# 출입국과 관련된 국가간 개인정보 profiling 제공의 문제점과 입법화 방안

문 준 조

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

# 출입국과 관련된 국가간 개인정보 profiling 제공의 문제점과 입법화 방안

## Aviation Profiling for the Strengthened Security Agaignst Terrorism

연구자 : 문준조(선임연구위원)

Moon, Joon-Jo

2009. 11. 5.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

# 국 문 요 약

9.11테러 사태이후 미국 정부는 자국 영토를 출입하는 항공기 승객 및 승무원의 개인 정보를 미 행정부에 제출하도록 요구하는 다양한 법령들을 제정하였는 바, 특히 항공사는 미 세관 및 국경보안국(CBP)이 passenger Name Records(PNRs: 항공기 승객기록)에 내장된 탑승객 정보에 접근할 수 있도록 허락하여야 하고 이를 위반할 경우 벌금부과, 착륙금지, 도착지연 등의 불이익을 당할 수 있다고 명시하고 있다.

테러에 맞선 이러한 대응은 민주사회의 필수 불가결한 요소임에는 틀림없지만, 이 과정에서 기본권 및 자유(프라이버시 및 정보보호권리 등)도 존중되어야 한다. 상업적 용도로 수집되어 항공사 데이터베이스 및 관련 예약시스템에 저당된 개인정보를 공공기관이 접근하도록 허락하는 행위는 전세계적으로 전례가 없는 경우일 뿐만 아니라 정보보호 기본원칙에도 어긋난다. 프로파일링은 보안이라는 명분하에 승객의 불편과 공항당국 및 항공사의 부담을 무한정 가중시킬 수도 없는 현실에서 한정된 보안자원을 이용하여 선량한 승객에 대한 검색노력을 줄이고 반면에 보다 위험가능성이 높은 승객과 수하물에 보안역량을 집중시킴으로써 승객이 보안검색을 위해 대기하여야 하는 시간을 단축하고 공항보안을 효율적으로 강화하는데 그 목적이 있다.

우리나라에 대한 직간접적인 테러위협이 증가하고 있는 가운데 인천국제공항 개항이후 지속적인 여행증가에 비례하여 위해물품의 적발 건수가 늘어나고 있어 검색장비의 첨단화, 검색요원의 전문화 및 숙련화에 따른 대책외에도 프로파일링과 같은 새로운 선진보안기법의 개발 및 도입필요성에 대한 공감대가 형성되어 가고 있다. 이미, 테러, 국제범죄 혐의자 등 국익위해자의 입국을 사전 차단하고 마약밀수 등 우범자들을 선별해냄으로써 다수의 선량한 승객의 신속, 편리

한 출입국이 가능하도록 한 법무부와 관세청의 승객사전정보분석시스템(APIS)에서 보듯이 승객의 예약정보를 이용하여 프로파일링한다는 것은 승객의 여행정보를 수집할 수 있는 정당한 권한이 있어야 하며 법적인 근거가 있어야 한다. 또한 프로파일링 기법 실시국에서 인권침해의 논란이 제기된 점을 고려하여 인권침해를 최소화하는 방안에 대한 충분한 사전검토가 선행되어야 할 것이다.

우리나라의 경우 현재 국내법에서는 수하물에 대해 프로파일링할 수 있는 실시규정을 마련되어 있으나 승객에 대한 프로파일링을 실시할 수 있는 법적 뒷받침이 부족하다. 이에 따라 동제도의 국내도입을 위해서는 항공안전 및 보안에 관한 법률 등 관련법규를 검토, 명확한 시행 근거를 마련할 필요가 있다.

※ 키워드 : 항공프로파일링, 테러리즘, 등록여행자프로그램, 컴퓨터 활용승객사전검색시스템, 테러리스트자금추적프로그램, 보안비행프로그램

# Abstract

In order to effectively combat terrorist-related activities and other serious international crimes, law enforcement authorities must identify terrorists and other international criminals during the only two instances in which they reveal themselves to the international community--when they travel abroad and when they transact abroad. Recognizing this notion nearly two decades ago, the United States and other global powers began sharing information pertaining to financial transactions for the purpose of combating money-laundering and its support of the international drug trade. Then, after the September 11, 2001 terrorist attacks, both governments started using this financial information sharing network to combat terrorism. During the same period, the United States began secretly subpoenaing financial records from SWIFT under TFTP. It also passed legislation that required air carriers "operating a passenger flight in foreign air transportation to the United States to provide the Commissioner of Customs with PNRs data," and that would eventually require the United States and the European Union to agree on how the E.U. airlines would provide that PNR data.

While the PNR data transfers and the TFTP maintain the appropriate focus of identifying suspected terrorists when they reveal themselves to the international community, they do not provide adequate privacy protection for citizens of foreign countries. Therefore, a careful balance must be struck between tracking down suspected international criminals--including terrorists--and the protection of privacy rights. In order to strike this delicate balance, (1) the United States should terminate the TFTP immediately and improve the existing system of financial information

exchange to satisfy its AML/CFT needs, and (2) the United States and the European Union should work to develop an international system of travel information exchange based on the existing model of financial information exchange.

The Registered Traveler Pilot Program is an airline passenger security assessment system that was tested in the United States air travel industry in 2005. It was used in several U.S. airports in a voluntary pilot phase and continues in operation in several airports around the country. There are also registered traveler programs in other countries, such as in London, UK. It is administered by TTAC, the TSA office responsible for Secure Flight, the replacement for the Computer Assisted Passenger Prescreening System (CAPPS) and the canceled CAPPS II counter-terrorism system. Registered Traveler is a public/private partnership with the TSA and the Registered Traveler Interoperabilty Consortium (RTIC) providing rules and standards for private Enrollment Providers that sign up participants. As of August 2007, FLO, Unisys, Verant, Verified, and Vigilant have met TSA's criteria to provide Enrollment services for Registered Traveler.

The program seeks to identify passengers who pose a minimal security risk, and then provide those passengers an enhanced security checkpoint experience. Passengers will voluntarily pay a fee and submit to a background check to become a Registered Traveler. Passengers who pass the background check will be issued a smartcard credential for use at the security checkpoints of airports that participate in the program. Registered Travelers will have access to a reserved security lane and will enjoy a shorter wait at the security checkpoint. Other benefits, such as allowing Registered Travelers to keep their coats and shoes on and their laptops in their bags have also been discussed and Clear Registered Traveler

does have machines that now screen shoes for metal, and as long as a traveler doesn't have metal, they may not have to take off their shoes. Any U.S. citizen or lawful permanent resident over the age of 18 can apply for membership, as can minors over the age of 12 with parental or guardian sponsorship.

In order to prevent a terrorist with a clean background from compromising the system, the Transportation Security Administration requires that registered travelers undergo the normal TSA screening (baggage x-ray and personal metal detector), as well as the RT kiosk checkpoint. Additionally, Registered Travelers are not exempt from random secondary screening and may not bring prohibited items into secure areas of terminals.

※ Key Words : Aviation Profiling, Terrorism, Registered Travelers, Computer Assisted Passenger Prescreening System (CAPPS), CAPPS II, Terrorist Finance Tracking Program(TFTP), Secure Flight

# 목 차

# 제 1 장 서 론

## 제 1 절 연구의 목적

테러리스트들은 국제항공의 글로벌한 성격 때문에 이를 표적으로 삼는 경우가 적지 아니하다. 그들은 굳이 테러 대상국가에 입국하지 아니하더라도 그 국가를 상징하는 대상(정부, 기업 또는 정부나 기업의 대표 등)을 충분히 공격할 수 있다. Pan Am 103편의 파괴는 이러한 점을 잘 보여주고 있다. 이 항공기는 1988년 12월 런던에서 미국으로 향하면서 스코틀랜드의 로커비 상공을 비행중에 플라스틱 폭발물에 의하여 폭파되었다. Pan Am은 미국의 국가소유 항공사가 아니였음에도 미국을 상징하는 것중의 하나였던 것이다. 따라서 테러리스트들은 자신들중 어떠한 사상자도 없이 그 항공기를 파괴함으로써, 자신들이 원하는 다양한 영향을 미칠 수 있었다. 9.11테러의 경우도 그 정치심리학적 영향을 대단히 크다. 테러리스트들은 미국 밖에서가 아니라 미국 국내선 항공기에 탑승하여 테러를 행하였던 것이다. 이와 같이 항공테러가 국제적인 경계를 요하는 범세계적 위협이 되고 있다는 있음은 분명하다.

2006년 8월 10일 영국 첩보기관은 보통 액체에 담긴 폭발물로 100개의 항공기를 폭파시키려는 테러 기도를 저지하였다.[1] 그에 대한 반응으로 교통보안청(Transportation Security Administration: TSA)은 일정한 휴대물품의 반입을 금지하였다.[2] 2007년 TSA는 밀봉된 병에 담긴 액체 폭발물을 탐지할 수 있는 휴대용 스캐너인 FIDO를 공개하였다.

1) Agent Infiltrated Terror Cell, U.S. Says, CNN.com, Aug. 11, 2006, http://www.cnn.com/2006/US/08/10/US.security/index.html.

2) Transp. Sec. Admin., Prepare for Takeoff: Permitted and ProhibitedItems, available at http://www.tsa.gov/assets/pdf/Prohibited%20and%20Permitted%20Itemsprinterfriendly3-16-07.pdf.

휴대반입 물품 제한 및 폭발물 탐지장치의 도입은 중요한 보안의 조치의 하나가 되고 있지만, 또 다른 한편으로 상업적 항공을 보호하기 위하여 프로파일링이 왜 필요한가를 보여주고 있다.

요컨대, 엑스레이, 장비, 폭발물 탐지기 등 장비와 인력을 이용한 전통적인 보안검색기법으로는 날로 지능화되고 교묘해지는 테러수법과 테러위해물품에 적절히 대응하는 것이 점차 어려워지고 있다. 또한 보안을 위해 승객의 불편과 공항당국 및 항공사의 부담을 무한정 가중시킬 수도 없다. 이러한 이유로 인하여 한정된 보안자원을 이용하여 선량한 승객에 대한 검색노력을 줄이고 반면에 보다 위험가능성이 높은 승객과 수하물에 역량을 집중시킴으로써 승객이 보안검색을 위하여 대기하여야 하는 시간을 단축시키고 공항보안을 효율적으로 강화하는 것이 필요하게 됨에 따라 이스라엘과 미국에서 개발시행중인 프로파일링에 대해 관심이 고조되고 있다.[3)]

한편, 일련의 테러리스트 기도에 대응하여 등장한, 사람이 아닌 물건에 꼼꼼하게 초점을 맞춘 국가 항공보안정책은 다소 퇴영적인 것이며 불량한 사람을 찾는 검색이 적어도 불량한 물건을 찾는 검색만큼 중요하다는 점에서 항공기승객 자체를 프로파일링하는 것은 상업적 항공의 보안에 필수적인 것이 되어야 한다는 주장이 제기되고 있다. 어떠한 의미에서 볼 때, 보안이 자유와 프라이버시를 희생하여야 비로소 가능하다는 관념을 배척하고 프로파일링이 불가결하고 합법적인 역할을 하는 항공보안정책이 수립되어야 한다는 시대적 요청을 무시할 수는 없을 것이다. 승객프로파일링을 다음과 같은 세 가지 문제와 관련되어 있다는 점도 유의하여야 한다. 첫째, 항공보안정책에서 확인하고자 하는 적(enemy)은 누구인가, 둘째 프로파일링은 과연 합리적인가 혹은 인종주의적인가, 그리고 세 번째 항공사 승객프로파일링시스

3) 황호원・이규황, “항공보안에서의 프로파일링 연구”, 항공우주법 학회지, 제22권 2호(2007), p.156.

템이 반드시 자유와 프라이버시의 권리 보다 국가안보를 우선시하는 정책선택을 요구하는가이다.

최근에는 국제적인 프로파일링 협력문제를 끌고 있다. 항공의 국제성을 고려해볼 때 지극히 자연스러운 현상이라 할 것이다. 국제항공테러의 대비책으로 주요 국가들이 외국인의 출입국과 관련하여 개인정보 프로파일링을 요구하거나 교환하고 있으며, 이는 전자여권의 도입과 더불어 크게 확산될 전망이다. 이와 관련하여 EU와 미국의 국제항공기 보안조치와 그들 간의 협력과 충돌을 살펴봄으로써, 국제적 협력의 가능성과 한계에 대해서도 살펴볼 필요가 있을 것이다.

일부 비판론자들은 항공프로파일링을 위하여 제공되는 데이터가 상업적인 또는 기타의 목적으로 이용될 수 있다는 점에서 개인 정보의 보호에 심각한 영향을 미칠 것이라고 지적하고 있으며 최근에는 국제적인 차원에서도 논란이 제기되고 있으며 미국과 EU에서도 상반된 입장을 보인 바 있다. 현재 미국에서 항공보안을 위한 다양한 프로그램이 시행되고 있는 바, 프라이버시의 보호 및 국가안보라는 두 가지 요청에 대한 관련성 및 조화를 검토할 필요가 있음은 두말할 여지가 없다. 현재 우리나라에서도 프로파일링 도입 필요성을 인정하고 연구가 진행되고 있으며, 국내에서 승객과 수하물에 대한 프로파일링을 시행하기 위해서서는 인권의 침해를 최소화하면서 법적 시행근거를 마련할 필요가 있을 것이다.

아래에서는 “Registered Traveller” 프로그램과 더불어 CAPPS, CAPPS Ⅱ, “Secure Fight”와 같은 정부부문과 민간부문의 프로파일링 시스템의 이론적 분석을 해보고 그러한 시스템이 장래의 항공기 테러에 대한 리스크를 관리하기 위한 효과적인 반테러주의 조치인지의 여부를 살펴보고자 한다. 이러한 작업을 수행하면서 이 보고서는 현재 진행중인 프로파일링 시스템의 발전을 무비판적으로 받아들이고 있지는 아니하다는 점을 밝히고자 한다.

## 제 2 절 연구의 범위

제2장에서는 항공프로파일제도의 발전과 법적 쟁점에 대해 소개하고 있다. 여기에서는 항공분야에의 도입배경, 항공프로파일링의 유형과 특징, 특히 미국에서의 발전에 대해 심도있게 소개하였다. CAPPS. CAPPS Ⅱ외에도 및 Secure Flight 및 Registered Traveller 프로그램 등을 다루었다. 특히 프라이버시의 권리와 프로파일링간의 충돌과 이를 둘러싼 미국에서의 논쟁도 아울러 상세히 소개하였다.

제3장에서는 프로파일링의 정보제공을 둘러싼 미국과 EU의 갈등과 해결방향에 대해 다루었다. 미국과 EU는 보안과 시민적 권리와 관련하여 상반된 시각을 보이고 있으며, 이러한 현상을 프로파일링 정보의 상호교환과 관련된 국제적인 노력의 어려움을 잘 보여주고 있다.

제4장에서는 국내프로파일링 도입방안에 대해서 다루었다. 이와 관련하여 항공보안 프로파일링은 아니지만, 이미 우리나라에서 도입되어 있는 관세청의 APIS 제도 즉 사전승객정보제도와 법무부의 제도를 분석하였으며, 항공보안 프로파일링의 입법방향에 대하여 다루었다.

# 제 2 장 항공프로파일링제도의 발전과 법적 쟁점

## 제 1 절 프로파일링의 개념과 항공분야 도입 배경

프로파일링이라 함은 우리에게 익숙한 단어인 프랑스어 profile에서 유래한 것으로 프로필이란 인물을 간략히 소개하는 평을 의미하는 바, 프로파일링은 1960년대 경찰당국이 중범죄를 수사하는데 사용되기 시작하였으며 수사과정에서 많은 결백한 사람을 포함하여 범죄와 관련되었을 수 있는 모든 사람에게 동일한 시간과 노력을 기울이는 것이 비효율적이라는 판단하에 잠재적 용의자, 특히 범죄자에게 노력을 집중하기 위하여 활용되고 있는 것이다. 이 용어는 '잠재적 위협이 될 수 있는 의심스러운 승객을 선별, 분류하여 승객과 승객이 소지한 수하물에 대하여 정밀 검색을 하여 효율적인 보안검색을 하기 위한 일련의 과정'을 의미하는 뜻으로 바뀌어 항공보안 업무에 사용되고 있다. 우리가 일반적으로 항공보안에서 사용하는 프로파일링의 명칭은 passenger profiling system이라 한다.[4] 다시 말해서 프로파일링이라 함은 가장 많은 위협을 가질 것으로 보이는 승객의 짐에 검색을 집중하고 위협을 가지지 아니할 것으로 보이는 승객의 짐에는 시간을 덜 소비함으로써 가방에 들어있는 폭탄을 발견할 가능성을 최대한으로 유지시키는 시스템이다. 요즘에는 프로파일링이라는 용어가 인종차별의 문제를 연상시키는 표현으로 거부감이 많아 사전검색시스템(prescreening system) 또는 선별검색시스템(Selectee system)으로 바꾸어 사용하고 있다.[5]

4) Ibid., p.157.
5) Ibid.

항공보안에서는 1969년 2월 18일 발생한 취리히 공항에 주기된 이스라엘 EL AL 항공기에 기관총과 수류탄으로 무장한 4명의 팔레스타인인민해방전선(PFLP) 테러분자가 난입하여 공격한 사건을 계기로 이스라엘 보안당국은 EL AL 항공기 보안에 대해 많은 대응대책을 수립하였으며, 기내 보안요원배치, 승객검색, 조종실 보안 등과 함께 수상한 승객에 대한 프로파일링을 실시하도록 하였다. 이것이 최초의 프로파일링 시스템의 시행이라 할 수 있다.[6] 그 후 미국도 1968년부터 연구하기 시작하였으며 1986년 이후 미국 항공기 공중납치와 폭격을 수반한 여러 사고가 잇따르자, AA항공사와 TWA는 유럽발 국제항공편에 프로파일링 시스템을 채택하였으며 앞서 언급한 Lockerbie사건 이후 FAA는 유럽발 모든 미국 항공편에 대하여 프로파일링 사용을 명하였으며 1996년 클린턴 미국 대통령이 CAPPS(승객사전검색시스템) 사용을 승인한 이후 2002년 한층 강화된 CAPPSⅡ가 미국에서 사용되기 시작하였다. 그후 프라이버시 침해 등을 이유로 한 반대여론에 부딪쳐 새로운 방안들이 도입되어 시행되고 있다. 이에 대해서는 후술한다.

