an individual’s records may be withheld if they were compiled by law enforcement, would endanger lives, expose an informant, detail agency functioning, invade personal privacy, or interfere with an individual’s right to a fair trial. Courts have also allowed agencies to withhold information when producing such information would lessen the ability of the government to obtain “necessary” information in the future.

F. U.S. Privacy Laws: Security over Individual Rights

In comparison to the EU’s strong personal and data privacy laws under the Directive, the U.S. is considered to have inadequate protection for personal data. Currently, the ECPA, FOIA, and Privacy Act of 1974 still govern the bulk of U.S. passenger data storage and collection. Congress intended these laws to strengthen individual privacy rights; however, the courts have interpreted the legal language to allow broad access to individual data.

A common theme throughout each of these laws is that the governmental need for security trumps individual privacy rights. This is evident in the Privacy Act of 1974, which was passed specifically to help define the penumbra privacy set forth in Griswold. The consent exception for “routine uses” has been the most litigated exception under the Privacy Act. The courts have given an agency’s interpretation of “routine uses” a great deal of deference. Various types of individual data transfers have been

110. See supra note 85, § 552 (b)(1)(A).
111. Id.
112. Id. § 552 (b)(4).
113. Id. § 552 (b)(6).
114. Id. § 552 (b)(7)(A-F).
117. See Dep't of the Air Force, Scott Air Force Base, Ill. v. FLRA, 104 F.3d 1396,
upheld by the courts under the Privacy Act, many of which have to do with agency investigations and security measures.\textsuperscript{118}

The ability of governmental security measures to trump individual privacy rights, especially as it relates to disclosure of data, is also evidenced in the court's approach to the FOIA protections. The Court has stated that "[t]he government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service."\textsuperscript{119} As such, deference is given to domestic security agencies when deciding not to provide requested data in compliance with FOIA requirements. "The appearance of confidentiality would hardly be enhanced if sources and future sources were to learn that their safety, and often their lives, was to depend upon judicial oversight."\textsuperscript{120}

Deference is similarly given to the protections afforded by the ECPA. Recently, airline passengers brought class action suits claiming that U.S. airlines violated ECPA data privacy restrictions. Specifically, JetBlue Airways,\textsuperscript{121} American Airlines,\textsuperscript{122} and Northwest Airlines\textsuperscript{123} have been involved in class action litigation

\begin{flushleft}
1402 (D.C. Cir. 1997); FLRA v. United States Dep't of the Treasury, 884 F.2d 1446, 1455-56 (D.C. Cir. 1989).


asserting that they transferred PNRs to third party companies and government entities. According to the plaintiffs, the ECPA applied because the airlines were transferring electronically stored PNRs without passenger consent.\textsuperscript{124} In each of the cases, the lower courts dismissed the complaints prior to trial. As such, it is still unclear as to whether the ECPA can be applied to airlines' electronic data and, if so, what remedies are appropriate.\textsuperscript{125}

The status of the airline passenger class action cases shows the deference courts give to governmental agencies when determining the scope of American's unenumerated privacy rights. In the drafting of each of these laws, individual privacy rights are often trumped by any governmental need for security. This standard is followed by the courts, which have been quick to give deference to governmental security efforts by allowing governmental wiretapping and granting immunity to companies that illegally transfer third party data to the government even if they violate statutorily protected privacy rights. When state security is at stake, the courts have not granted individual citizens any redress for the violation of their right. This enables the impermissible transfer of personal data to continue without any reasonable regulation by the government or checks by the courts.

\textbf{VI. Differences in Domestic Privacy Laws}

The U.S. and the EU are similar in their focus on domestic and global state security and in maintaining strong privacy protections for individual data. However, despite shared interests, fundamental differences arise during state efforts to apply their domestic laws and standards toward an international agreement. In terms of the ATSA, increased threats to domestic and global state security have resulted in collective and large-scale information gathering. The collection and analysis of individual traveler's data, however, necessarily intrudes on their personal property. Thus, the state is forced to balance between maintaining state security and protecting individual data privacy.

In passing the ATSA, the U.S. committed itself to preserving domestic and global state security over individual privacy rights.