## 제 2 절 항공보안프로파일링 유형

프로파일링에 대한 방식은 크게 3가지로 발전하였는 바, 시스템 프로파일링(자동식)과 매뉴얼프로파일링(수동식) 방식, 최근 시스템 프로파일링과 매뉴얼프로파일링의 혼합식 프로파일링 방식이다. 매뉴얼프로파일링은 이스라엘이 1970년대 이후부터 사용하고 있으며 체크인 전에 실시하는 방식이다. 체크인시에 승객으로부터 정보를 얻어 분석한다는 것이 가장 큰 특징이다. 체크인 이전에 훈련받은 요원이 모든 승객을 대상으로 구두로 질문하여 특정 수상한 승객을 가려내는 방식

6) Ibid., p.158.

으로 선별된 해당 승객에 대해 몸수색 및 수하물 수색을 하는 방식으로 고전적인 프로파일링 방식이다. 실제로 이스라엘 EL AL 항공사는 거의 완벽하게 테러리스트를 차단하였으며 이로 인해 현재까지 항공기 납치나 폭파사건은 발생하지 않고 있다. 매뉴얼 프로파일링의 대표적인 성공사례는 Ann Marry Murphy 사건이다. 1986년 4월 17일 런던 히드로발 텔아브 비행 EL AL 항공기 016편에 탑승하려던 아일랜드 여자승객 휴대물에서 폭발물이 발견된 사건이 발생하였다. 이 여자 승객은 보안요원의 프로파일링 질문에 논리적으로 답변하지 못하였으며 이를 수상히 여긴 보안요원이 소지물을 정밀 검사하여 가방내 폭발물이 장착되어 있음을 발견하였다. 조사결과 정보요원인 Nezsr Hindawi의 여자친구로 밝혀졌다. 이 사건은 이스라엘 프로파일링의 우수성을 널리 알리는 계기가 되었다.[7)]

한편, 시스템프로파일링 방식을 대표적으로 사용하는 국가는 미국이다. 미국에서는 체크인시 시스템 프로파일링을 실시하는 바, 예약된 기존 승객자료를 이용하여 승객의 유해여부를 판단하는 방식이다. 최근 모든 시스템이 전자시스템화되어 승객에 대한 기본정보(국적, 항공권 구매상태 ) 등 특정 정보만 입력하면 자동으로 해당 승객에 대한 위험여부를 가리는 방식으로 완전 자동화되어있으며 공동사용터미널 장비(Common Use Terminal Equipment) 시스템과 연결되어 사용되고 있다. 이 방식을 신속하고 간편하게 위해인물을 찾을 수 있다는 장점이 있어 널리 사용되고 있다. 9.11테러이후 기존의 프로파일링이 모든 승객의 상세한 개인정보를 제공하여야 하는 문제로 인권단체들의 거센 반발이 있자 자동방식과 연계하여 공항에서 체크인 과정에서 의심스러운 승객의 행동을 분석하여 위해승객을 가려내는 매뉴얼 프로파일링과 시스템 프로파일링을 혼합한 새로운 대안으로 등장하고 있다. 혼합식 프로파일링방식은 체크인 전의 과정에 걸쳐 실시되는 방식으

7) Ibid., p.159.

로 예약된 기존 승객의 항공권 예약상태, 여권정보 등 범죄자나 테러범 명단이 입력된 다른 데이터베이스를 대조하여 해당승객의 위험여부를 1차적으로 가려내는 한편 체크인 과정에서 전문교육을 받은 항공사 보안요원이 단순한 문답식 방식에서 벗어나 의심스러운 행동을 하는 승객을 선별하여 정밀 검색대상자로 분류하는 방식이다. 이중에서 관찰기법에 의한 프로파일링은 기존 인터뷰 방식에서 벗어나 수상한 자의 행동을 파악하여 이를 분석하여 더욱 더 정확히 승객을 가려내는 방식이다.[8] 이스라엘이 최초 개발하여 사용된 매뉴얼 프로파일링 방식은 미국에서도 9.11테러 사건이후 항공보안 강화에 대한 일환으로 미국 보스턴 공항을 비롯한 주요 공항에서 도입되어 자동방식과 연계하여 현재 사용중에 있다. 이를 통하여 보스턴 공항세관에서 적용하여 마약소지자 검거율이 20% 이상 올랐다는 기록이 있다. 또한 보스턴 공항 체크인 카운터 요원 및 검색 요원에 지속적인 교육을 실시하여 효과를 보고 있으며, 샌프란시스코 공항 체크인 카운터요원, 검색요원 교육이 실시되었다. 아래에서는 미국에서의 최근에 인권침해와 관련하여 논란이 되고 있는 프로파일링시스템의 발전과 현황에 대하여 소개한다.

8) 1999년 12월 24일 Port Angles를 통하여 캐나다에서 미국으로 입국하는 사람들중에 Ahmed Ressam이라는 자는 브리티시 콜롬비아주 빅토리아 섬에서 페리 여객선을 타고 미국에 입국을 시도하였는 바, 자동차 트렁크에 가방폭탄이 있었다. 그는 LA 국제공항 터미널 수하물 카트에 여행용 가방을 두고 타이머를 작동시킬 계획이었다. 그는 여객선을 타기 전에 Bennie Antonie Noris라는 이름의 가짜 신분증으로 세관을 무사히 통과하였으나 워싱턴 Angels 항공에서 세관직원의 질문에 안절부절 못하며 불안해하는 모습을 보이고 눈 접촉을 피하는 등 일반인과 다른 수상한 행동을 하였다. 이를 수상히 여긴 세관직원이 해당자의 트렁크를 정밀수색한 결과 가방에서 폭발물이 발견되었다. 조사결과 그는 크리스마스에 LA 공항에 폭발물을 설치하여 폭파하고자 하였던 것으로 밝혀졌다. Ibid., p.161.

## 제 3 절 미국의 프로파일링시스템의 발전

### 1. 프로파일링 둘러싼 최근의 논쟁

#### (1) 실효성 논쟁

테러주의자들은 항상 상업적 항공여행을 위협하여왔다. 최초의 공식적인 항공기 납치는 일찍이 1931년에 발생하였다. 당시 페루 혁명주의자들은 선전을 하기 위하여 국내비행기를 탈취하였다. 납치범들은 그후 정치적 수형자들과의 교환을 위해 협상하기 위해 또는 특정한 목적지로 탈출하기 위해 상업항공기를 탈취하여왔다. [9] 이와 대조적으로 9.11 항공기납치범들의 목적은 미국인들을 죽이고 미국의 경제, 군사 및 정치적 힘의 아이콘(icon)을 파괴하는 것이었다.

그들 19인중 10인은 컴퓨터 승객프로파일링 시스템에 의한 보다 세밀한 보안검색으로 적발되었다. 그들은 4대의 항공기를 납치, 모든 미국 상업적 항공 보안시스템과 인프라를 농락함으로써 수십 년 동안 운영되어온 미국의 보안시스템의 잘못된 과정을 적나라하게 보여주었다. 또한, 9.11테러는 항공기테러의 역사적 관념을 뒤바꾸어놓았으며, 항공보안정책수립자들이 항공테러의 역사를 제대로 평가하지 못하였음을 보여주고 있다.

민간항공기가 파괴의 무기가 되는 것을 방지하지 못한 가장 큰 장애물은 수십년 동안의 축적된 선입관이었다. 9.11테러사건에서 보듯이 탈취범들이 항공기에 대한 통제권을 장악하려고 하는 상황에서는 항공기의 보존과 그 탑승자들의 생존은 더 이상 고려요소가 아니었다. 이 사건에 대한 반성으로 테러리스들이 항공기 통제권을 장악하여 항공기를

9) Humphrey G. Dawson, “Civil Aviation, Hijacking and International Terrorism: An Historical and Legal Review”, Int'l Bus. Law, Vol.15(1987), pp.57-8.

대량 파괴를 위한 무기로 전환시키는 것을 방지하는 것도 우선적인 고려대상이 되고 있다.[10] 미국 교통부(Department of Transportation: DOT)에서 감사관(Inspector General)을 역임한 어떤 사람은 다음과 같이 언급한 바 있다: 4대의 제트항공기를 탈취하려는 시도가 있었다. 그 위기에서 벗어난 비행기를 포함시킨다면 아마 5개가 될 것이다. 어찌되었건 그들은 4대의 항공기들을 탈취하여 미국의 이스라엘에서의 역할에 항의하기 위하여 지하드(聖戰)로 끌어들였다. 이러한 지하드에서 그들은 자신들이 혐오하는 미국에 최대한의 피해를 입히기 위하여 납치항공기를 건물에 충돌시켰다. 그러나 유감스럽게도 많은 사상자들을 낳았다. 그들은 사상자들에 대해서는 고려조차 하지 아니하였을 것이다. .....1970년 9월 12일 이와 유사한 사건이 발생한 적이 있다. 3대의 항공기가 중동으로 탈취되어 폭파되었다. 이 사건에서 그들은 승객들이 항공기에서 내리기 위해서 서로 다투어 아수라장이 되도록 하는 기묘한 방법을 택하였다.

아무튼 9.11테러의 전략은 완전히 새로운 것이고 최초의 사례가 되었지만 최근 항공기에 대한 테러 위험은  과거 항공정책수립자들이 직면하였던 국가보안상의 우려사항과는 개념적으로 다르다. 과거 소련이 냉전체제하에서 새롭게 행한 행위들은 관찰이 가능하고 대처가 가능하였지만 최근의 테러행위는 무한의 위협이 되고 있다. 즉, 테러주의자들은 엄청남 큰 힘을 들여야 찾아낼 수 있는 일상적인 활동에서 테러행위를 하기 때문이다.[11] 이러한 새로운 상황에서 항공기프로파일링시스템은 항공보안관리들에게 테러주의자들을 찾아낼 수 있는 선험적이고 미래예측적인 메커니즘이 될 수도 있을 것이다.

---

10) Phillip A. Karber, “Re-Constructing Global Aviation in an Era of the Civil Aircraft as a Weapon of Destruction”, Harv. J.L. & Pub. Pol'y, Vol.25(2002), pp.781-93.

11) Paul Rosenzweig, “Civil Liberty and the Response to Terrorism”, Duq. L. Rev., Vol.42 (2004), p.663.

그러나 항공기승객에 대한 프로파일링은 논란의 대상이 되고 있다. 항공사 승객프로파일링시스템에 대한 비판론자들은 4가지의 주된 우려를 표명한다. 첫째, 프라이버시 옹호론자들과 자유주의자들은 보안조치로서의 프로파일링이 너무 극단적이라고 주장한다. 그들의 견해에 따르면 9.11테러와 같은 의도를 가진 잠재적인 테러주의자들은 항공기 승객들중 극소수에 해당한다. 결과적으로 프로파일링 시스템은 항공기보안에 전혀 위협이 되지 아니하는 압도적 다수의 항공기승객의 프라이버시를 침해하기 때문에 항공보안의 대안이 될 수 없다는 것이다.

둘째, 프로파일링 비판론자들은 승객에 관한 기록(dossier)상의 정보의 출처와 소유권에 관하여 의문을 제기한다. 프로파일링스시스템이 승객의 자신의 신상 정보에 대한 통제권을 박탈한다는 점은 분명하다. 미국 연방정부는 승객 프로파일과 위협평가를 작성하기 위하여 어떠한 정보에 의존하는가에 대하여 밝히기를 거부하고 있다. 프로파일링데이터의 자료원(source)은 정부만이 알고 있으며 일부 프로파일시스템의 비판론자들은 정부의 프로파일링데이터의 자료원은 항공여행과 아무런 관계가 없는 신뢰할 수 없는 상업적 데이터베이스라고 주장한다.

셋째, 프로파일링시스템은 운영면에서 비효율적이며 위협이 되는 사람을 잘못가려낼 수 있다(false negative 와 false positive)는 것이다. 그동안의 프로파일링시스템의 비효율성은 다른 사례를 살펴보면 쉽게 입증된다. 예컨대, TSA, FBI 및 Secret Service는[12] 어느 항공기 승객의 이름이 알 카에다의 확실한 자금제공자의 이름과 유사하였기 때문에

12) 현・전직 및 차기 대통령, 현대통령의 가족, 부통령 등 국가 요인에 대한 미국의 비밀경호관을 말한다. 1860년 창설 당시는 위폐 단속의 재무부 검찰부였으나 1901년 윌리엄 매킨리(1843~1901) 대통령 암살사건 후 임무가 바뀌었다. 각 주에 총 70개 가량의 파견기관이 있으며 연방수사국(FBI)・중앙정보국(CIA)으로부터 독립해 활동하고 있다. http://k.daum.net/qna/openknowledge/view.html?category_id=KL&qid=2du3Z&q=Secret+Service&srchid=NKS2du3Z.

22차례 걸쳐 켄터키주에서 항공기를 타지 못하게 한 바 있다. 그 동안에도 현재의 검색(screening)시스템은 미국의 최우선 수배자인 오사마 빈 라덴의 이름으로 테스트 해본 결과 주목할 만한 아무런 성과도 얻지 못하였다. 이러한 비효율성에 개인 신상자료의 유출 위험이 덧붙여져 항공위협 평가를 위하여 기계에 의존하는 항공보안제도의 중대한 결함이 드러났다.[13)]

마지막으로 사실의 관점에서 볼 때 어떠한 항공기승객이 보안에 위협요소가 되는지는 개인마다 다르기는 하지만, 법적 관점에서 볼 때는 프로파일링시스템이 승객을 불평등하고 차별적으로 다루게 된다. 따라서 비판론자들은 컴퓨터활용 검색이 그 태도나 입장이 미국의 이익에 저촉되는 세계의 지역들- 즉 중동- 과 관련성이 있는 승객에 대하여 처음부터 편견을 갖고 있음을 지적한다. 또한 프로파일링이 여행객을 언어・습관에 따른 종족, 인종 또는 종교에 의하여 분류하는 것은 위헌적인 것이라고 판단한다. 또한 미국 정부가 프로파일링이 그러한 기준에 입각하여 운영된다는 생각을 부인하지만 많은 비판론자들은 여전히 정부가 9.11테러주의자들이 종족적・지리문화적・종교적 공통성을 가지고 있다는 사실을 무시한 인류평등주의적 시스템을 만든다는 것을 믿지 않는다. 한편 프로파일링시스템 옹호론자들은 "우리는 과거 테러주의자들에 대하여 알고 있는 것을 이용하여야 한다" 라고 지적하며 상식에 호소하여 이러한 우려를 배척한다. 이러한 주장이 실제적인 측면에서 본다면 타당한 것이기는 하지만 프로파일링은 많은 미묘한 법적 문제점들을 제기하고 있다. 아래에서는 9.11테러 사건이후의 미국의 민간 및 정부의 주요 프로파일링 방안을 소개하고 양자의 실제적 그리고 법적 장점과 결함을 분석하기로 한다.

---

13) Addie S. Ries, “Comment, America's Anti-Hijacking Campaign - Will It Conform to Our Constitution?”, N.C. J.L. & Tech., Vol.3(2001), p.123.

(2) 인권과 보안의 충돌

즉, 우선 먼저 살펴보아야 할 문제로서 프로파일링시스템이 누가 테러주의자이고 그러한 가능성이 있는지를 신뢰성있게 예측할 수 있는 것인지에 대한 의문이다. 테러주의자들은 다양한 배경하에서 등장하고 있으며 연령, 성별, 인종, 교육 및 경제적 상황은 프로파일링 목적에는 부적절한 고려요소들이 되고 있다.[14] 예컨대, 2006년 8월의 액체 폭발물에 의한 폭파기도 사건에서 체포된 혐의자들중 세 사람은 런던의 부유한 교외에 사는 이슬람교 개종자들이었다. 그 중 한 남자는 영국보수당 당원의 아들로서 Team America라는 영화를 좋아하는 사람이었다. 그렇다면 실제로 프로파일링을 통하여 테러주의자를 확인하는 것은 불가능하며 단순히 직관에만 의존할 수도 없으며 사실상 불가능할 수 있다.

또한 법적으로 승객 프로파일링은 공항에서 보다 엄격한 보안이 필요하다는 이유로 포기해버릴 수는 없는 중요한 헌법상의 문제를 제기하고 있다. 생명 및 행복추구와 같은 자유는 양도불가의 권리에 속한다. 또한 자유, 프라이버시 또는 간섭받지 아니할 권리(right to be let alone)와 관련되어 있다. 자유와 프라이버시는 추상적인 개념이며 그동안 그 범위에 대해 많은 정의가 제시되었고 그와 동시에 고정적인 의미를 부여하기 어렵다.[15] 그럼에도 불구하고 미국인들은 9.11테러사건이후 특히 상업항공 보안과 관련하여 확실성을 요구하여왔다. 역사적으로 시민의 자유와 같은 추상적 개념은 그 불확실성의 시기 그리고 국가안보상의 위기시기에는 도전을 받아왔으며, 현재 테러주의적

14) Richard W. Bloom, Commentary on the Motivational Psychology of Terrorism Against Transportation Systems: Implications for Airline Safety and Transportation Law, Transp. L.J., Vol.25(1998), pp.175-79.

15) R.I.R. Abeyratne, “The Effects of Unlawful Interference with Civil Aviation on World Peace and the Social Order”, Transp. L.J., Vol.22(1995), pp.451-56.

행위를 저지하기 위한 항공보안안정책 수립자들의 자유와 프라이버시 제한적인 시도들은 상당한 호소력을 가지고 있다.[16] 효과적인 항공사 승객프로파일링시스템의 설계와 시행은 서로 상반되는 정책선택이라고 할 수 있는 "자유와 프라이버시" 및 "국가안보"를 동시에 고려하여야 한다.[17]

자유와 프라이버시 옹호론자 및 보안 옹호론자들은 항공사 승객프로파일링시스템에 대한 절대적인 의미에서 찬성논과 반대론은 제시하고 있다는 점에서 모두 비난받아 마땅하다. 미국의 많은 자유주의와 프라이버시 옹호론자들의 출발점은 "약간의 일시적인 안전을 얻기 위하여 본질적인 자유를 포기하려는 자들은 자유와 안전 어느 것도 얻을 가치가 없다"라는 1759년의 벤자민 프랭클린의 비타협적인 선언이다. 그에 반대하여, 어느 유명한 항공사 CEO는 이에 대해 "항공기에 탑승하여 여행하고 싶다면 당신의 프라이버시를 포기하시오. 당신의 프라이버시를 포기하고 싶지 않다면 항공기여행을 하지 마시오. 당신의 프라이버시는 나머지 우리들의 안전과 동등한 것은 아니오"라고 말한 바 있다.[18]

16) Daniel W. Sutherland, "Homeland Security and Civil Liberties: Protecting America's Way of Life", Notre Dame J. L. Ethics & Pub. Pol'y, vol.19(2005), p.289.

17) K. A. Taipale, Technology, "Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd", Yale J.L. & Tech., Vol.7 (2004-2005), pp.120-27; Darren W. Davis & Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", Am. J. Pol. Sci., Vol.48(2004), pp.28-9.

18) Robert Crandall, "Security for the Future: Let's Get Our Airlines Flying, Address at the Freedom Versus Fear: The Future of Air Travel Conference (Oct. 29, 2001)", J. Air L. & Com., Vol.67(2002), p.7, 19.

## 2. CAPPS와 CAPPSⅡ

### (1) CAPPS

FAA는 1960년대 당시의 항공기납치 증가에 대응하여 승객프로파일링을 만들었다.[19] 연방보안관리들은 자신들이 납치범들이 전형적으로 가지고 있었던 개인적 특성들의 집합인 프로파일링에 기초하여 잠재적인 항공기납치범을 찾아낼 수 있을 것이라고 판단하였다. 특히 FAA의 항공납치방지 프로파일(Anti-Air Hijack Profile은 그 동안의 경험을 통대로 항공기납치범들과 연관성이 있는 대략 25가지의 특징을 설정하였다.[20] 만약 승객이 프로파일상의 요건에 들어맞는 경우, 보안요원들은 그 승객의 휴대수하물을 엑스레이로 투시하거나 다른 검색절차를 통하여 승객을 조사하였다. 그러나 FAA는 1972년 비효과적임을 확인하고 프로파일링을 포기하고 이에 갈음하여 모든 휴대수하물을 엑스레이 투시하는 보안검색대를 만들어냈다.

항공기승객 검색의 필요성은 1996년 7월 17일 뉴욕에서 파리로 비행하던 TWA의 보잉 747기가 이륙직후 폭발하자 다시 제기되었다. 연료장치의 결함으로 그러한 비극을 초래하였지만 정부 관리들은 처음에는 테러주의자들이 그 항공기를 폭파하였다고 믿었던 것이다. 결과적으로 1996년 8월 22일 클린턴 대통령은 항공안전 및 보안에 관한 백악관 위원회(White House Commission on Aviation Safety and Security)의 설치를 선언하였다. 이 기구는 Gore Commission으로도 알려져 있으며 국내적으로 또한 국제적으로 항공안전과 보안을 개선하기 위한 전략을 개발하여 대통령에게 권고하는 임무를 가지고 있었다. Gore

19) Jack H. Daniel III, “Comment, Reform in Airport Security: Panic or Precaution?”, Mercer L. Rev., Vol.53(2002), pp.1623-25.

20) Dempsey & Lara M. Flint, “Commercial Data and National Security”, Geo. Wash. L. Rev., Vol.72(2004), pp.1459-64.

Commission은 1960년대의 승객프로파일링의 부활과 개편을 포함하는 몇 가지 보안관련 권고를 한 최종 보고서를 1997년 2월 공표하였다. 그 내용을 간략히 소개하면 다음과 같다.

첫째, FBI, CIA 및 알콜・담배・총기류국(Bureau of Alcohol. Tobacco and Firearms)은 최선의 프로파일링 시스템을 개발하기 위하여 필요한 알려진 테러주의자, 항공기납치범 및 폭파범(bombers)에 관한 조사를 평가하고 확대하여야 한다. 그들은 그러한 프로파일이 항공사가 보관하고 있는 자동화된 승객정보와 대조될 수 있다면 항공사에 가장 유용한 것이 될 것이라는 점에 유의하여야 한다. 둘째, FBI와 CIA는 알려진 또는 혐의가 있는 테러주의자에 관한 중요한 첩보정보가 그러한 첩보 또는 그 자료원(sources)의 통일성(integrity)을 손상시키지 않고 승객프로파일링에 이용되는 것을 허용하는 시스템을 개발하여야 한다. 셋째, 동 위원회는 프로파일링시스템의 개발・이용으로부터 제기되는 시민권(civil liberties) 문제에 관한 자문위원회를 설치한다.

FAA는 이러한 청사진을 이용한 컴퓨터활용승객검색프로그램(computer assisted passenger screening program)을 개발하였다. 제1세대 컴퓨터활용 항공사승객프로파일링시스템은 FAA의 양해하에 1996년 Northwest Airlines가 개발하였다. 최초의 시스템을 테스트한 후 동 항공사는 1997년 FAA를 통하여 다른 항공사들에게 프로파일링 소프트웨어를 공개하였으며, 미국 전역에서 1998년부터 시행하였다. 그 프로파일링 소프트웨어는 각 항공사들의 내부 컴퓨터보존시스템을 통하여 운영되었으며 CAPPS(Computer Assisted Passenger Prescreening System)로 알려지게 되었다. 정부는 이러한 최초의 방안을 프로파일링스템으로서가 아니라 일종의 관리수단(management tool)으로 제시하였으며 그 목표는 건초더미에서 바늘을 찾는 것이 아니라 건초더미를 더욱 작게 만드는 것(not to pick a needle out of the haystack, ...but to make the haystack smaller)이었다. CAPPS는 민간항공을 위협하고자 하는 사람들

을 식별해내기 위해 승객의 프로파일링을 평가한 항공사에 의하여 운영되는 FAA로부터 승인을 받은 자동시스템으로, 폭발물 탐지를 위하여 모든 여행객의 가방을 전체 검색(Full screening)하기보다는 선별적으로 검색할 수 있도록 테러리스트 요주의리스트(Terrorist Watch List)와 항공기 탑승예정 승객을 대조하는 간단한 방식의 시스템이다. CAPPS I는 승객이 항공사에 제공하는 정보(결제정보 등)에 기초하여 경험적인 데이터마이닝 기법을 이용하여 여행객들에게 위험점수를 부여하여 모든 승객을 분류하고자 만들어진 시스템으로 위험수준에 따라 초록, 노랑, 빨강으로 분류되며 빨강으로 분류된 승객의 경우에는 심각한 위험을 초래할 수 있다고 판단하여 법집행 기관의 조치가 필요(탑승거부 등)함을 의미하는 것이다. 또한 무작위로 일정 퍼센트를 추출하여 선별 검색대상자로 지정한다. 이와 같이 선별된 자들에 대하여 수하물 검색 또는 승객 수하물 일치시스템을 적용시켰다. CAPPS는 선택적으로 일부 승객을 선택하고 프로파일과 일치하는 사람들은 추가적인 보안검색을 받도록 하는 것으로 9.11 사건 당시 19명의 테러범중 CAPPS에 의해 10명은 식별되었다. 항공사 체크인카운터 직원들은 보안에 관한 질문에 정확한 답변을 못하거나 신분증이 없거나 항공사의 기타 기준에 부합하지 못하는 승객에 대해서는 “selectees”라고 표시한다.

CAPPS는 (어느 것은 정돈되고 어느 것은 정돈되지 아니한) 데이터베이스에서 탑승전의 데이터중에서 대략 39개 부분을 수집한다. CAPPS가 수입한 데이터는 높은 수준의 보안절차를 받아야 할 여행자를 선별해내는데 도움을 준다. 프로파일을 공개하는 것은 프로파일을 합법적인 것으로 만들기 위해 필요하지만 그렇게 하면 그 유용성을 떨어뜨리게 된다.[21] 실제로 정부는 CAPPS 프로파일 작성기준을 공개

21) Jamie L. Rhee, “Comment, Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats”, Depaul L. Rev., Vol.49(2000), pp.847-65.

하지 아니하려고 하지만 항공사보안을 관찰한 일부 사람들은 CAPPS가 항공권 지불방법(즉 현금이냐 신용카드이나), 구입시기(출발 직전 또는 그 보다 훨씬 빨리), 동행자가 있는지 있다면 누구인가를 포함한 여행자의 신원, 승객이 차를 빌리려고 하는지의 여부를 포함한 목적지에서의 활동, 최종목적지가 승객이 탑승한 비행기의 도착지와 다른 경우 그 최종목적지를 포함한 승객의 구체적 여행계획 및 항공여행이 왕복인지 아니면 편도인지의 여부 등과 같은 특정한 사항에 대해 초점을 맞추고 있다는 것을 확인해내었다. CAPPS에 의하여 선별된 승객은 추가적인 검색을 받게 된다.

CAPPS로 선별된 승객에 적용되는 추가적인 보안조치는 다음중의 하나가 된다. 가방대조(bag matching) 즉 수하물을 체크한 승객이 항공기에 탑승하였다고 판단되는 경우에만 체크된 수하물을 적재하도록 하는 것, 인증받은 폭발물탐지시스템에 의한 검사, 또는 폭발물 탐지장치 또는 추적탐지기(trace detector)와 같은 기타의 선진기술을 이용한 검사 등이다. CAPPS 비판론자들은 프로파일링이 아무런 쓸모가 없다고 주장한다. 그들은 항공분야 밖에서의 프로파일링이 성공하지 못하였음을 지적하였다. 예컨대, 미국의 세관국(Customs Service)은 프로파일링을 이용하여 마약거래를 중지시키지는 못하였다. 프로파일링 시스템 비판론자들은 또한 CAPPS가 있었다 하더라도 미국내에서의 상업항공기에 대한 최초의 공식적인 폭파사건도 방지하지 못하였을 것이라고 주장하였다. 그 최초의 사건은 1955년 어느 승객의 아들이 보험금을 타기 위해 그녀의 어머니의 짐속에 몰래 폭탄을 집어넣은 사건이었다. 이를 전혀 의심하지 아니한 승객은 어떠한 추가적인 보안검색도 받지 않고 탑승하였던 것이다. 프로파일링 비판론자들은 범죄의 의사가 전혀 없는 승객이 사악한 목적으로 조종되었던 이러한 상황에서는 프로파일링도 아무런 효과가 없었을 것이라고 주장한다.

오늘날에도 역시 “false negative”의 리스크가 위험한 사람이나 물건을 찾아내지 못하는 경우 현실화될 것이다.[22] 따라서 항공사 승객프로파일링시스템 비판론자들은 CAPPS의 이론과 운영 및 관련 프로그램이 지나치게 광범위한 대상을 선정함으로써 승객의 과반수를 대상으로 하면서도 정작 진짜 대상을 놓치는 것이라고 폄하한다.

항공사 승객프로파일링 비판론자들은 또한 만약 정밀검색 대상이 되는 승객을 찾아내기 위한 경쟁 가능성에 대해서도 우려를 표명하고 있다. DOT는 CAPPS의 변형시스템들은 승객의 인종, 종족, 종교 또는 성별에 기반을 두고 있지 않다고 지적하였고 Gore Commission도 프로파일링은 인종, 종교 또는 출신국과 같은 위헌소지가 있는 특성에 관한 정보를 포함하여서는 아니 된다는 점을 언급함으로써 인종에 기초한 프로파일링을 막기 위한 안전장치를 사용하도록 공식적으로 권고한 바 있다. 이러한 안전장치는 리스크를 예측할 수 있는 것으로 입증된 데이터에 기초한 검증된 프로파일 요소들만 이용할 것, 프로파일링 기록의 확산에 대한 엄격한 제한을 설정할 것, 그 시스템을 감시하고 시민의 자유가 훼손되지 아니하도록 보장하기 위한 독립적인 패널을 설치할 것, 그리고 효과적인 폭발물탐지시스템이 개발될 때까지만 프로파일링을 지속할 것을 강조하고 있다. Gore Commission은 다음과 같은 구체적으로 설명하였다. 즉, 프로파일의 구성요소로 간주되어야 할 요소들은 고정관념 또는 일반화가 아닌 합리적인 리스크예측이 가능한 것이어야 하며 따라서 측정가능하고 검증가능한 데이터에 기초하여야 한다는 것이다. 또한 선정된 요소들과 불법행위의 위험간의 관계가 입증되어야 한다는 점도 언급하였다. 그 밖에도 동위

22) Anita Ramasastry, “Lost in Translation? Data Mining, National Security and the “Adverse Inference” Problem”, Santa Clara Computer & High Tech. L.J., Vol.22(2006), pp.757-61; Stephen W. Dummer, “False Positives and Secure Flight Using Dataveillance When Viewed Through the Ever Increasing Likelihood of Identity Theft”, J. Tech. L. & Pol'y, Vol.11(2006), p.259.

원회는 자동화 프로파일링시스템에 의하여 선별되는 자 또는 그러한 자의 수하물을 수색하는 절차 또는 심문하는 절차는 모든 승객들을 존중하고 의심하지 않고 효율적으로 대우할 것이 전제가 되어야 한다고 주장하였다.

1997년 미국 법무부도 CAPPS에 사용할 선별기준을 검토하여 CAPPS는 승객을 불법적으로 차별하거나 인종, 종족 또는 종교와 직접 연관되는 이름이나 복장과 같은 승객의 특징을 포함시켜서는 아니된다는 견해를 제시하였다. 미국 법무부는 CAPPS는 어떠한 승객 집단에게 부당한 (다른 승객들과는) 다른 영향을 미치지 아니할 것이라는 결론을 내렸다. 그럼에도 불구하고 프로파일링시스템 반대론자들은 Gore Commission의 공식적인 목표를 외양만 그럴듯한 것이며 법무부의 결론은 믿을 수 없는 것이라고 판단하였다.

마지막으로 일부 CAPPS 비판론자들은 표면상으로는 항공사 승객프로파일링을 위하여 사용되는 정보의 출처, 무결성 및 잠재적 영향에 대하여 의문을 제기하였으며, 특별히 테러 또는 항공보안과 관련이 없는 목적을 위하여 다는 정부기관에 CAPPS 프로파일을 유포시킬 수도 있다는데 주목하였다. 미국시민권연맹(American Civil Liberties Union: ACLU)은 특히 프로파일링시스템이 다음과 같이 개인 프라이버시를 침해할 가능성이 있다는 우려를 표명하였다: 컴퓨터활용 프로파일링시스템은 그 성격상 핵심적인 프라시버시 원칙과 충돌하는 것이다. 어떠한 하나의 목적을 위하여 제공된 정보는 그 정보의 관련자의 동의 없이는 다른 목적으로 사용되어서는 아니된다. 사람들은 자신들에 관한 데이터를 대규모 프로파일링시스템을 위해 제공하기를 원해서가 아니라 여행을 하기를 원해서 그리고 기회가 되면 공짜 여행을 하기를 원해서 항공권을 구입하거나 상용여객우대프로그램에 등록을 하는 것이다. 컴퓨터활용 프로파일링시스템은 항공사가 프로파일링이외의 목적으로 수집한 승객들의 방대한 데이터에 의존하고 있다. 항공사가

승객이 이름, 주소, 특정한 항공편에 탑승하여 여행한 목적지, 승객의 항공권 지불방법 및 그 승객의 항공권을 지불한 자, 승객의 동반자, 승객이 자동차 또는 호텔 등 여행을 계속하기 위한 예약을 하였는지의 여부 및 기타 정보를 포함한다. 이러한 개인적 데이터는 보호되어야 할 필요가 있다.

항공보안을 약화시키지 않고 항공기 승객의 프라이버시를 보호하기 위해 ACLU는 다음과 같이 프로파일링이 아닌 다른 보안조치를 상정하였다. 즉, 판에 박은 듯한 내용이 아니라 합리적이고 명확한 근거에 입각하여 의심이 가는 범죄활동에 대한 확실한 증거를 찾아내기 위하여 보안요원들을 훈련시킬 것, 항공사 직원 및 항공보안업체의 직원들의 합헌적 방법에 의한 검색 및 외국공항에서의 보안기준을 집행하기 위한 조치를 취할 것, 범죄의 추정원인에 입각한 법원의 명령에 의한 경우를 제외하고 승객 기록물에 대한 FBI 및 법집행기관의 접근을 제한할 것 등이다. 9.11테러사건이후 항공보안정책 수립자들은 CAPPS의 능력을 제고하는 방향으로 전환하였다.

(2) CAPPS Ⅱ

2001년 9월 11일 미국에서 테러주의자들이 항공기를 탈취하여 세계무역센터와 국방부로 돌진함으로써 미국 항공업계를 뒤흔들었으며 규제와 보안 문제에 대하여 각성시킨 바 있다. 이러한 공격에 대응하여 연방항공청(Federal Aviation Administration: FAA), 새로 설치된 국토안보부(Department of Homeland Security), 운송보안청(Transportation Security Administration: TSA) 등 미국 정부기관들은 지상에서의 항공보안 개선 및 여객에 대한 사전검색(pre-screening)을 통하여 미국영토에 대한 추후의 테러공격을 방지하기 위한 방법을 모색하여 왔다.[23] 그 무렵 이

23) Yousri Omar, “Note, Plane Harassment: The Transportation Security Administration's Indifference to the Constitution in Administering the Government's Watch Lists”, Wash.

미 민간데이터마이닝(data mining) 회사들은 수백만 미국인들의 신원확인가능한 방대한 정보를 구입·판매 및 편집(compiling)하고 있었다. 이들 회사들은 다른 회사들이 그들의 고객들을 찾아내는 것을 돕기 위하여 개인의 거의 모든 구입, 거래 및 상호 교류(interaction)를 추적·기록하여 그 정보를 당해 개인에 관한 많은 데이터를 포함하는 다른 정보와 결합시키는 작업을 수행하였다. 그러므로 이러한 데이터마이닝회사들은 개개의 미국인들이 어떠한 사람이며 그들이 빌린 비디오에서부터 구입한 책에 이르기 까지 무엇을 좋아하고 싫어하는지에 관한 방대하고 세부적인 프로파일을 편집하여 왔던 것이다. 수많은 데이터마이닝회사들은 9·11테러이후 처음에는 정부에 접근하였으며 승객프로파일링 프로그램을 개선하기 위하여 그들의 방대한 자료들을 제공하였다.[24] 그 결과 개인데이터마이닝회사들은 당시 존재하던 CAPPS(Computer Assisted Passenger Pre-Screening System)를 CAPPS-Ⅱ로 전환시키는데 모든 노력을 경주하였다.[25] 최초의 CAPPS는 항공사와 FAA가 1998년 수립한 것으로 오직 승객의 이름을 알려진 테러리스트 명단과 대조만으로도 승객을 가려낼 수 있는 능력을 가지고 있었다.[26]그런데 2002년 CAPPS-Ⅱ는 CAPPS의 보다 정밀한 신원확인을 가능하게 하기 위하여 도입하기 위하여 개발되었으며 CAPPS에 승객의 관련 특성을 적용함으로써 그 승객의 리스크를 평가하는 컴퓨터 활용 알고리즘(algorithm)을 추가하였다.

---

& Lee J. C.R. & Soc., Vol.12(2006), pp.260-61, 269-70.

24) U.S. Dep't of Homeland Sec., Office of Inspector Gen., Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (2005) p.25, available at http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr-05-12Mar05.pdf (이하 “DHS Report on TSA”이라 한다.