\textsuperscript{124} In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d at 306.
\textsuperscript{125} See, e.g., supra note 67.
Following 9-11, the U.S. has been more domestically focused on maintaining state security. As shown in Roe and Griswold, the government is permitted to trump individual privacy rights when faced with a compelling governmental interest that is narrowly tailored toward the state goal. Here, the governmental interest in state security, especially as it relates to air traffic, is highly compelling. The question becomes whether the personal data fields demanded under the ATSA are narrowly tailored enough to meet the requirements of the Supreme Court. It can be argued that much of the data sought, such as meal preferences or seat assignments, are not, on their own, strong predictors as to whether an individual traveler is a terrorist. However, U.S. intelligence agencies argue that having all the data allows them to more effectively anticipate the risks posed by individual passengers. Thus, in light of the domestic laws regarding individual privacy along with the civil cases regarding air travel, this may be sufficient for the courts to hold that the ATSA is sufficiently narrow to warrant intrusion into individual privacy.

For the EU, however, finding a balance between state security and individual data privacy is more difficult due mostly to a different tradition of privacy laws and safeguards. The EU statutes place a different balance on state security and individual privacy. Like the U.S., the EU is highly dedicated to maintaining state security; however, it must occur within the context of protecting individual privacy and data. As discussed in Section II, both Section 6 and 8 of the Directive require that all personal data must be collected and safeguarded, even upon transmission to a legitimate third party, for "specific, explicit, and legitimate purposes"\textsuperscript{126} and is retained for only a specific and limited time period. In addition, the collection of sensitive passenger data, such as race, religion, or political affiliations, is prohibited unless it is for public security, defense, or state security purposes, is "narrowly related to the reason [the data is] collected [and] strict retention guidelines are ensured."\textsuperscript{127} Thus, under EU law, the collection and transmission of personal data must be supported by informed and legitimate suspicion.\textsuperscript{128}

Moreover, the collection and retention of individual data fields

\textsuperscript{126} Council Directive, supra note 4, art. 6.
\textsuperscript{127} Id.
\textsuperscript{128} Id. art. 6(1)(b).
under the ATSA is neither specific nor narrowly tailored enough to satisfy EU law. Third party data transfers must abide by the EU's strong domestic privacy protections unless faced with a legitimate and identifiable security threat.¹²⁹ This requirement is not met through the ATSA, which requires the whole-scale collection of all passenger data, regardless of the existence of any credible threat.¹³⁰ Under EU's standard, the ATSA does not provide enough protections because there are few limiting constraints on the collection and use of sensitive data.¹³¹ For the EU, the protection of private data, unless necessitated by a legitimate security threat, trumps that of state security.¹³² This position is drastically different than that taken by the U.S. courts and legislature, which have chosen to maintain security - even when the threats are ambiguous and not credible - over individual privacy rights.¹³³

VII. ATSA and International Efforts to Bridge Different Domestic Approaches to Privacy

Even with dichotomous views on privacy, the EU and U.S. have needed to compromise to gain international compliance with important domestic laws, such as the ATSA.

A. History of Compliance

Prior to the enactment of the ATSA, the U.S. and European Commission began developing appropriate guidelines for third party transfer of personal data. In 2000, the U.S. Department of Commerce and the European Commission developed "Safe Harbor Privacy Principles" in order to facilitate data transfer within the confines of the Directive requirements.¹³⁴ Under the Safe Harbor

¹²⁹. Id. art. 13(1)-(2).
¹³⁰. See supra note 3, § 44909 (where no requirement of a threat is enumerated as a prerequisite to the collection of PNRs).
¹³³. See supra note 3, § 44909.
Principles, U.S. companies agreed to comply with and be bound by principles that fit the Directive requirements. If U.S. companies agree, they are bound to 1) provide “clear and conspicuous” notice of the purpose, use, and transfer of personal data; 2) provide individuals an opportunity to “opt out” of data transfers to third parties; 3) ensure data transfers to third parties occur only to other organizations that abide by data privacy principles; 4) take “reasonable” protections against data “loss, misuse and unauthorized access, disclosure, alteration and destruction”; 5) ensure “personal information must be relevant for the purposes for which it is to be used”; 6) allow individuals access to their personal data and correct or delete any inaccuracies; and 7) have an effective method for ensuring compliance with these principles.135

B. First International Agreement and Differing Privacy Law

Following the passage of the ATSA in 2001, the U.S. and EU began negotiating to ensure that EU airlines could comply with both U.S. law and the EU Directive. In June 2002, the U.S. Customs Service published interim rules for implementing ATSA requirements, which allowed the U.S. unfettered and unlimited access to EU passenger data. Under the interim Agreement, the U.S. could access EU records for any “legitimate law enforcement purposes” including those beyond fighting terrorism.136 Since there were no enumerated protections or limits on the access, collection, or storage of EU passenger data, the interim rules were met with extreme resistance from the European Parliament, Data Commissioners and privacy groups.137 The primary complaint was that the agreement was too broad and lacked any of the protections and safeguards necessary for compliance with the EU Directive.138 In response, the EU Working Party rejected the interim agreement and instead called for a formalized agreement that reduced the fields of data collected, excluded the collection of “sensitive” data, adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce).