25) Anita Ramasastry, “Lost in Translation? Data Mining, National Security and the “Adverse Inference” Problem”, Santa Clara Computer & High Tech. L.J., Vol.22(2005), pp.784-86.

26) DHS Report on TSA, op.cit., pp.9-10.

9. 11. 테러사건 조사결과 CAPPS의 여러 가지 미비점이 발견되었다. 이에 따라 이 시스템을 근본적으로 보완하기 위하여 TSA에서 CAPPS Ⅱ 도입을 검토하였다. 또한 2001년 11월 제정된 미 교통보안법에서 모든 공항에 CAPPS를 설치하도록 의무화하였다. CAPPS와 달리 CAPPSⅡ는 많은 정보를 토대로 해당승객의 위해 여부를 판단하게 되며 신분을 정확히 하기 위하여 승객의 성명, 주소, 전화번호, 생년월일, 여행일정 등을 방대한 데이터베이스에 입력시킨 다음 이를 범죄자나 테러범 명당이 입력된 다른 데이터베이스와 대조하여 시스템상 3등급으로 구분한다. 적색으로 분류된 승객은 탑승이 거부되고, 황색은 보안검색대에서 추가 정밀검사 및 조사의 대상이 되며 녹색은 정상적으로 보안검색대를 통과할 수 있도록 하였다.[27]

9.11테러 당시 납치된 비행기 4대중 3대는 5명의 테러리스트가 탑승하였지만 유나이티드항공 093편은 유일하게 4명의 테러리스트가 탑승하였다. 그리고 실제 목표물로 추정된 백악관 또는 국회의사당이 아닌 서부 펜실베니아 들판에 추락하면서 테러는 실패로 돌아갔는데 여기에는 프로파일링이 중요한 역할을 하였다 테러범중 1인 모하메트 알 카타니가 2001년 8월 4일 올랜도 국제공항을 통하여 미국에 입국, 다른 테러범과 합류 예정이었으나 항공분야 프로파일링의 중요성이 부각되기 전에도 다양한 경험과 체험으로 프로파일링을 체득한 입국심사관의 활약에 의해 미국입국이 좌절되었다. 그는 26년의 군생활 및 12년간 이민감독관으로 세관과 국경보호 부서에서 재직하였으며 군 생활에서 효과적인 듣기와 몸짓 관찰 등의 기술을 습득하였고 이민감독관 생활에서 위조문서 감지기술 및 인터뷰기법을 교육받았다.[28]

27) 황호원・이규황, op.cit., p.160.
28) Ibid., p.161.

미국의 고급관리는 CAPPS Ⅰ의 후속 프로파일링시스템을 국가 항공보안 인프라의 유일한 가장 중요한 구성요소라고 규정지었다.[29] CAPPSⅡ는 완전한 성명, 집주소, 전화번호 및 출생년월일을 포함하는 각 여행 승객이름(passenger name records: PNRs)을 보안평가를 위한 정부의 데이터베이스와 대조함으로써 상업적 항공기 승객의 신원 진위를 가리기 위하여 마련된 것이었다.[30] CAPPSⅡ의 목적은 법집행기관 데이터베이스 및 정보기관(intelligence) 데이터베이스의 갭을 메우는 것이었다. CAPPSⅡ는 또한 검색과정에서 그에게 의심되는 점을 발견하게 되면 여행과 무관한 사건의 경우에서도 법집행 관리에게 통보하였을 것이다. CAPPSⅡ가 반테러의 목적을 위하여 상업적 데이터베이스를 이용한다는 것 자체에 대해서도 논란이 많았다.

반대론자들은 항공기 여행과 무관한 목적을 위하여 상업적 데이터베이스를 이용함으로써 항공기 여객의 헌법상의 권리를 침해하게 된다고 주장하였다. 예컨대, 파산을 신청한 또는 신용카드청구 금액의 지불이 늦어진 항공기 승객은 불량신용의 리스크가 있지만 재정적인 지급불능상태 때문에 테러의 위협의 가능성이 있는 것은 아니다. 그럼에도 불구하고 프로파일링시스템은 경제적인 곤경을 “미심적음”(shiftiness)으로 간주하여 버리게 된다.[31] 이러한 상황에서 CAPPSⅡ 비판론자들은 항공기 여행의 안전을 위하여 상업적 데이터베이스를 이용하는 것을 승객의 프라이버시의 권리에 대한 허용할 수 없을 정

29) Deborah von Rochow-Leuschner, “CAPPS II and the Fourth Amendment: Does It Fly?”, J. Air L. & Com., Vol.69(2004), pp.139-46; Michael J. DeGrave, “Note, Airline Passenger Profiling and the Fourth Amendment: Will CAPPS II Be Cleared for Takeoff?”, B.U. J. Sci. & Tech. L., Vol.10(2004), p.151.

30) Yousri Omar, “Note, Plane Harassment: The Transportation Security Administration's Indifference to the Constitution in Administering the Government's Watch Lists”, Wash. & Lee J. C.R. & Soc. Just., Vol.12(2006), pp.271-72.

31) Chris Jay Hoofnagle, “Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement”, N.C. J. Int'l L. & Com. Reg., Vol.29(2004), p.595.

도의 높은 대가를 치르도록 하는 것이라고 주장하였다.

시민권 및 프라이버시 옹호론자들은 CAPPSⅡ를 좌절시키기 위하여 CAPPS Ⅰ의 몇 가지 운영상의 실패사례를 발표하였다. 2004년 9월 영국의 대중가수 Cat Stevens(그는 1970년대 무슬림이 되었으며 개명하여 현재는 Yusuf Islam으로 알려져 있다)는 미국발 항공기의 탑승이 거부되었다. 그의 이름이 미국 정부의 탑승거부자 명단(“No-Fly” list)에 올라있었던 것이다. CAPPSⅠ은 또한 미국의 상원의원 Edward M. Kennedy와 하원의원 Dong Young를 추가 보안검색의 대상으로 분류하였다. CAPPSⅡ 반대론자들은 이 사례를 들어 항공사 승객프로파일링 시스템은 합법적으로 또는 신뢰할 정도로 항공기 여행을 더욱 안전하도록 하지 못할 것이며 오히려 승객에게 뜻하지 아니한 부정적인 결과를 초래할 것이라고 주장하였다.

결국, CAPPSⅡ를 둘러싼 주된 우려는 어떠한 목적을 위하여 의도된 정보가 다른 목적으로 이용될 수 있다는 “mission creep”(슬금슬금 업무를 확장하는 것)이었다. CAPPSⅡ 비판론자들은 항공기 승객 프로파일링이 포함된 정보는 점차 항공보안외의 목적으로 TSA외의 다른 정부기관들에게 흘러들어갈 것이라고 주장하였다. 이로 인하여 항공사 승객프로파일링 시스템은 침습성(invasiveness)이라는 특징을 가지게 될 것이라는 것이다.

예컨대, 만약 어떠한 사람이 Amazon.com이 다른 고객의 구매패턴에 근거하여 권고한 서적을 구입하지 아니하였다면 부정적인 결과는 경미하다. 만약 신용카드회사가 비상례적인 사용형태를 확인하고 다른 사람이 본인의 카드를 훔쳤을 것이라고 판단하였기 때문에 본인의 카드 사용을 정지시켰다면, 본인은 상황에 대해 설명하고 다시 카드를 사용할 수 있다. 그러나 반테러 목적을 위하여 그 데이터를 이용한다면 결과는 훨씬 더 심각해질 것이다. 체포, 강제출국, 실직, 여러 검색

대에서의 강화된 검색, 수사 또는 감사 및 요주의인물 명단에의 추가 등의 불이익을 당하는 결과를 초래할 수 있다.

이러한 비판은 TSA에 전달되어 TSA는 결국 제안된 CAPPSⅡ계획안에 대해 다음과 같은 몇 가지 중요한 수정안을 제시하였다. 첫째, TSA는 승객이 그들의 예정된 여행을 마친 후 7일내에 CAPPSⅡ 시스템상의 대부분의 승객 정보를 삭제하고, 둘째, 실수로 제2차 정밀보안검색의 대상이 된 승객을 위한 이의제기 메커니즘을 마련하며, 셋째, 오직 승객의 신원 확인을 위한 목적으로만 상업적 데이터 제공자에게 PNR 정보를 전송하겠다는 것이다. 더욱 더 중요한 것은 TSA는 여행자의 보안 프로파일을 구성하기 용도로 개인의 상업적 데이터의 이용을 제한하겠다는 것이다. 상업적 데이터마이너들(data miners)은 어떠한 승객이 예약시 제시한 신원정보와 일치하는가를 평가하게 될 것이다. CAPPSⅡ시스템은 이러한 진위 확인과정을 완료하는 즉시 승객의 상업적 신원정보를 법집행기관의 데이터베이스와 정보기관의 데이터베이스와 대조하게 된다. 승객이 그러한 데이터베이스와 다르지 아니한 것으로 확인된 경우, 항공여행을 위한 절차를 계속할 수 있을 것이다. 만약 주목할 만한 프로파일을 가진 승객은 추가조사 또는 법집행조치의 대상이 될 것이다. CAPPSⅡ 반대론자들은 이러한 조치들은 소기의 목적을 달성하는데 부적절한 것이며 따라서 CAPPS Ⅱ가 결코 성공할 수 없다고 판단하였다.

외부의 비판론 및 그 내용적인 문제외에도 CAPPSⅡ는 시장재앙적 성격을 가지고 있기 때문에 좌절되었다. 즉, 중요한 일반인의 논평을 위한 통지를 하거나 그러한 논평기회를 부여함이 없이 시스템을 개발함으로써, TSA는 프라이버시 옹호론자들이 CAPPSⅡ가 시민에게 적법절차를 부인하게 될 것이라는 우려를 무시하였던 것이다. CAPPSⅡ가 비공개적으로 개발되었다는 사실은 연방정부가 헌법을 위반하였다는 시민의 자유 옹호론자들의 비난을 더욱 거세게 만들었다.

일부 항공사들이 CAPPSⅡ시스템을 시험하기 위하여 그들 각자의 승객 명단을 자발적으로 TSA에 제공하였다는 것이 알려지자 CAPPSⅡ프로그램 반대론은 절정에 달했다. 예컨대, JetBlue Airways는 데이터마이닝 정부 도급업자에게 900만명의 승객 기록(이금, 주소, 전화번호 등)을 제공하였다는 이유로 피소되었다. 소비자 조사회사(consumer research company)는 직업, 수입, 성별, 집과 차량 소유 경력 및 가계구성을 포함하고 승객의 정보가 담긴 이러한 기록들을 평가하였는 바, 이 정보에는 자신의 신원이 공개되는 승객의 인지 또는 동의 없이 수집되고 전송되었다. 또 다른 항공사들은 CAPPSⅡ 개발을 위하여 연방정부와 협력 작업을 하였다는 이유로 피소되었다.[32] 결국 CAPPSⅡ는 PNRs 데이터의 상업적 데이터베이스 및 법집행기관 데이터베이스와의 결합 우려로 인하여 좌절되었다. 미국 General Accounting Office가 TSA가 CAPPSⅡ의 프라이버시 계획을 마무리할 때까지 그 시스템이 Privacy Act에 완전히 부합될 것임을 보장할 수 없다고 보고한 후인 2004년 7월 13일 TSA는 CAPPSⅡ 계획을 포기하였다.

(3) 미국에서의 프로파일관련 소송과 법적 구제

1) 의 의

2001년 9월 11일 이후 미국정부는 자국의 항공안전을 보장하기 위한 노력을 배가하였다.[33] 전자 프로파일링·사전검색 프로그램들도 그러한 노력의 일환인 바 이 프로그램은 장래 있을 수 있는 항공기납치범아 탑승하기 전에 제지하기 위한 목적을 가지고 있다.[34] 최근 미

32) Richard Sobel & John A. Fennel, “Troubles with Hiibel: How the Court Inverted the Relationship Between Citizens and the State”, S. Tex. L. Rev., Vol.48(2007), p.613; Drew Shenkman, “Comment, 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”, Alb. L.J. Sci. & Tech., Vol.17(2007), p.4.

33) Omar, op.cit.

34) Ibid. pp.269-70, 285-86.

국에서는 항공사에 의한 개인 데이터 정보의 공개로 인한 집단소송이 제기되었다. 피소되지 아니한 그 밖의 항공사들도 승객의 개인 데이터를 제3자에게 공개하였음을 인정하였다는 점에서 이와 유사한 소송이 앞으로도 뒤이을 것으로 예상된다.[35]

미국의 항공사들이 미국 정부기관에 데이터를 공개한 것은 그들의 자발적 의사에 의한 것이며 법원의 서류제출요구나 또는 행정기관의 법적 근거에 따른 요청에 의한 것은 아니었다.

새로운 CAPPSⅡ 프로그램을 테스트하기 위하여 미국 정부기관들은 데이터를 필요로 하였으며 많은 미국 항공사들이 정부기관의 요청에 의하여 또는 자발적으로 정부기관과 민간정보 도급업자(contractor)들에게 광범위한 승객정보를 제공하였다.[36] 그러나 그와 같이 제공된 데이터는 많은 부분이 민간기업들로 부터 얻은 다른 데이터와 결합되어 있었기 때문에 데이터의 개인 프라이버시 침해가능성이 커지게 되었다. 뿐만 아니라 정부의 민간도급업자들이 새롭게 얻어진 승객 데이터를 향후에도 구입·판매하지 아니할 것이라는 보장도 없었다.[37] 일반인들이 항공사에 의한 데이터의 공개 사실을 처음으로 알게 된 것은 2003년 9월 JetBlue Airways가 민감한 승객정보를 정부도급업자에게 공개하였음을 최초로 인정함으로써 비롯되었으며 그 후 다른 항공사들도 그러한 행위를 하였음을 시인함으로써 많은 집단소송이 원인이 되었다.[38]

JetBlue Airways,[39] American Airlines[40] 그리고 Northwest Airlines는[41]

35) Shenkman, op.cit., p.

36) DHS Report on TSA, op.cit., pp.25-26.

37) Deborah von Rochow-Leuschner, “CAPPS II and the Fourth Amendment: Does it Fly?”, J. Air L.& Com., Vol.69(2004), pp.147-48.

38) Shenkman, op.cit., p.7.

39) In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005); Privacy Rights Clearinghouse v. JetBlue Airways Corp., No. D045568, 2005 WL 3118798 at 1 (Cal. App. 4th Dist. 2005).

40) In re Am. Airlines, Inc. Privacy Litig., 370 F. Supp. 2d 552 (N.D. Tex. 2005).

모두 각기 다른 집단소송의 피고가 되었는 바, 이러한 집단소송에서 원고들은 이들 항공사들이 정부기관이나 제3의 회사에 승객이름기록(Passenger Name Records: PNRs)을 넘겨줌으로써 승객의 사적인 이익을 침해하였다고 주장하였다. PNRs는 승객의 이름, 항공편 번호(flight number), 신용카드 데이터, 호텔・렌트카 예약 및 여행동반자 유무 등에 관한 정보로 구성되어 있다. 아마도 PNRs는 항공기에 탑승한 승객에게 안전을 제공하는 것과 관련한 개인적인 건강정보를 알 수도 있을 것이다.[42] 그러나, PNRs상의 정확한 정보는 항공사마다 다르다.

항공사들은 승객들이 인터넷을 통하여 또는 전화상으로 항공사여행을 구매하는 때에 PNRs정보를 수집한다.[43] 교통안전청(Transportation Security Administration: 이하 "TSA"라 한다)은 승객의 항공기 탑승을 위하여 완전한 성과 이름(full name)을 요구할 수 있으며[44] 법령에 의하여 항공사로부터 승객명단을 요구할 수 있는 권한을 가지고 있다.[45] 뿐만 아니라 일부 항공사들은 항공권 판매시에 출생연월일과 신용카드번호 그리고 때로는 승객의 항공에 필수적이지 아니한 데이터를 요구한다.[46] 이러한 정보는 항공사의 개인항공사의 개별적인 PNRs 데이터베이스에 입력되어 흔히 마케팅 목적으로 이용되는 승객 프로파일을 만드는데 사용된다.[47] 또한 항공사의 웹사이트들은 자신들이 제3자와 재정 및 개인 정보를 공유하지 아니하며 개인이 제공한

41) In re Nw. Airlines Privacy Litig., No. Civ. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196 (D.N.D. 2004).

42) Jay Boehmer, TSA Demands PNR Data: Secure Flight Program Renews Privacy Issues, Bus. Travel News Online, Oct. 4, 2004, http://www.btnmag.com/businesstravelnews/headlines/frontpagedisplay.jsp?vnucontent id=1000651781.

43) In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 304 (E.D.N.Y. 2005).

44) Boehmer, op.cit.

45) DHS Report on TSA, op.cit., p.5.

46) Boehmer, op.cit., p.13.

47) In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d at 304.n23.

정보는 안전한 서버에 의하여 보호를 받는다는 프라이버시 정책을 천명하고 있었다.

아래에서는 2001년 9월 11일 이후 제기된 몇 개의 주요 집단소송사건과 관련된 법적 쟁점을 간략히 분석함으로써 미국 법원의 입장을 확인하고자 한다. 이 문제를 다루어온 법원들은 승객이 주장하는 법적 구제 대부분을 기각함으로써 프라이버시권을 침해받았다는 승객의 주장을 받아들이지 아니하였다. 사실, 항공사가 민감한 개인 데이터를 다른 자들과 공유함으로써 당사자의 프라이버시가 침해되었거나 침해될 가능성이 있다면 그에 대한 규제가 필요한 것이지만 항공테러의 방지 더 나아가 국가안보라는 중대한 요청과의 충돌이 발생할 수도 있다. 이어서 이러한 소송과 관련된 몇 가지 법적 쟁점들을 미국의 전자통신프라이버시법(Electronic Communications Privacy Act: ECPA)과 The Airline Deregulation Act 0f 1978(ADA)와 결부시켜 분석하게 될 것이다.

2) 몇 가지 집단소송사건 판결

① Northwest Airlines 집단소송

Northwest Airlines사건에서 미국의 국가항공우주국(National Aeronautics and Space Administration: 이하 “NASA”라 한다)은 2001년 9월 11일 사건 직후 항공사보안연구(airline security study)를 수행하기 위하여 Northwest 항공사에 3개월 동안의 승객데이터를 공개해주도록 요구하였다.[48] 그 후 NASA의 그러한 비상례적인 요청은 CAPPSⅡ를 위한 알고리즘 테스트 때문이었음이 드러났다. 즉, Northwest는 NASA에 2001년 7월부터 12월까지 탑승한 승객에 대한 PNRs를 제공하였으며 Northwest의 국가항공우주국에 대한 승객 데이터 공개사실은 2003년 후반기에 비

48) Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1197 (D.N.D. 2004).