137. Id.

limited data retention times, limited the data use solely to fighting terrorism, and ensured effective enforcement of passenger privacy rights.\textsuperscript{139}

Consequently, U.S. authorities postponed the application of the ATSA until February 5, 2003. However, the U.S. refused to waive the penalties imposed on airlines that failed to comply with the ATSA requirement for electronic access; thus, a number of large airlines in the EU have granted the U.S. authorities access to their PNR data.\textsuperscript{140} The EU and U.S. continued negotiations until "U.S. Deputy Customs Commissioner Douglas Browning and officials of the European Commission agreed to give the custom officials direct access to the personal data of passengers flying to, from and through the U.S."\textsuperscript{141} In exchange, the U.S. Customs Department made broad concessions\textsuperscript{142} and promised to at least "respect the principles of the Data Protection ... as long as these principles don’t stand in the way of the secret services."\textsuperscript{143} Specifically, the U.S. agreed to heightened protections and reasonable limitations on the collection of "sensitive personal data," which includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade-union membership.\textsuperscript{144} This modified agreement, known as the Passenger Name Record Deal ("PNRD"),\textsuperscript{145} was only possible after the U.S. promised to respect passenger privacy rights in accord with the EU Directive.

The PNRD was met with apprehension in the EU and, in order to address many of the concerns, the EU Working Party issued the

\textsuperscript{139} Id.


\textsuperscript{143} Id.


Working Party Opinion 4/2003.\textsuperscript{146} In the Opinion, the Working Party identified areas where the U.S. needed to improve in order to meet the adequacy standard set by the Directive.\textsuperscript{147} The EU agreed with the U.S. that "the fight against terrorism is both a necessary and valuable element of [democracy]." However, the EU does not agree that security should come at the expense of fundamental individual rights.\textsuperscript{148} The need for internal domestic security was unable to trump the privacy rights enumerated in the Directive, Article 8 of the European Convention on Human Rights, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.\textsuperscript{149} Consequently, any "limitations to fundamental rights and freedoms regarding the processing of personal data in the EU should take place only if necessary in a democratic society and for the protection of public interests exhaustively listed in those instruments."\textsuperscript{150} As such, the Working Party rejected the PNRD as insufficient and called for proportionality in all areas of U.S. data collection, storage and transfer, thereby increasing transparency, heightening protections of individual privacy rights, limiting data collection and transfer, and ensuring that the U.S. data methodologies were compatible with EU privacy laws.\textsuperscript{151}

Nevertheless, on May 17, 2004, the European Council adopted Decision 2004/496/EC ("the Council Decision"), which authorized the Council President to sign the PNRD agreement with the U.S.\textsuperscript{152} The decision to accept the PNRD was supported by the European Commission, but it was against the advice of the European Parliament,\textsuperscript{153} which argued that the PNRD violated the civil

\begin{itemize}
\item \textsuperscript{147} 2004 O.J. (L 183) 83.
\item \textsuperscript{148} See Digital Civil Rights, supra note 136, at 3.
\item \textsuperscript{149} Id.
\item \textsuperscript{150} Id. at 4; see also supra note 18.
\item \textsuperscript{151} See supra note 136, at 8-10.
\item \textsuperscript{153} See also News Release, European Parliament, Air passenger data: MEPs look
liberties of passengers under the Directive by allowing third country transfers without adequate protections.\textsuperscript{154}

The PNRD became a power struggle between the EU branches. For years, the European Parliament had been successfully asserting greater powers vis-à-vis the other two branches, namely the Council and the Commission. The PNRD lawsuit represented an effort by the Council and the Commission to gain greater powers in foreign relations.\textsuperscript{155} As such, the EU Parliament, angered by the adoption of the PNRD, challenged the authority of the Council and the Commission to render the agreement effective under internal law. The Parliament brought suit in the European Court of Justice and challenged institutional policies largely unrelated to the substance of the PNRD.

\textbf{D. European Court of Justice Strikes Down the First Agreement}

The PNRD was criticized as being without adequate legal basis. As a result, the Advocate General of the European Court of Justice called for its annulment.\textsuperscript{156} Actions for annulment were brought to the European Court of Justice, under Article 230 EC, on July 27, 2004.\textsuperscript{157} The EU Parliament challenged the PNRD claiming it was an ultravires action that breached fundamental principles of the Directive, fundamental rights, and the principle of proportionality.\textsuperscript{158}

In its ruling, the European Court of Justice focused on legal authority and did not address the privacy implications of the passenger data transfers.\textsuperscript{159} The Court addressed only the first

\textsuperscript{154} See supra note 26.


\textsuperscript{157} Id.

\textsuperscript{158} Id. at 50.

\textsuperscript{159} The Court found that based on the Directive, the PNRD concerned matters that go to the core of national sovereignty and therefore the EU was more constrained by Member States and lacked the power to enter into the PNRD agreement. The Court left it open, however, for a new agreement to be formed that
argument and found that "Article 3(2) of the Directive, relating to the exclusion of activities which fall outside the scope of Community law, was infringed." In other words, the Court found that the EU did not have the power, under their constitutional rules, to enter into the agreement. Article 3(2) of the Directive determines the scope of privacy rights and states that the Directive does not apply to "activity which falls outside the scope of Community law... [and] to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law." Since the PNRD framework "was dictated by public authorities, and amounted to processing operations concerning public security, the Court held that the EU Commission lacked legal competence under the Directive to address public and state security issues."

The EU Court of Justice held that the EU Council and Commission overstepped their political boundaries and that therefore the PNRD between the U.S. and EU was invalid. In accord with its findings, the Court issued a denunciation which nullified the PNRD effective September 30, 2006. In not addressing privacy directly, the Court left open the possibility that a new agreement, which did not rely solely on the Directive, could be valid under EU law.

E. Second International Agreement and Continuing Domestic Privacy Tensions

In response, the U.S. and EU modified and adopted a new passenger data transfer agreement, which was signed by the EU in June 2007. The 2007 agreement struck a balance between the U.S.

---

was not based solely on the Directive. Bignami, supra note 155.
160. See supra note 153, at 51.
161. Bignami, supra note 155.
162. See supra note 4, at art. 3(2).
163. See supra note 134.
need for security and the EU privacy rights. The new agreement called for the data collected by U.S. authorities to be reduced from thirty-four to only nineteen data fields, including name, contact data, payment details, and itinerary information. In addition, the data collected and processed would be treated in “accordance with applicable U.S. laws, constitutional requirements, and without unlawful discrimination, in particular on the basis of nationality and country of residence.” Thus, EU citizens are afforded protections consistent with the FOIA and the Privacy Act of 1972, including increased transparency and the ability to obtain and correct inaccurate data. Although the new agreement does not extend EU citizens the full protections of the Privacy Act, it does allow the EU and U.S. to share the active monitoring of programs, policies, and compliance with either party’s domestic laws. Under the new agreement, the EU was assured that sufficient safeguards were in place; thus allowing airlines in member countries to transfer passenger data to the U.S.

The new agreement addressed many of the EU concerns and, to a large degree, was supported by the U.S. government. The U.S. government took active steps to support the new agreement. For instance, following the formalization of the second agreement, the “Senate Commerce committee passed new legislation that would promote inbound travel by foreigners” and “the U.S. Department of Homeland Security, along with congressional leaders and industry representatives, were discussing the latest efforts to collect biometric information from both inbound and outbound international travelers.”

Yet, even with Congress and numerous federal agencies in support, the new agreement quickly failed. On February 11, 2008, President George W. Bush flouted the new agreement and demanded increased passenger information with the promise to restrict U.S. airspace, unless an expanded range of data was

167. See supra note 134, at art. 5.
169. See supra note 147, at 2.
170. Id.
provided. This destroyed the 2007 agreement and, as of August 2008, no new agreement has been produced.

VIII. ATSA and Instituting International Privacy Agreements

The different domestic constraints have impacted the ability of the U.S. and EU to negotiate an effective international privacy agreement. The U.S. and EU share the same goals of advancing state security and protecting individual rights; however, they cannot agree on how to achieve these goals within the requirements of the ATSA. Finding a way to implement international agreements that are consistent with domestic law is fundamental to ensuring that domestic and global state security is preserved.