로소 일반인에게 알려지게 되었다. 이에 따라 여러 건의 집단소송이 연방법원에 제기되었는 바, 예컨대, North Dakota에서 일단의 승객들이 소송을 제기하였으며, Dyver v. Northwest Airlines Corp.가 바로 그 사건이다. 그 밖에도 Minnesota에서 몇 건의 소송 그리고 Tennessee에서 한 건의 소송이 병합되어 In re Northwest Airlines Privacy 소송이 되었다.

② JetBlue Airways 집단소송

Northwest 소송이 정부기관인 NASA에 직접적인 승객정보 공개와 관련되어 있는 반면에 JetBlue 사건은 정부의 민간도급업자에게 PNRs를 공개한 것과 관련되어 있다.[49] 국방부(Department of Defense)의 데이터마이닝 도급업자인 Torch Concepts의 요청에 따라 JetBlue Airways의 데이터관리 도급업자인 Acxiom은 2002년 9월 약 5백만건의 PNRs를 제공하였다. 그 후 Torch는 제공받은 PNRs를 더 많은 데이터와 결합시켜 도급업자인 SRS Technologies와 함께 프로파일링 사전검색프로그램을 제작하였다. 그러나 PNRs는 정리된 후, 미국 국방부가 어떠한 사람들이 - 항공보안이나 CAPPs-Ⅱ가 아닌- 군사기지 보안에 위험요소가 될 것인가를 예측하기 위한 목적을 위하여 데이터 유형분석을 하는데 제공되었다. 본토안보부(Department of Homeland Security: DHS) 보고서에 따르면 JetBlue는 TSA에게 CAPPSⅡ와 유사한 정부 프로그램의 완전성 확보를 위하여 사용할 수 있도록 요청받은 PNRs를 제공한 것으로 판단하고 있었다. 이 프로그램의 목적은 군사기지 부근을 비행하는 승객의 안전을 목표로 한 것이며 군사기지 자체의 안전 확보를 위한 것은 아닌 것이었다.[50] JetBlue가 PNRs를 Torch에

49) In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 304-05 (E.D.N.Y. 2005).

50) Shenkman, op.cit., p.8.

인계한 사실을 공개함에 따라, 승객들은 여러 지역에서 제기된 소송을 병합하여 집단소송을 미국의 뉴욕 동부지구 지방법원에서 제기하였는 바, In re JetBlue Airways Corp. Privacy Litigation이 그것이다. 2004년에는 이와 유사한 소송이 캘리포니아 주법원에 제기되었다. 바로 Privacy Rights Clearinghouse v. JetBlue Airways Corp.사건이다.

③ American Airlines 집단소송

American Airlines는 정부기관인 TSA와 4개의 민간 데이터수집회사에 PNRs를 공개하였다. 승객들은 120만 PNRs의 공개를 이유로 American Airlines와 이 4개의 회사들을 상대로 소송을 제기하였다.[51] TSA가 American Airlines로 하여금 TSA 및 TSA와의 도급계약체결을 위해 경쟁하는 4개의 민간 도급회사들에 PNRs를 넘겨주도록 요청하였다는 점은 명백하였다. 이 소송은 American Airlines의 PNRs가 Airline Automation, Inc.(AAI)이라는 별도의 회사가 보관하고 있었다는 점에서 독특한 성격을 지니고 있었다. American Airlines는 AAI가 PNRs를 TSA에 넘겨주는 것은 허용하였지만 그 4개의 민간 데이터수집회사들에게는 허용하지 아니하였다고 주장하였다. 승객들은 텍사스 북부지구 지방법원에 전국적인 집단소송을 제기하였는 바, In re American Airlines Inc., Privacy Litigation(American Ⅰ)사건이 그것이다. 전자통신프라이버시법(Electronic Communications Privacy Act: 이하 "ECPA법"이라 한다)과[52] 주법에 근거한 청구가 American Ⅰ사건에서 기각된 후 법원은 원고 승객들에게 계약에 근거하여 손해배상을 청구한 그들의 소장 변경을 허용하였으며 그에 따른 재심리 결정은 American Ⅱ이라고 부른다.

51) In re American Airlines, Inc. Privacy Litig. (American I), 370 F. Supp. 2d 552, 555 (N.D. Tex. 2005).

52) Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§2701-2711 (2000).

3) 청구의 법적 근거

① 개 요

집단소송의 원고인 승객들은 항공사를 상대로 그리고 일부 소송절차에서는 항공사로부터 PNRs을 넘겨받은 제3자인 회사들을 상대로 소송을 제기하였다. 청구는 다음 3가지로 크게 분류된다. 첫째, ECPA법에 근거한 청구, 둘째, 주의 공정거래법 및 기타 관련법에 의한 청구 그리고 이러한 주법들에 대하여 항공산업규제완화법(Airline Deregulation Act of 1978: 이하 "ADA법"이라 한다)이[53] 우선적 효력을 갖는지의 여부, 셋째, 주법의 계약상의 구제수단에 의한 청구 등이다. 미국에서 프라이버시권의 청구는 단순히 일반적인 프라이버시 침해행위로 부터 기인한 것이거나 ECPA법에 의거하는 것만도 아니다. 승객들이 주장한 컴몬로와 주법상의 청구는 항공사에 의한 개인정보의 공개를 저지하는 강력한 수단이 되었다. 승객 개인 정보의 공개를 이유로 한 항공사에 대한 공개억제와 징벌적인 손해배상은 승객의 궁극적 목적이다.[54] 이 보고서에서 소개하는 다섯 개의 집단소송중 한 건만이 기각청구에도 불구하고 진행되어 계류중이인 바, 계약상의 청구(contract claim)에 관한 재심리를 기다리고 있는 American Ⅱ가 그것이다. 각기 JetBlue Airways와 Northwest Airlines를 상대로 한 나머지 집단소송들은 기각되었다.

② 관련 법 적용상의 문제에 관한 분석

가. ECPA법에 의거한 청구

1986년 미국 의회는 통신기술의 발전에 따른 일반인의 프라이버시에 대한 관심에 부응하여 ECPA법을 의결하였다.[55] 간단히 말해서

53) Airline Deregulation Act (ADA) of 1978, 49 U.S.C. § 41713 (2000).
54) Shenkman, op.cit., p.10.

ECPA법은 프라이버시 침해에 대한 국내적인 감시를 위한 규정을 두고 있다.[56] 상기의 집단소송과 관련된 것은 전자적 저장(electronic storage)에 의한 통신(communications)을 규율하는 ECPA법의 "Stored Communications Act"이다.[57] 6건의 집단소송중 4건에서 원고인 승객들은 항공사가 ECPA법의 규정을 위반하였다고 주장하였는 바, 전자적으로 저장된 PNRs이 승객의 동의 없이 누설되었기 때문에 ECPA법이 적용된다고 주장하였던 것이다.[58] 형법상의 규정에도 불구하고 ECPA법은 1,000달러 이상의 손해배상액, 합리적인 변호사비용 및 징벌적 손해배상의 가능성 등을 포함하여 동 법의 위반에 대한 개인의 소송제기의 권리에 대하여 규정하고 있다.[59] ECPA법의 두 개조가 특히 이와 관련되어 있는 바, 제2701조는 권한 없는 전자적 접근 그리고 제2702조는 권한없는 공개를 다루고 있다.

**<제2701조: 권한없는 접근>**

제2701조(a)는 저장된 전자적 정보에 대한 권한 없는 접근을 금지하고 있다. 제2701(b)조는 (1) 전자통신서비스가 제공되는 시설에 권한없이 고의로 접근하거나 (2) 당해 시설에 접근할 수 있는 권한을 고의로 유월한 자에 대한 벌칙을 규정하고 있다. 2005년 텍사스주 북부지구 지방법원은 American I 사건에서 다른 법원들이 제2701(a)조를 反해킹(hacking) 법조항으로 그 성격을 규정지어왔음을 지적하였다. 제2701조와 관련하여 자주 인용되는 사건인 In re Doubleclick Inc. Privacy Litigation에서 뉴욕주 남부지부 지방법원은 정보에 대한 권한

55) Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act", Geo. Wash. L. Rev., Vol.72(2006), pp.1564-65.

56) Daniel J. Solove, "Reconstructing Electronic Surveillance Law", Geo. Wash. L. Rev., Vol.72(2004), p.1264.

57) 18 U.S.C. §§2701-2711 (2000).

58) Solove, op.cit., p.1283.

59) 18 U.S.C. § 2707 (2000).

없는 접근이 개인의 프라이버시의 권리 침해를 구성하는 필요적인 요소임을 강조하였다. 이 사건에서 인터넷사용자들은 자신들의 개인 컴퓨터상의 쿠키(cookies)를 저장한 것은 프라이버시의 권리를 침해한 것이라고 주장하며 인터넷 광고업자 Doubleclick사를 제소하였다. Doubleclick사는 자신의 제휴(affiliated) 웹사이트들이 유저(users)이며 원고들의 이들 웹사이트들과의 모든 통신은 권한(authorization)에 해당한다고 반론을 제기하였다. 법원은 원고들이 제2701조에 의하여 요구되는 있는 바와 같이 어떠한 접근이 권한 없이 이루어진 것이라는 증거를 제시하지 못하였음을 지적하고 그 웹사이트들의 방문자들에 의한 묵시적 권한(implicit authorization)이론을 확립하였는 바, 이는 American Ⅰ사건 판결과 Northwest 사건 판결에서도 유사하게 유추하여 적용되었다.[60]

현재 계류중인 사건들중에서 American Ⅰ과 Northwest 승객들만이 제2701조(a) 상의 청구를 제기하였다. American Ⅰ 법원과 Northwest 사건 법원은 모두 항공사에 의한 PNR의 제3자에의 제공은 “unauthorized access”에 해당하지 아니한다는 주장을 기각하였다. 승객들은 PNR의 이용에 대하여 이의를 제기한 반면에 제2701(a)조는 unauthorized access 만을 다루고 있다. American Ⅰ 법원은 데이터베이스의 권한 있는 접근권을 가진 자의 경우에는, 그의 접근의 의도된 이용이 아무리 악의적이거나 절도에 해당하는 것이라 하더라도, 제2701조의 위반에 해당하지 아니한다고 부언하였다. 이러한 논지에 따라 항공사를 상대로 한 제2701(a)조에 의거한 배상청구는 기각되었다. American Ⅰ사건에서 AAI를 상대로 한 승객들의 제2701(a)조에 의한 소송도 비록 American이 AAI가 비정부적 실체인 제3자에의 정보제공을 위한 PNRs 접근권을 유월하였다고 주장하였음에도 불구하고 이와 유사한 논지로 기각되었다.

60) Shenkman, op.cit., p.11.

**<2702조 권한없는 공개>**

제2702조는 PNRs를 제3자에 누설함으로써 자신들의 개인 정보를 권한 없이 공개한 것이라는 승객의 이의와 더욱 직접적으로 관련되어 있다. 제2702조는 일정한 예외를 두고 있지만 원칙적으로 전자적 통신서비스 또는 원격컴퓨팅(remote computing)서비스를[61] 제공하는 자는 (1) 어떠한 자에 대하여 전자적으로 저장되어 있는 통신의 내용을 "알면서도"(knowingly) 그러한 서비스에 의하여 누설하거나 (2) - 그러한 서비스의 고객과 관련된 기록 또는 정보를 "알면서도" 누설하는 것을 포함하여 - 그러한 서비스에서 전달되거나 보관되고 있는 어떠한 통신의 내용을 다른 자에게 "알면서도" 누설하는 행위를 금지하고 있다. 이 조항은 "전자적 통신서비스"를 "무선 또는 전자적 통신을 그 이용자가 송신 또는 수신할 수 있도록 하는 서비스"라고 정의하고 "원격컴퓨팅서비스"를 "전자적 통신시스템에 의하여 공중에게 컴퓨터 저장 또는 처리(processing) 서비스를 제공하는 것"이라고 정의하고 있다. 무엇이 전자적 통신서비스에 해당하는가가 애매하기 때문에 승객의 배상청구와 관련하여 항상 쟁점이 되었다. 뿐만 아니라. 어느 시점에서 항공사들이 제3자에게 PNRs를 누설하였음을 인정하게 되면 "알면서도"라는 요소가 충족된다.[62]

연방법원에 제소된 사건에서 각각 원고들이 제2702조에 의한 주장을 제기함으로써 유사한 논거를 제시하였다. 예컨대, In re JetBlue Airways Corp. Privacy Litigation 사건에서 승객들은 JetBlue는 동사가 웹사이트를 운영하고 있고 동 항공사와 그 고객간에 데이터를 수신하

61) 통신회선 등을 이용해 떨어진 곳에서 컴퓨터를 사용하는 것. 온라인 리얼타임 처리, 리모트 배치처리, 타임 셰어링 처리 등을 포함한 총칭. 이들 각종 서비스를 리모트 컴퓨팅 서비스라 한다. 종전에는 리모트배치 서비스, TSS서비스 등 처리형식에 따라 각각 달리 불렸으나 기술진보에 의해 구별이 명확하지 않게 되어 미국을 중심으로 리모트 컴퓨팅 서비스라는 말이 많이 사용되고 있다. http://enc.daum.net/dic100/contents.do?query1=11XXXX7192

62) Shenkman, op.cit., p.14.

고 전송하고 있기 때문에, 전자적 통신서비스 업체라고 주장하였다. 승객들은 제3자에 PNRs를 누설한 것은 ECPA 제2702조에 의거한 자신들의 프라이버시를 침해한 것이라고 주장하였다.

그러나 관할 법원은 전자적 통신서비스업체는 일반적으로 Internet service provider(ISP)라고 부르는 업체이며 단순히 온라인서비스를 판매하는 업체는 아니라고 판시한 연방법원들의 비구속적인 판례법의 논지에 따랐다. 1998년 Anderson Consulting v. UOP 사건에서 미국 일리노이주 북부지구 지방법원은 일방 당사자가 타방 당사자와 인터넷을 통하여 통신할 수 있다는 이유만으로 ISP에 해당하는 것은 아니라고 판시한 바 있다. 이 사건에서 UOP는 시스템통합사업을 수행하기 위하여 Anderson (Consulting)사를 고용하였던 것이다. UOP의 Anderson과의 계약관계는 UOP가 Anderson사로부터 온 이메일을 월 스트리트 저널에 공개함으로써 파기되었다. Anderson사는 UOP를 ECPA 위반으로 제소하였다. Anderson은 UOP에 의하여 고용되어 있었기 때문에 UOP가 Anderson에 UOP이메일 서비스에 대한 접근을 허용하였던 것이다. 법원은 인터넷을 통하여 제3자가 UOP와 통신을 할 수 있었다는 사실만으로는 UOP가 공중에게 전자적 통신서비스를 제공하였다고 볼 수 없다고 판시하였다. 그 결과, UOP는 여전히 ISP로부터 인터넷 접근권을 구매하여야 했다. 법원은 Anderson의 청구를 기각하였다. Anderson 사건의 관할법원의 판지에 따르면 항공사의 웹사이트는 항공사가 승객에게 인터넷에 접근할 수 있는 수단을 제공하지 않았기 때문에 ISP에 해당되지 아니한다고 볼 수 있다.[63]

2001년에는 Doubleclick 사건 법원이 ISP는 웹사이트 그리고 웹사이트의 이용사들과는 다르다고 판시하였다. 동 법원은 전형적인 ISP라 할 수 있는 American Online 및 Juno등을 이용자자 인터넷에 접근하는 수단을 제공하는 전자적 통신서비스 제공자의 예로 들었다. 또한

63) Ibid.,p.16.

Cryowley v. CyberSource Corp.사건에서 캘리포니아 북부지구 지방법원은 Amazon.com은 비록 그 고객들이 물품의 구매와 관련하여 직접적으로 당해 회사의 웹사이트를 통하여 동 회사와 직접 통신할 수 있다 하더라도 전자적 통신서비스 제공자는 아니라고 판시하였다. 법원은 ECPA법이 유저를 제공자와 달리 취급하고 있다고 지적함으로써 Anderson 사건 판결을 따랐다. 요컨대, JetBlue사건, Northwest사건 및 Dyer사건의 관할법원들도 모두 Anderson, Doubleclick 및 Crowley 사건 판결을 종합해보면 항공사의 웹사이트는 Anderson, Doubleclick 및 Crowley 사건 관할법원이 ECPA가 유일하게 적용된다는 ISP가 아니기 때문에 항공사가 제2702조에 의한 책임을 지지 아니한다고 판시하였던 것이다.

가장 주목할 한 것은 1993년 미국 제9항소법원이 American Airlines의 컴퓨터예약시스템은 전자적 통신서비스에 해당한다고 판시한 United States v. Mullins사건이다. 그러나, Jet JetBlue법원이 언급하였듯이 Mullins사건은 여행대리점이 항공사의 통신내용을 모니터링하여 얻은 범죄혐의에 대하여 다툰 형법상 유선(wire) 사기사건이다. JetBlue법원은 제4차 개정헌법에 대하여 다소 제한적인 형법적 해석하여 쟁점을 다루었기 때문에 Mullins의 청구를 기각하였던 것이다.[64]

보다 최근인 2003년 제1항소법원은 Pharmatrack Privacy 사건에서 온라인 형태의 전송은 전자적 통신이라는 판결을 내렸다. Pharmatrack는 웹 활동을 추적하는 프로그램을 제공하기 위하여 몇몇 제약회사들과 제휴하였다. 그러나 그 과정에서 Pharmatrack는 고객인 제약회사들의 명시적인 요청에 반하여 개인의 신상확인이 가능한 정보에도 접근하였다. Pharmatrack사건 법원은 ECPA는 인터넷 확산 이전에 제정된 법

64) Joanna L. Geraghty, Christopher G. Kelly & Judith R. Nemsick, “District Court Dismissal of In re JetBlue Airways Corp. Privacy Litigation Moves to the Forefront of Courts Dismissing Privacy Claims Against Air Carriers”, Air & Space Lawyer, Vol.20 (2005), pp.405.

령이었기 때문에 동 법령에 대한 문리적인 해석에 대하여 우려를 표명하였다. 그러나, JetBlue 사건법원은 제2702조가 아닌 ECPA의 다른 조항들을 다루었다는 이유로 Pharmatrack 법원의 판지를 받아들이지 않았다.

American Ⅰ 법원은 Anderson, Doubleclick 및 Crowley 사건의 판결과는 다른 입장을 취하여, American Airlines의 행위가 18 U.S.C. 제2702(B)(3)에 의한 책임의 배제사유에 해당된다고 판시함으로써 항공사의 웹사이트가 전자적 통신서비스에 해당하는지의 여부의 문제를 다루는 것을 회피하였다. 이에 따르면 대상이 되는 수신인이 통신에 관하여 동의를 한 경우 통신의 공개도 그러한 책임이 배제된다. 원고들은 American 항공사가 자신의 프라이버시 정책을 위반하였으며 자신들이 어떠한 동의도 한 바 없기 때문에 American 항공사는 책임배제의 대상이 될 수 없다고 주장하였다. 그러나 법원은 제2702조가 사실상 형법적 규정이고 계약위반은 통상적으로 형법상의 책임을 초래하는 것은 아니기 때문에 법원은 원고들의 청구를 기각하고 American 항공사는 제2702(b)(3)의 책임배제의 적용을 받을 수 있다고 판시하였다.

요컨대, ECPA법의 이론에 입각하여 항공사에 책임을 추궁하여 승소할 수 있을 것인가는 명확하지 않다. 법원의 제2701조의 해석에 입각해서 살펴보면 승객이 승소할 가능성은 희박해 보인다. 그 동안 법원들은 제3자에게 PNRs 데이터를 그 사실을 인지하면서도 제공한 항공사는 그러한 데이터에 접근한 권한 없는 제3자와는 다르다는 사실에 초점을 맞추어왔다. 예컨대, American 항공사가 자신의 변론서에서 자신의 도급데이터취급업자(contracted data handler)인 AAI가 PNRs 데이터를 제3자에게 전송할 권한이 없다고 주장하였지만, 재심리과정에서 법원은 원고들이 계약에 근거한 청구를 인용하였다. 그 후 American Ⅱ사건의 법원은 American Ⅰ 사건 법원이 내린 AAI도 역시 ECPA법

상의 책임을 지지 아니한다는 판결을 확인하였다. 이러한 사실을 인용한 법원은 아직은 단 하나에 불과하지만 항공사 외의 당사자들에 대하여 그러한 전략을 추구한다 할지라도 아무런 쓸모가 없을 것임을 시사해주고 있다.

그러한 항공사에 대한 제2702조에 의한 청구를 제출하는 것은 아직은 그 가능성이 없지만 훨씬 성공률이 높을 것으로 판단된다. 민사책임이 존재하는지의 여부는 본질적으로 법원이 항공사의 웹사이트를 동 규정에서 언급한 전자적 통신서비스로 볼 것인지의 여부에 달려있다 할 것이다. JetBlue, Dyer, 및 Northwest 사건의 법원들은 모두 항공사의 전자적 통신제공자가 아니라는 Anderson, Doubleclick 및 Crowley 사건의 판지를 채택하였음에도 불구하고 이러한 판결들은 당해 지방에서만 구속력을  갖는 것일 뿐이다. 비록 다른 지방의 법원들이 이 사건 판결을 합당한 것으로 판단한다 할지라도 또 다른 법원들은 전자적 통신제공자라 함은 단순한 ISP 이상을 의미한다고 판시한 Mullins 와 Parmatrack 법원의 보다 광범위한 시각을 받아들일 수도 있을 것이다. ECPA법은 인터넷 등장이전에 제정된 법령이기 때문에 이 법은 장래의 소송에서도 적용될 수 있는 것이어야 한다. 따라서, 법원이 시대적 상황에 부합되도록 확대해석할 수도 있을 것이며 또한 의회가 ECPA법을 개정할 수도 있을 것이다. 미국의 프라이버시에 관한 학자인 Daniel J. Solove는 이 법은 기술적인 발전추세에 따라가지 못하고 있으며 따라서 현행 규정을 보다 치밀하고 세부적인 것이 되도록 개정할 필요가 있다는 점을 지적한 바 있다.

나. ADA법에 의거한 청구

그 동안의 집단소송사건에서 승객들은 항공사에 대하여 불공정무역관행법 위반, 재산 및 권리침해(trespass), 프라이버시 침해 또는 부당이득(unjust enrichment) 등을 포함하는 다양한 주법상 및 컴먼로상의

청구를 제기하였다. 그러나, ECPA법을 원용한 사건과 마찬가지로 그 동안의 집단소송에서 주법상의 또는 컴먼로상의 어떠한 청구도 기각되었다. 그러한 청구를 법령에서 명문화하고 있지 아니하였기 때문이다. 그러나, 많은 청구들이 인용되지 못하였던 이유는 바로 연방법의 우선적 효력에 관한 ADA법의 명시적인 규정 때문이었다. 연방최고법원은 그 동안 헌법규정 또는 관련 연방법과 충돌하는 주법 또는 컴먼로는 전자에 비하여 하위의 효력을 가짐을 판시하였다. 특히 연방법에서 명시적으로 연방법의 주법에 대한 우선적 효력을 규정한 경우에는 그러한 점이 더욱 명확해진다.

1978년 미국 의회는 항공산업에서의 시장경쟁을 촉진하기 위하여 ADA법을 제정하였다.[65] 각주들이 규제완화과정을 간섭하는 것을 저지하기 위하여 의회는 "항공운수를 제공하는 항공운송인의 가격, 노선 또는 서비스에 관한" 주법에 대한 ADA의 우위성에 관한 명문 조항을 두었다.[66] 항공사들이 자신들이 피소되었을 경우 ADA법의 우위성을 들어 반론을 제기하는 것이 관례였다. 그런데 이 보고서에서 언급된 집단소송의 경우에도 항공사를 상대로 제기된 주법 및 컴먼로상의 청구와 관련하여서도 그러한 ADA의 우위성이 적용되는 것이다.[67] 이러한 집단소송에서 ADA의 주법에 대한 우위성은 개개의 청구에 따라 다를 수 있기는 하지만 그러한 우위성에 대한 해석은 모든 법원이 일치된 의견을 보이고 있다. 사실 우위성에 대한 표현이 다소 추상적이기 때문에 무엇이 요금(rates), 노선 또는 서비스인가와 관련된 의문이 제기되었다.

---

65) Ryan L. Bangert, "Comment, When Airlines Profile Based on Race: Are Claims Brought Against Airlines Under State Anti-Discrimination Laws Preempted by the Airline Deregulation Act?", J. Air L. & Com., Vol.68(2003), pp.791-95.

66) 49 U.S.C. § 41713(b)(1) (2000).

67) Bangert, op.cit., pp.794-95.

미국의 최고법원은 ADA 우위성 조항의 범위에 대하여 두 번 해석을 내린 바 있다. 첫 번째는 1992년 Morales v. Trans World Airlines, Inc사건에서 “관한”(relating to)의 해석에 관한 것이었다.[68] 이 사건에서 문제가 된 것은 몇 개의 주의 항공사 광고에 관한 주법무부장관의 지침이었다. 이들 주법무부장관들은 지침은 항공사의 가격, 노선 또는 서비스와 관련된 것이 아니라는 주장을 하였다. 그러나 Antonin 대법관은 항공사의 광고에 사용될 수 있는 언어를 제한하는 것은 항공사의 소비자에 대한 판로개척능력에 중대하게 영향을 미칠 수 있기 때문에 결과적으로 그러한 지침은 ADA이 연방규칙으로 정하도록 명확히 규정한 영역(territory)을 잠식하였다고 판시하였다.

그러므로 법원은 항공사의 요금, 노선 또는 서비스와 연관된 또는 이를 언급한 주법에 대해서는 ADA가 우위성을 가진다고 판단하였던 것이다. 이 사건판결은 하급심법원이 다른 주법의 규정에 대해서는 ADA의 우위성을 인정하기에는 너무나 사소하고 관련성이 없다고 판결을 내릴 수 있는 여지를 남기고 있으면서도 그 기준을 설정하거나 그 범위를 명확히 설정하지도 않았다. 한편, John Paul Stevens는 반대의견에서 입법역사와 입법의도를 살펴보면 ADA는 “relating to”라는 용어를 사용함으로써 광범위하게 동법의 주법에 대한 우위성을 갖도록 의도되지 아니하였음을 주장하였다. 그는 ADA가 요금, 누선 또는 서비스에 간접적으로 영향을 미치는 모든 주법 또는 컴먼로보다 우위성을 갖는 것에 대하여 우려를 표명하였다.

1995년 연방최고법원은 ADA의 주법에 대한 우위성에 대하여 두 번째로 해석하였는 바, American Airlines v. Wolens 사건판결에서 “요금, 노선 또는 서비스를 규율하는 주의 실체적인 기준은 ADA보다 하위의 효력을 가지지만 항공사가 자신이 행한 약속을 위반한 경우에는 그러

68) Morales v. Trans World Airlines, Inc., 504 U.S. 374, 383 (1992).

하지 아니하다"라고 판시하였다.[69] 원고들은 주의 기망적 거래행위의 규제와 관련된 법령 및 계약위반을 주장하며 常用고객프로그램(frequent-flyer program)의 소급적인 변경을 이유로 American Airlines를 기소하였다. 법원은 Morales의 판지를 적용하여 ADA에 하위적 효력을 갖는다는 이유로 기만적 거래행위 규제 관련 주법에 의한 청구를 기각하였으며 그 대신 계약위반에 근거한 청구를 인용하였다.

Wolens사건 법원은 Morales사건의 일반적인 판지를 받아들인 반면에 계약위반에 대해서는 ADA의 우선적 효력을 인정하지 아니하였다. 동 법원은 계약은 당사자들의 합의에 근거한 것이며 그러한 합의를 집행하도록 하는 것은 항공사의 요금, 노선 또는 서비스와 관련이 없다고 판시하였다. 법원은 원고가 항공사가 스스로 부담한 약속위반을 유일한 이유로 한 손해배상을 얻으려고 하는 때에는 ADA법이 계약상의 청구를 저지할 수 없다는 결론을 내렸다.

Morales 사건에서와 마찬가지로 Stevens 대법관은 불공정거래관행에 대한 청구와 관련하여 반대의견을 제시하였다. ADA법의 우위적 효력조항은 컴먼로상의 민사불법행위청구 및 기타 청구에 완전히 상위적 효력을 갖는다는 것은 아니라는 점을 지적하였다. 이와 반대로 Sandra Day O'Connor 대법관은 일부 반대의견을 제시하였는바, 계약상의 청구에 대해서도 다른 청구와 더불어 ADA법이 상위적 효력을 가진다는 결론을 내렸다.

연방최고법원이 명확한 방향을 설정하지 못하였기 때문에 하급법원들은 사건별로 각기 다른 선례를 적용하였다. 미국 제2항소순회법원도 그러한 사건별(case by case) 접근방법을 채택하였으며 연방최고법원의 판결들을 혼란을 초래하는 기준(illusory test)이라고 부르고 명쾌한 노선을 설정하기 어려울 것이라고 판단하였다.

---

69) American Airlines, Inc. v. Wolens, 513 U.S. 219 (1995).

한편 제7순회법원은 주의 법령이 항공사의 요금, 노선 또는 서비스에 중대한 경제적 영향을 미치지 아니하는 한 ADA법이 그 법령에 근거한 청구에 대하여 상위적 효력을 갖는 것은 아니라고 판시하였다. 뿐만 아니라 제5순회항고법원은 경제적 영향(economic impact)에 초점을 맞추기 보다는 요금, 노선 또는 서비스에 영향을 미치는 근접성(proximity)에 더 초점을 맞추었다. 다시 말해서 소송원인이 된 상황이 요금, 노선 또는 서비스에 영향을 미치는 정도가 어느 정도인지를 중시하였던 것이다. 예컨대, 제5순회법원은 승객이 기계적 결함으로 인하여 신체적인 상해를 입은 경우의 민사불법행위 책임에 대하여는 ADA법의 상위적 효력이 인정되지 아니한다고 판시하였다. 또한 마찬가지로 항공기가 납치된데 대한 항공사의 부주의에 의하여 초래된 정신적 고통(emotional distress)에 대해서도 역시 마찬가지라고 판단하였다.

Morales 및 Wolens사건 법원들은 일반적인 규준을 설정하지 못하였을 뿐만 아니라 그 동안의 집단소송에서 제기되었으나 연방최고법원이 아직 직접적으로 규명하지 아니한 문제인 무엇이 서비스에 해당하는가에 대해서도 규명하지 아니하였다. Wolens사건 법원은 사건의 사실관계와 관련하여 간략히 서비스를 언급하였을 뿐이며 서비스를 비행에 대한 접근(access to flight) 및 서비스등급(class-of-service)의 승급이라고 불렀다. 하급심 법원들도 서비스에 대하여 세 가지 기본적인 범주의 해석을 내놓았다.

첫째, 가장 광범위한 해석은 서비스의 교환을 위하여 협상한(bargained for exchanges) 것들로 정의하고 그동안의 집단소송에서 채택되었다. 제5순회법원은 요금, 노선 또는 서비스를 실제로 다루고 있는 주법외에도 일반적인 주법은 ADA법보다 하위적 효력을 가진다고 판시하였다. 이러한 해석에 따라 ADA법의 상위적 효력은 문제의 집

단소송들에서 국가의 사생활, 권리침해, 부당이득 및 사기적 거래관련법에 대해서도 적용된다고 판단된다.

둘째, “서비스”의 해석은 광범위한 의미로 해석되어야 할 것이지만, 주로 개인에 대한 침해에 대해서는 예외적이니 사유를 인정하여야 한다.

셋째, 현재의 집단소송 법원들은 “서비스”의 구성요소들에 관한 보다 폭넓은 입장을 취하고 있다. 예컨대, Northwest 사건 및 JetBlue 사건 법원들은 일부 주법상의 청구와 컴먼로상의 청구가 ADA 법의 상위적 효력에도 불구하고 인용되었다.

### 3. Secure Flight

TSA는 좌절된 CAPPSⅡ 프로그램에 뒤이어 2004년 8월 “Secure Flight” 프로그램을 추진하였다. Secure Flight는 의회가 TSA로 하여금 국토보안부가 승객 정보를 자동선별된 자(automatic selectee) 및 탑승거부자 명단과 대조하는 업무를 허용한 개선된 승객 사전검색시스템에 대한 시험작동을 시작하도록 요구한 “Intelligence Reform and Terrorism Act of 2004”의 산물이다. Secure Flight는 정부의 “No-Fly” 및 자동선별자 리스트를 개선하기 위하여 안출된 것이며 알려진 또는 혐의가 있는 테러주의자들을 색출할 수 있는 가능성을 제고하면서도 보다 엄격한 검색 대상인 되는 항공기승객의 숫자를 줄이기 위한 의도를 가지고 있다.[70] Secure Flight는 논란거리였던 前身인 CAPPS Ⅱ의 기술적 기반위에 구축되었다. CAPPSⅡ와 Secure Flight의 기술적 유사성은 Secure Flight는 전자의 표현을 완화한 것이며 소비자친화적인 명칭으로 눈가림한 것에 불과하다는 주장의 근거가 되었다.[71]

---

70) Peter M. Shane, “The Bureaucratic Due Process of Government Watch Lists”, Geo. Wash. L. Rev., Vol.75(2007), p.804.

71) Daniel J. Steinbock, “Designating the Dangerous: From Blacklists to Watch Lists”, Seattle U. L. Rev., Vol.30(2006), pp.77-89.

CAPPS Ⅱ와 유사하게 Secure Flight는 9.11테러사건이후 항공보안에 직접 관여하는 연방정부의 행정부처에 의한 노력의 산물이었다. 예컨대, Secure Flight는 승객사전검색 책임을 민간항공사로부터 연방정부로 이전시킨 것이다. 항공사들은 현재 승객이름은 정부가 제공한 테러주의자 감시리스트와 대조하고 있으며, 이러한 리스트는 정보기관과 법집행기관을 포함한 연방기관들의 권고와 그들로부터 얻은 정보에 입각해 있다. 그러나, 어떠한 민감한 정부감시리스트 정보는 항공사들이 이용할 수 없다. 이러한 정보의 갭을 메우기 위해 Secure Flight는 오직 정부만이 테러주의자검색데이터베이스(Terrorist Screening Database: TDSB) 등 정부 자체의 감시리스트와 승객의 신원을 대조하는 작업을 수행하도록 함으로써 그러한 대조과정을 통합하였다.

TSA는 Secure Flight는 CAPPS Ⅱ와는 다른 시스템이며 Secure Flight는 오직여행자의 실제 신원을 확인하고 상업적 항공보안과 관련된 목적만을 위하여 위험도를 측정하기 위하여 상업적 데이터베이스에 접근할 것이라는 입장을 밝혔다. 뿐만 아니라 TSA는 Secure Flight는 과실로 또는 불공평하게 제2차 검색대상으로 선별된 여행객에게 항소절차를 인정함으로써 더욱 보강될 것이라고 설명하였다. 결국, TSA는 승객들이 부당하게 정밀 보안절차대상이 된 경우 그들이 도움을 구할 수 있는 승객 변호인(advocate)을 고용할 것을 제안하였다. 공고를 하고 수백만 달러짜리 계약을 IBM과 체결한 후 TSA는 승객 정보를 수집하고 그 정보를 상업적 데이터와 대조함으로써 Secure Flight를 테스트하기 시작하였다. 이러한 대조작업은 TSDB 기록과 맞지 않는 “false positive”의 내용을 해결하려는 시도였다.

Secure Flight를 테스트하기 위하여 TSA는 70개 이상의 국내항공사들에게 2004년 6월 한 달 동안의 PNRs를 제출하도록 명하였다. TSA가 요청한 데이터는 항공사마다 달랐다. 그 데이터에는 동행자의 이

름, 좋아하는 음식, 예약을 변경하였는지의 여부, 항공권 지불방법 및 어떤 승객이 술에 취했거나 호전적이었는지의 여부와 같은 문제들에 대한 항공사직원들의 다양한 유형의 논평 등을 포함하고 있었다.

CAPPSⅡ는 항공사에게 승객의 이름, 출생일, 집 주소 및 집전화번호만을 전달해주도록 요구하였으나, Secure Flight는 항공사로 하여금 보안기관에 각 여행자별 승객명단 - 승객의 종전에 예약한 좌석기록에서부터 여행 동반자의 신원에 이르는 39개 분야의 정보를 포함하는 문서를 제공하도록 의무화하였다. 바로 이러한 점 때문에 프라이버시 옹호론자들은 Secure Flight가 CAPPSⅡ보다 훨씬 프라이버시 침해적이라는 주장을 하였다.