Thus far, the negotiations surrounding the ATSA have failed because neither side is able to conform to domestic legal and security requirements. The U.S. needs increased security and the assurance that the EU will aid in intelligence gathering to minimize the risk of any potential future attacks. For the EU, the effort is to minimize the reduction of individual privacy protections while ensuring that any data transferred to the U.S. is protected in accordance with EU standards. The effect of these domestic constraints is evidenced in the 2007 agreement. There, the U.S. demanded a more limited PNR transfer and agreed to abide by some EU privacy protection guidelines. In exchange, the EU agreed to make U.S. privacy law and protections the foundation for international PNR transfers. This, however, was domestically problematic because it would subject EU citizens to more relaxed U.S. privacy laws, which might violate the EU Directive and fundamental EU liberties. However, it would have an impact internationally because if the EU was to fail to comply with U.S. demands, then it would impact international travel, international relations, and airline revenue.

Although the negotiated positions appear diametrically opposed, in terms of the ATSA, the primary problem appears to be embedded in different domestic understandings of when a law is narrowly tailored enough to warrant intrusion into individual

rights. Thus, in order for the U.S. and EU to successfully negotiate, they must discuss ways to tailor the reach of the ATSA in ways that are acceptable to both parties. One possibility is to have the U.S. institute a more transparent collection, transmission, and retention program for ATSA-collected materials. During their negotiations, the EU expressed reservations about how passenger data was collected and the length of retention. The U.S. was unwilling to provide many details to quell the EU concerns; thus, with more transparency, the EU could be more willing to participate in intelligence gathering.

A second possibility is to make the collection and analysis of global terrorism a shared responsibility. Although this would modify the demands of the ATSA in some respects, it would result in increased and more effective risk analysis. Under the Directive, individual data collection and sharing is drastically limited, except for other EU members. Thus, with shared responsibility, there is the opportunity for the EU to analyze passenger data and only transmit data that represents a legitimate risk to security to the U.S.

Through improved collaboration, the U.S. and the EU would be able to meet their respective domestic interests while enhancing global security through increased communication, data sharing, and voluminous intelligence gathering. For the U.S., increased collaboration would reduce some of the burden on the U.S. to collect and analyze large amounts of data quickly. In addition, global collaboration, especially in the realm of international terrorism, would help preempt global threats to state security. Also, collaboration with the EU could help quell some of EU concerns about data safeguards and, perhaps, persuade the EU to provide more data over time. The EU needs would be met because, with greater transparency and involvement, they could ensure that the necessary safeguards were in place to satisfy their domestic regulations.

A third possibility would be to shift the focus of the discussion away from the dichotomy of state security versus individual rights and onto human security. Under the theory of human security, state security is not at odds with personal freedoms, such as privacy. Instead, human security and national security should be, and often are, mutually reinforcing.\textsuperscript{173} The methods employed focuses on

"preventive diplomacy, conflict management and post-conflict peace-building" through increased collaboration in order to promote equitable economic development.\textsuperscript{174} One of the main methods for increasing human security is to increase international collaboration and information sharing, in order to reduce misunderstandings and promote dialogue.\textsuperscript{175} This possibility suggests that the best way to maximize national and international security is to increase collaboration between the U.S. and EU regardless of the requirements of domestic laws. Instead of the goal being state security or individual privacy, the state interest shifts toward improving the overall human condition, which results in increased security for all.

\textbf{IX. Conclusion}

The U.S. and EU share similar interests in state security and personal liberties, and these similar interests have influenced the development of their respective political and legal systems. Although similar on many fronts, the U.S. and EU have implemented fundamentally different domestic laws. In terms of domestic legislation and case law, the U.S. and EU are constrained in very different ways. Especially after 9-11, the U.S. has become more concerned with maintaining state security, even at the risk of encroaching on personal privacy rights. The U.S. federal government, as evidenced in the recent legislation and case law, has focused largely on increasing state security. In the U.S., privacy rights are unenumerated and implicitly tied to abortion, which makes them easier to trump. To the contrary, the EU has a long history of protecting personal data unless a legitimate and recognizable threat to state security exists. In the EU, privacy rights are enumerated and tied to theories of human rights and fundamental freedoms. Thus, it is significantly more difficult for the EU Parliament or courts to establish any binding precedent that allows for the subrogation of privacy. This note has analyzed the differences between U.S. and EU privacy laws and has shown how these differences have impacted efforts to develop an international


agreement regarding the ATSA. Although no agreement has yet been achieved, the situation is not hopeless. With some minor alternations to their perspectives, the deadlock can be broken and the U.S. and EU can move toward securing international security within domestic constraints.