사실, Secure Flight는 CAPPSⅡ를 좌절시킨 헌법에 근거한 반대론을 불러일으켰다.[72] 시민들은 Secure Flight가 신원정보 절취라는 상황을 회피 또는 구제하게 될 것인가 그렇다면 어떻게 그렇게 할 것인가를 포함하여 Secure Flight에 대한 다양한 견해를 표명하였다. 한편으로 정보자유법(Freedom of Information Act)상의 요청을 통하여 워싱턴 D.C.에 본사를 둔 공익집단인 Electronic Privacy Information Center (EPIC)는 TSA가 FBI가 테러주의자 검색데이터베이스상의 기록을 유지하는 과정에서 여행자의 프라이버시를 보호하려고 했는가, 그리고 어떻게 보호하려고 했는가를 설명하는 문제를 제출하여 주도록 요구하였다. EPIC의 주요 비판은 Secure Flight와 같은 프로파일링시스템은 항공사 승객들에게 법적으로 집행가능한 권리를 부인하게 될 것이라는 것이었다.

그 전신인 CAPPS와 마찬가지로 Secure Flight는 Privacy Act의 핵심적인 규정의 적용을 받지 아니하여왔으며, 이로 인하여 정부가 보관

72) Stephen W. Dummer, “Comment, Secure Flight and Data Veillance, a New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It”, Miss. L.J., Vol.75(2006), pp.583-90.

하고 있는 자신에 관한 신원정보에 대하여 개인이 가지는 권리를 제한하게 될 것이다. 예컨대, Secure Flight는 항공보안과 무관하고 불필요한 개인 정보를 수집하고 이용한다. 더구나 승객은 그 프로그램을 위하여 보관중인 자신에 관한 신원정보에 접근하거나 바로잡을 수 있는 사법적으로 집행가능한 권리를 가지고 있지 않다. 그러나, TSA는 테스트단계가 끝나면 즉시 Secure Flight가 운영되기 전에 Secure Flight 프로그램을 위한 포괄적인 승객구제절차와 개인데이터와 시민권 보호장치를 확립할 것을 공개적으로 보장하였다. 이러한 보호장치에 대한 세부적인 사항 및 Secure Flight를 위하여 수집한 PNR 데이터를 보관하는 기간 등은 이 프로그램을 둘러싼 논쟁을 해소시키는데 다소나마 기여할 것이다.

이러한 비판에도 불구하고 연방정부의 Secure Flight를 개발하려는 노력은 4년 동안 2억 달러의 경비를 사용하면서 진행되었다.

그러나, 2005년 9월 19일 Secure Flight는 Aviation Security Advisory Committee가 9이의 위원으로 구성되는 보안 및 프라이버시 전문가 패널 - Secure Flight Working Group(SFWG)의 다음과 같은 내용의 보고서를 아무런 권고안이 첨부하지 않고 TSA에 제출하였다: SFWG는 TSA가 Secure Flight에 관한 어떤 핵심적인 문제에 대한 답변을 하지 아니하고 있다. 무엇보다도 TSA는 Secure Flight의 목적이 무엇인지를 명확히 하지 않고 있다. 우리는 우리에게 제시된 제한적인 테스트 결과에 입각해서는 승객들이 항공보안에 대하여 가지고 있는 리스크에 대하여 평가를 하는 일반적인 목표가 현실적이거나 실현가능한 것인지 또는 TSA의 어떻게 그러한 목표를 달성하고자 하는지 평가할 수 없다. Secure Flight의 목적과 구성에 관한 이상과 같은 그리고 그 밖의 해소되지 못한 우려는 2006년 그 프로그램의 전망을 어둡게 하고 있다. 그럼에도 불구하고 DHS는 2008년과 2010년 사이의 어느 때쯤에는 개선된 형태의 Secure Flight를 공표하기 위하여 그 프로그램이

과실을 줄이고 프라이버시의 권리를 보호하고 신뢰를 얻을 수 있도록 운영될 것이라고 주장하고 있다.

## 4. 생체(Biometrics) 및 등록여행자 프로그램 (Registered Traveler Program)

CAPPS, CAPPS Ⅱ 및 Secure Flight와 같은 보안프로그램을 둘러싼 논쟁은 부분적으로 (그 정보와 관련된 당사자의 동의가 없다는) 비자발적 성격에 초점이 맞추어져있다. 그러나 항공보안에 대한 선진생체기술 적용시스템을 개발하기 위한 미국 의회의 지침에 뒤이어 자발성에 기초하여 운영되는 프로파일링 시스템을 개발하려는 노력도 진행되고 있다. 이러한 노력의 산물이 Registered Traveler Problem이다.

Registered Traveler Problem은 승객으로 하여금 본질적으로 낮은 수준의 연방 신원증명(security clearance)을 위한 자신들의 전력 및 생체데이터를 자발적으로 제공함으로써 프로파일링에 동의하도록 유도하는 연방의 방안이다. 이 프로그램은 최초에는 5개의 공항에서 시험운영되었으며 Registered Traveler Program은 항공기 승객가 그의 전력에 관한 정보, 지문, 홍체사진(iris image) 및 가입비에 관한 생체암호 통과카드 또는 스마트 카드의 교환을 제안하고 있다.[73] 등록 여행자는 보안위협평가를 받은 후 스마트카드로 특별보안검색줄에 서서 표준적인 공항검색절차를 통과함으로써 대기시작을 줄일 수 있다.

Registered Traveler Program은 주로 민간사업이며 TSA는 제한적이고 또한 본질적으로 정부 기능에 속하고 절차간소화적 성격을 가지는 역할 예컨대, 보안위협에 대한 평가 및 프로그램 감독 그리고 TSA 검색장에서의 물리적 검색의 실시 등의 업무를 수행한다. 후원공항에서

73) Eric P. Haas, “Comment, Back to the Future? The Use of Biometrics, Its Impact on Airport Security, and How This Technology Should Be Governed”, J. Air L. & Com., Vol.69(2004), p.478.

민간서비스제공업자들은 등록여행자들을 관리한다. 그러한 서비스제공업자 4개중의 하나인 Verified Identity Pass는 “Clear”이라는 프로그램을 운영하고 있다. 선별된 공항에서 간이 칸막이 공간에서 인터넷을 통하여 또는 여객이 직접 이용가능한 “Clear”는 승객이 신청서를 작성하고 가입비(그중 일부는 TSA 등록비)를 지불하고 예컨대 운전면허증 번호, 이전이 집주소 및 사회보장 번호(social security number) 등의 신상 정보를 제공함으로써 clear card를 얻을 수 있다.

한편, 이 프로그램은 CAPPS, CAPPSⅡ 및 Secure Flight에 비교해볼 때, 이 프로그램이 親고객적이고 비교적 투명하기는 하지만, 부당한 프라이버시 침해를 하는 것이라는 비난을 받고 있다. 특히 ACLU는 이 프로그램이 상정한 장점이 항공기 승객이 단순히 “신뢰받는 여행자”(Trusted Traveler)의 지위를 얻기 위하여 중요한 프라이버시의 권리를 포기하는 것을 정당화하지 못한다고 주장하고 있다. 또한 이 프로그램 비판자들은 이 프로그램이 항공기 승객들을 신뢰받는 여행자와 그렇지 못한 자로 이원화시키고 있음을 주목하고 그 시스템에 비용을 지불할 능력이 있는 자에게 특별한 대우를 부여하는 것이며 보안과는 무관하다고 지적하였다. 또한 ACLU는 이 프로그램이 테러주의 지도자들이 그들의 행동대원들이 테러 요주의인물 명단(Terrorist watch list)에 올라 있는지를 확인할 수 있도록 함으로써 기존의 테러방지 프로그램을 무력화시킬 수 있다는 이의를 제기하였다. 암약하는 세포조직 구성원들이 가짜 신분증(false identification)을 얻어 등록여행자가 됨으로써 발각을 회피하여 테러행위를 저지르기 위하여 완화된 보안검색을 이용할 수 있다고 주장하는 비판론도 제기되었다.

이 프로그램은 운영상의 우려사항 외에도 매력적인 사업항목이 있는 바, 상용여행객이 보다 편안하게 항공기 여행을 하기 위하여 이 프로그램을 이용할 수 있기 때문이다. Verified Identity Pass와 같은 민간업체들은 Trusted Travelers로부터 징수하는 연회비의 일부를 받기

위하여 공항과 제휴함으로써 사업적 이득을 얻고 있다. 보스톤 Logan 국제공항의 공항당국은 “Trusted Travelers”에게 공항주차 및 음식 가격을 할인해줌으로써 이 프로그램에 대한 관심을 자극하고 있다. 바로 이러한 이유 때문에 이 프로그램이 테러방지 역할보다는 수입증대제도가 아닌가라는 의문을 갖게 해준다.

2007년 8월 Mel Martinz 상원의원은 DHS가 국제적 Registered Traveler Program을 창설함으로써, 캐나다, 이스라엘, 일본, 네덜란드 및 영국을 이끌어 갈수 있도록 권한을 부여하자는 제안을 하였다. 그러나 동시에 TSA 국장은 이 프로그램이 보안 프로그램이 아니며 리스크에 대비한 보안 제도를 민영화한 후, TSA는 납부자의 재원이 보다 긴급한 필요성이 있는 분야에 가장 효과적으로 사용될 수 있다는 결론을 내렸다고 주장한 바 있다. 2006년 9.11테러 5주년이 다가오자 미국은 상업항공기의 보안이 2001년 이후 개선되었는지의 여부를 검토하였다. 2006년 8월 10일의 미국발 국제항공기에 액체폭발물로 폭파하려는 기도가 실패로 돌아갔지만 이 사건은 보안 문제에 대하여 다시 한번 각성을 촉구하였다. 이 사건이 발생한 후 2주 동안 약 25차례의 보안사건이 공항에서 발생하였으며 9대의 상업항공기가 그 목적지에서 이탈한 바 있다. 2006년 8월 25일 하루만 하더라도 7대의 상업항공기편이 운항중지되었다.

# 제 3 장 프로파일링을 위한 정보제공을 둘러싼 미국과 EU의 갈등

## 제 1 절 미국의 항공교통보안법 및 EU Directive 와의 충돌

### 1. 보안과 시민적 권리에 대한 미국과 EU의 시각차이

미국과 EU가 항공보안을 최대한으로 확보하여야 한다는 점에서도 공통의 이익을 가지고 있지만 보안과 시민의 자유사이의 균형을 유지하는데 대해서는 다소간의 입장 차이를 보여왔다.[74] 미국인들은 프라이버시를 “자유”라는 자신들의 이익의 보호막이라는 차원에서 접근하지만 유럽인들은 프라이버시를 개인의 존엄을 보장하는 기본적 인권으로 관념화하고 있다.[75] 유럽인들은 프라이버시를 개인의 존엄성 및 자신의 공적인 이미지(public image)를 지배할 수 있는 권리로 보며 대중매체, 인터넷 및 상업적 데이터창고에 이하여 제1차적으로 위협을 받는다고 판단하고 있다. 이와 대조적으로 미국인들의 프라이버시에 대한 관념은 개인의 자유 및 국가의 감시로부터 자유로운 권리에 중점이 부여되어 있다. 이러한 권리는 제1차적으로 정부가 가정으로까지 침투함으로써 위협은 받는다고 판단한다.[76]

---

74) Francesca Bignami, “European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining”, B.C. L. Rev., Vol.48(2007), p.609; Edward C. Harris, “Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers”, Am. U. Int'l L. Rev., Vol.22(2007), p.745.

75) Ruwantissa Abeyratne, “Attacks on America - Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada”, J. Air L. & Com., Vol.67 (2002), pp.98-99.

76) James Q. Whitman, “The Two Western Cultures of Privacy: Dignity Versus Liberty”,

유럽인들은 훨씬 더 정부를 신뢰하여 정부가 미국인들이라면 수락하지 아니하였을 방식으로 개인의 선택을 규제하는 것을 기꺼이 허용한다. 바로 이러한 이유 때문에 유럽에서의 항공사 승객프로파일링시스템은 CAPPSⅡ와 Secure Flight 시스템이 고려하지 아니하는 데이터에 대해서도 관심을 기울여왔다. 9.11테러전의 유럽의 항공사 승객프로파일링 시스템은 법집행기관의 데이터들을 이용하였으며 더 나아가 해외프로파일링시스템은 여행자가 어떤 의심스러운 자선단체에게 기여하고 있는지의 여부와 같은 정보까지도 상세히 다루어왔다. 2001년 이후에는 암스테르담 스키폴공항은 Privium이라는 시스템을 운영하고 있다. 이 시스템은 2007년 미국내에서 운영되고 있는 미국의 Registered Traveler 프로그램과 마찬가지로 수수료를 받고 일정한 개인의 신상정보와 생체인식정보(지문 또는 홍체사진 등)의 제공 대가로 보안검색대를 통하여 승객들에게 신속한 검색을 제공하고 있다.[77] 사실, 9.11테러이후 유럽에서의 국가의 감시권한의 확대 현상은 미국보다 훨씬 현저하다.

유럽인들이 미국인보다 훨씬 더 정부당국을 존중하고 있기 때문에 독일, 프랑스 등의 국가들이 미국의 Patriot Act보다 어떤 의미에서 더욱 강력한 감시조치를 9.11 테러사건이후 채택할 수 있었다. 예컨대, 독일에서는 보안기관이 권한을 확대하는 포괄적인 법령을 채택하였다. 이로써 정부는 지문과 종교적 배경을 포함하는 외국인에 관한 개인정보를 가진 중앙데이터베이스를 구축하였다. 이 법은 또한 독일 국민신분증에 지문과 같은 생체인식 데이터를 포함시킬 수 있는 권한을 부여하였다. 또한 데이터마이닝을 명시적으로 인정하고 있으며 정

Yale L.J., Vol.113(2004), pp.1151-60; Ruwantissa Abeyratne, “Attacks on America - Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada” op.cit., pp.98-99);

77) Jennifer McClennan & Vadim Schick, ““O, Privacy” Canada's Importance in the Development of the International Data Privacy Regime”, Geo. J. Int'l L., Vol.38(2007), p.669.

부기관으로 하여금 개인 정보를 연방경찰에 전송해주도록 요구하고 있다.

EU가 채택하고 있는 현행 항공테러방지 보안방안은 미국에서 개발중인 프로파일링 시스템과 병존하고 있으며 항공기승객 검색은 국제협약의 대상이 되어야 함을 보여주고 있다. 현재 정보 공유의 확대가 테러 방지의 최선의 방법이지만 공적 부문과 사적 부문간의 정보 공유는 미국인들이 국가 감시시스템의 위험성을 중시하고 있고 EU 등 다른 국가의 국민들이 개인의 존엄성 보호에 관심을 가지고 있고 있기 때문에 그 실현에는 큰 장애가 가로 막고 있다. 사실, 미국과 EU의 항공보안 정책은 프라이버시와 안보라는 두 가지 쟁점에 의하여 장벽에 부딪치고 있다.

## 2. EU와 미국간의 데이터 보호관련 충돌과 해결

### (1) EU와 미국의 데이터보호법: EU의 포괄적(blanket) 보호 v. 미국의 완화된 보호

#### 1) 의 의

EU와 미국은 데이터 프라이버시를 입법화하는데 각기 별도의 아마도 양립될 수 없는 방식을 취하고 있다. EU는 수집되는 데이터의 양을 제한하고 데이터가 그 수집목적이외의 목적으로 사용되는 것을 방지하는 것을 목표로 하고 있다. 미국은 반면에 보다 광범위한 데이터수집 및 저장을 허용하고 있다. 더구나 EU가 당사자의 확인이 가능한 정보의 이용이 가능한 모든 범위를 다루는 포괄적인 데이터보호정책을 엄격하게 수립하고 있는 반면에 미국은 그 보호에 있어 대단히 느슨하여 구체적인 개인의 문제가 발생하는 때에만 제한하는 입법을 채택하고 있다. 이러한 양측의 데이터보호 정책의 근본적인 차이는 PNR 데이터 전송과 TFTP 분쟁에 내재된 가장 근원적인 문제라고 할 수 있다.

2) EU와 데이터보호 지침(directive)

1995년 유럽의회와 유럽이사회는 개인 데이터의 처리(processing)와 관련된 개인의 보호와 그러한 데이터의 자유이동에 관한 Directive 95/46/EC를 의결하였다(Data Protection Directive). Data Protection Directive는 일반적인 틀을 정하는 입법규정이며 여기에서는 그 주된 목적을 첫째, 개인데이터의 처리과 관련하여 개인의 프라이버시의 보호 둘째, 회원국들의 데이터보호의 조화라고 규정하고 있다.

Data Protection Directive의 또 다른 중요한 원칙은 개인 데이터는 "충분한 보호수준"(adequate level of protection)을 보장하는 EU역외 국가들에게만 전송 할 수 있다는 것이다. 그러므로 Data Protection Directive는 EU내의 공적·사적 부문 모두에게 데이터에 대한 불충분한 보호를 부여하는 역외국가로의 전송을 금지하고 있다는 점에서 영토외적 효과를 가지고 있다. 어떠한 역외국가가 충분한 수준의 보호를 부여하는지의 여부를 결정함에 있어서 EU 위원회는 다음을 종합적으로 평가한다. 즉, 데이터의 성격, 처리공정(processing operations)의 목적, 정보제공국과 정보최종목적지국, 법의 지배(rules of law), 당해 국가에서의 편집(compile)과 관련된 전문적인 규칙 및 보안 조치 등을 특별히 고려하여 데이터 전송 운영을 둘러싼 상황을 평가하게 된다. 유럽위원회가 어떠한 외국이 충분한 보호수준을 유지하고 있지 않다고 판단하는 경우, 회원국들은 그 외국에 어떠한 데이터를 전송할 수 없으며 위원회는 그 문제를 시정하기 위하여 당해 국가와 교섭을 하여야 한다.

Data Protection Directive의 마지막 주요 원칙은 동 Directive가 감시에 초점에 맞추고 있다는 것이다. Directive 제28조는 각 회원국들에게 독립된 집행기구를 설치하도록 요구하고 있다. 각회원국 정부는 개인데이터의 프로세싱에 관한 법안을 기초하는 때에는 그 독립적인

당국과 협의하여야 한다. 이러한 독립적인 당국은 조사를 수행하고 법적 소송을 제기하고 데이터보호 위반에 관한 청구를 심리하는 권한을 가지고 있다. 또한 제29조는 위원회에 데이터보호와 프라이버시 문제에 관하여 조언을 하는, 각 회원국의 대표들, 1인의 Community 대표 및 1인의 위원회 대표로 구성되는 실무단(Working Party)을 설치하고 있다.

3) 미국의 데이터보호에 관한 부문별・자율규제적 접근방법

EU가 Data Protection Directive에서 데이터 보호에 특별히 초점을 맞추고 있는 반면에 미국의 프라이버시법은 보다 일반적인 프라이버시권을 언급하고 있다. 이것은 미국의 프라이버시권이 컴몬로로 진화하였기 때문이다. 그와 같이 컴몬로에 의하여 진화한 원인은 바로 미국이 권리장전(Bill of Rights)가 특별히 프라이버시 기본권을 규정하고 있지 않았기 때문이다. 프라이버시라는 용어는 미국법에서 여성의 낙태의 권리에서부터 텔레마케팅 명부에서 자신의 이름을 유지할 것인지 삭제할 것인지의 선택에 이를 정도로 다양한 의미를 가질 수 있기 때문에 각각의 개인은 자신이 데이터의 어떤 부분이 미국내에서 어떻게 보호받는지를 판단하기 위해서는 여러 기관들을 살펴보아야 한다. 이러한 부문별 접근방법은 때로는 많은 사람들이 자신의 데이터에 대한 사적인 침해로부터 보호받지 못하는 현상을 초래하게 되고 특히 기술발전으로 인하여 일부 관련 법이 그 기능을 발휘하지 못할 때 문제가 된다.

미국의 의회는 공적 부분과 사적 부문간에 공평하게 보호를 적용하여왔다. 정보자유법(Freedom of Information Act(FOIA)와 1974년 Privacy Act가 보여주는 바와 같이, 미국 의회는 공적 부분에서 데이터의 이용을 규제하려는 경향을 보여왔다. FOIA를 개정한 1974년 Privacy Act는 개인 기록이 정부기관의 누설로부터 보호하고 있으며 연방기관들로

하여금 기록의 보안과 비밀성을 보장하고 그러한 보안 또는 무결성에 대한 예상되는 위협이나 위험으로부터 보호하기 위한 적절한 행정적, 기술적 및 물리적 보호장치를 마련하도록 요구하고 있다. 또한 Privacy Act에 의하여 연방기관들은 어떠한 기록시스템의 설계, 개발, 운영 또는 유지에 관련된 자들을 위항 행동규칙을 설정하여야 한다. 그러나 의회가 의도적으로 1974년 Privacy Act를 사적 부문까지 확대적용하지 않는 입장을 취하였다는 사실은 미국 정부가 개인과 기업의 문제에의 개입을 자제하려는 정부의 태도를 보여주는 것이다.

이러한 데이터 프라이버시 입법의 조각작업 누빔(patchwork quilt) 방식외에도 미국은 다양한 형태의 자율규제에 의존하고 있다. 그러한 자율규제속에서 회사와 상업단체들은 종합적인 프라이버시 보호장치를 가지고 있지 않았다. 미국과 EU간의 지속적인 자유로운 상업적 흐름을 가능하게 하기 위하여 양측은 2000년 11월 21일 발효한 Safe Harbor Principles를 승인하였다. EU 위원회는 2000/520/EC의 결정에서 Safe Harbor Principles는 EU로부터 미국으로의 데이터 전송에 대하여 충분한 보호수준을 부여하고 있다고 선언하였다. Safe Harbor Principles가 EU와 미국간의 자유로운 정보 흐름을 가능하게 하는 반면에 이 원칙은 정부기관으로의 정보의 전송에 대해서는 적용되지 아니한다.

(2) 미국의 2001년 항공교통보안법

9.11테러 발생후 불과 2개월이 경과한 2001년 11월 19일 미국은 Aviation and Transportation Security Act of 2001(ATSA)을 제정하였다. 이 법은 미국을 왕래하는 항공기들에게 연방당국에 PNRs 정보에 대한 전자적 접근을 제공하도록 요구하고 있다. 즉, ATSA는 미국과 EU간의 모든 항공기운송인에 대하여 미국의 세관 및 국경보호국(U.S. Customs and Border Protection Bureau 이하 “미국 세관”이라 한다)에

항공기의 예약 및 출발통제시스템에 포함된 PNR 데이터에 대한 전자적 접근을 제공하도록 요구하고 있다. ATSA는 또한 미국 세관에 전송된 정보는 국가안보를 보호하기 위한 목적으로 다른 연방기관들과 공유될 수 있다고 규정하고 있다. 사전승객정보시스템(Advance Passenger Information System)에 포함된 비행전 정보를 제공하도록 요구하고 있다. 그러나 미국의 항공사 승객프로파일링에 포함된 정보 39개 부분 중 20개는 EU 프라이버시 법에 의하여 공개될 수 없다. 결과적으로 미국의 국제비행을 위한 PNRs에 관한 미국의 제출 요구는 그 보호를 보장하지 아니하는 수령인에게 개인데이터를 전송하는 것을 금지한 EU 데이터보호법과는 직접적으로 저촉된다. 특히 미국행 항공편을 가진 EU 항공사들은 불가능한 상황에 처해있다. 그들은 보호되는 승객정보를 EU 법을 위반하여 공개하거나 아니면 그러한 정보를 공개하지 아니함으로써 미국에서의 착륙권을 거부당하거나 하는 양자택일을 하여야 했다.[78]

(3) 미국과 EU의 공동선언과 협정체결

ATSA는 유럽 상업항공기들에게 Data Protection Directive를 위반하거나 그렇지 않다면 ATSA의 위반으로 상당한 벌금을 지불하여야 하기 때문에 데이터 프라이버시에 관한 최초의 미국・EU간 분규를 야기하였다. Data Protection Directive가 공공안전, 방어 및 회원국 안보에 관련하여 운영중인 개인 데이터의 프로세싱에는 적용되지 아니하지만, PNRs은 상업적 목적(해외 비행)을 위하여 사용되고 국가안보 정보를 위해서만 그 후 이용될 수 있다. 도한 가설적으로 만약 데이터가 보안 목적만을 위하여 수집된 것이라면 프라이버시관련 국내법이 안보 및 정책적 문제에 대해서 설정한 예외조치를 적용받을 수 있다.

78) Gehan Gunasekara, “The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows”, Int'l J.L. & Info. Tech., Vol.15(2007), pp.362-64.

EU위원회와 미국간의 최초의 회담이 개최되지 1년여가 지나고 ATSA의 발효가 연기된 후 EU 위원회와 미국 세관의 고급관리들이 2003년 그러한 충돌의 해결을 위한 협상을 위하여 브라셀에서 회동을 하였다. 쌍방은 ATSA와 Data Protection Directive와의 조화점에 대하여 합의에 도달하지는 못하였지만, 공동선언을 발표하게 된다. 그 공동선언은 미국세관이 동의한 최초의 데이터보호 약속을 상세하게 정하고 있으며 쌍방이 EU 위원회가 “충분성”(adequacy)여부에 대한 확인을 하여 미국의 데이터 보호장치가 Data Protection Directive 제25조 제6항에 의거해볼 때 충분한 것이라고 선언할 수 있도록 하기 위한 목적으로 협상을 지속할 것이라는 쌍방의 의사를 확인하였다.

10개월 후인 2003년 12월 16일, 유럽이사회에 의회에 보내 통신문(Communication)에서 위원회는 PNRs 데이터의 미국으로의 전송에 관한 자신의 접근방법을 표명하였다. 그러한 전송을 위한 법적 기틀을 마련하기 위해서는 미국과 EU간의 “가벼운”(light) 쌍무적 협정과 EU 위원회에 의한 충분한 확인이 필요하였다. 그 통신문은 미국과의 일련의 약속을 개략적으로 설명하고 있는 바, 이에 따르면 미국은 다음에 대하여 합의하였다. 첫째, 미국의 PNRs 요청을 일정한 34개 항목으로 제한한다. 둘째, 모든 민감한 데이터의 부류는 삭제한다. 셋째, 테러 및 그와 관련된 범죄를 방지하고 대처하기 위해서만 데이터를 이용한다. 넷째, PNRs 데이터를 3년 6개월 이상 보유하지 아니한다. 다섯째, 국토안보부(Department of Homeland Security)에 커다란 불만을 가진 EU시민을 대신하여 EU 데이터 보호당국으로부터 진정을 접수하여 처리한다. 여섯째, EU 위원회가 이끄는 EU팀과 함께 연차공동검토(annual joint review)에 참여한다.

상기의 통신문은 데이터 전송의 push 시스템의 성격을 상세히 설명하였는 바, 이 시스템은 항공사가 데이터를 미국 당국에 전송하게 된다는 것을 의미한다. 이는 미국정부가 항공사예약시스템에 접근하는

것을 허용하는 당시의 “pull” 시스템과는 상반되는 것이다. 통신문은 2004년 중반에는 필터(filter)를 가진 push 시스템으로 전환하는 것을 상정하였으며 PNRs 데이터 전송에 대한 다자간 접근방법이 개발되어야 한다는 입장을 옹호하였으며 국제민간항공기구(International Civil Aviation Organization: ICAO)가 다자간 제도를 발의하는데 가장 적당한 기구라는 점을 지적하였다.

2004년 5월 14일 EU 위원회는 Data Protection Directive 제25조 제2항에 따라 또한 미국과의 공동선언 및 통신문에 따라 미국 세관이 EU로부터 전송되는 PNRs 데이터에 대하여 충분한 수준의 보호를 보장하고 있다는 판단을 하였다. 그 후 2004년 5월 17일 EU 이사회는 PNRs 데이터 프로세싱 및 전송 협정의 체결을 승인하였으며 5월 28일 양측은 협정에 체결하였다(원 협정). 원 협정은 ICAO에 의한 다자간 접근방식이나 협정의 유효기간에 대한 언급이 없었지만 통신문에서 규정된 내용들을 포함하고 있었다.

## 3. 유럽사법재판소의 PNRs 협정 무효 판결

2006년 중반기에 프라이버시 그리고 특히 데이터보호와 관련된 두 가지 중대한 쟁점이 미국의 테러와의 전쟁(War on Terror)을 위한 조치들의 전면에 등장하였다. 먼저, 2006월 5월, European Court of Justice (ECJ)가 항공기승객정보 또는 승객이름기록(passenger name records: PNRs)을 EU로부터 미국으로의 전송에 관한 미국과 EU간의 협정을 무효라고 판결하였다.[79] ECJ에 의한 PNR 데이터전송(data transfer) 협정의 무효화는 그러한 전송이 EU의 데이터보호법을 위한 한 것인지의 여부에 관한 논쟁을 재점화하였다. 한편 2006년 6월 24일 뉴욕타임즈가 테러리스트자금조달 추적프로그램(Terrorist Finance Tracking

79) Allen Shoenberger, “Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead”, Ind. Int'l & Comp. L. Rev.,Vol.17(2007) p.355.

Program: 이하 “TFTP”라 한다)라고 부르는 미국정부의 재정기록감시(financial record surveillance) 비밀프로그램을 폭로하면서 다시 데이터 보호의 문제가 세간의 주목을 끌게 되었다. 어떤 사람들은 ECJ의 항공기승객협정 무효 결정은 승객정보를 보호하고 9.11테러 사건이후의 국가안보라는 명분하의 미국의 자국 관할권 확장 노력을 퇴패시키기 위한 EU 프라이버시법의 승리라고 환영하였다. 그러나 또 다른 사람들은 ECJ의 결정을 technicality에 근거하여 사건을 판결한 것으로서 EU 위원회와 미국이 동 협정을 대단히 경미하게 조정하기 위한 - 또는 EU위원회가 단순히 협정 체결의 법적 근거를 변경하기 위한 - 또한 데이터 전송이 계획대로 지속될 수 있도록 하기 위한 기초작업을 한 것이라고 판단하였다.

테러리스트들은 해외여행을 하는 때 또는 해외에서 거래하는 때에만 국제사회에 자신들을 노출시키기 때문에, PNRs 전송과 TFTP는 미국의 주목할 만한 테러방지노력의 일환이라 할 수 있다. 그러나 PNRs 데이터전송협정의 무효판결 및 TFTP의 국제사회에의 노출은 EU와 미국간의 관계를 긴장시켰다. EU와 미국은 그들의 데이터보호정책이 위에 언급한 두 가지의 구분되는 문제에 미치는 영향에 관한 공통 기반을 발견할 수 없다면 양측의 관계를 개선하는데 상당한 어려움을 겪게 될 것이다. 이러한 상황에서 미국이 취할 수 있는 조치는 TFTP의 종료시키고 테러의 자금조달을 차단하기 위하여여 필요로 하는 정보를 얻기 위한 재정정보교환에 관한 기존 시스템을 개선시키는 방법이 될 수 있을 것이다. 또한 미국은 재정정보교환에 관한 현재의 시스템을 PNRs 데이터 전송 과정에 적용할 수도 있을 것이다. 아래에서는 유럽의회의 PNRs 협정에 대한 반대 동향에 대해 소개한다.

2004년 7월 27일 유럽의회는 충분성에 대한 결정은 월권이며 EU설립조약(Treaty Establishing the European Union) 제95조는 동 협정의 체결을 승인하는 결정의 적절한 법적 근거가 되지 아니하며 이로 인하

여 기본권이 침해되었다고 주장하며 ECJ에 2004년 5월 17일의 이사회의 결정 및 미국 데이터보호의 충분성에 관한 위원회의 결정 무효를 신청하였다. 2006년 5월 30일 ECJ는 이사회를 상대한 한 소송(C-317/04)과 위원회를 상대로 한 소송(C-318/04)를 병합하여 월권 주장이나 기본권침해 주장을 다루지 않고 이사회와 위원회의 결정을 무효라고 판결하고 2006년 9월 30일까지 새로운 협정에 대하여 타협하도록 하였다. 위원회를 상대로 한 소송에서 ECJ는 PNRs 데이터가 처음에는 항공사에 의하여 상업적 목적(서비스 제공을 위한 항공권발매)으로 수집될 것으로 보이지만, 위원회의 충분성에 관한 결정은 공공보안(public security)을 보호하기 위하여 또한 법집행목적을 위하여 필요하다고 판단되는 데이터프로세싱과 관련되어 있다고 판단하였다. DATA Protection Directive 제3조 제2항은 공공보안, 방어 및 회원국 안보에 관련된 운영을 위한 데이터 프로세싱을 동 지침의 적용범위에서 제외하고 있기 때문에 ECJ는 위원회의 충분성에 대한 결정은 동 지침의 적용범위내에 있지 아니하며 따라서 무효라고 판시하였다.

한편, ECJ는 이사회를 상대로 한 소송에서는 Data Protection Directive 제25조는 제3국이 충분한 수준의 보호를 부장하는 경우에는 그 국가에 개인데이터를 전송 하는 것을 허용하고 있기는 하지만, EU 설립조약 제95조를 동 지침 제25조와 결부시켜 해석한다 할지라도 동 제95조는 미국으로의 PNR 데이터 전송은 동 지침의 적용범위 밖에 있기 때문에 EU가 동 협정을 체결할 수 있는 권한을 정당화하는 것은 아니라고 판시하였다. 따라서 EU 이사회는 그러한 결정을 내릴 수 있는 적절한 근거를 가지고 있지 아니하였다고 보았던 것이다.

## 4. PNRs 전송에 관한 중간협정 및 개정협정

2006년 10월 16일 EU와 미국은 잠정 합의에 도달하였으며(Interim Agreement: 중간협정) 2007년 7월 31일 종료되었다, 양측은 2007년 7

월 개정 협정에 서명하였는 바, 이 협정에서는 미국의 국토안보부가 제시한 방법에 의한 PNR 보호수준은 충분한 것이라고 판단하고 있으며 당사자들이 이에 대체한다는 합의를 하지 아니하는 한, 그 효력기간은 7년으로 하되, 일방은 언제든지 협정을 종료시킬 수 있다고 규정하고 있다.

한편, 개정협정은 종전의 두개의 협정에서 규정된 많은 안전장치를 약화시키고 있다. 첫째, 데이터 보유기간을 3년 6개월에서 15년 또는 그 이상으로 연장하였으며 둘째 미국 국토보안부가, 데이터의 당사자 또는 다른 자의 생명이 위험에 처하거나 심각하게 손상될 수 있는 예외적인 경우에는, 당사자의 인종 또는 종족, 정치적 의견, 종교적 또는 철학적 신념, 노동조합 가입여부 및 건강 또는 성생활에 관한 데이터를 보여주는 개인 데이터의 민감한 요소들을 이용할 수 있도록 하였다. 개정 협정은 미국 당국에 전송되는 PNRs 구성부분을 34가지에서 19가지로 감소시켰지만, 이러한 변경은 34개중 하나를 제외하고 모든 부분을 19개의 데이터 조합들중의 하나로 그룹핑하였다는 점에서 종전과 크게 달라지지 아니하였다.

또한 개정협정은 종전 협정에서는 요구하지 아니하였던 추가적인 수하물 및 상용승객우대프로그램 가입여부를 포함하여 새로운 PNR 데이터의 전송을 요구하고 있다.

## 제 2 절 테러리스트자금조달 추적프로그램과 EU의 반응

2006년 뉴욕타임즈는 미국 정부의 TFTP를 상세히 폭로하였다. 이 TFTP는 CIA가 운영하고 재무부(Treasury Department)가 감시하는 것이며 전세계의 대규모 재정정보교환네트워크(financial communication network)인 the Society for Worldwide Interbank Financial Telecommunication

(SWIFT)로부터 재정거래에 관한 정보를 얻기 위하여 국제비상사태경제권한법(International Emergency Economic Power Act of 1978)에 의한 행정부의 권한에 의존하고 있다. 미국정부는 9.11사건직후부터 테러리스트들의 자금조달 활동을 추적하기 위한 노력의 일환으로 SWIFT로부터 금융자료(financial data)를 비밀리에 요청하여왔다. 미국 재무부가 SWIFT로부터 정보를 수령하게 되면 그 데이터를 대규모 데이터베시스에서 편집하게 되며 이 데이터베이스는 CIA, FBI 및 기타 정부기관이 검색할 수 있다.

SWIFT는 재정기관들의 컨소시움에 이하여 소유・운영되는 벨기에 회사로서 200개 이상의 국가에서 8,100개 이상의 금융기관에 보안메시지서비스(secure messaging service)를[80] 공급하고 있다. 일반적으로 SWIFT가 전송하는 보안메시지(secure message)는, 수익자(beneficiary)의 이름이나 주문고객의 이름과 참조번호(reference number) 등과 같은 제한된 개인데이터만을 포함하고 있다. SWIFT가 처리하는 모든 메시지는 미국과 벨기에의 두 운영센터(지사)에서 124일 동안 저장된다. 미국 재무부의 외국인자산통제청(Office of Foreign Assets Control:OFAC)은 SWIFT로부터 자신이 원하는 데이터를 얻기 위하여 행정소환장(administrative subpoenas)을 보내게 되면 SWIFT는 그 정보를 제공한다. 이는 SWIFT의 이사회가 1990년대 초 채택한 수락정책(compliance policy)에 의한 것으로 이 정책은 SWIFT가 자신이 제공하는 데이터메시지서비스를 위하여 최고 수준의 무결성(integirty)과 비밀성을 보장하기 위한 모든 조치를 취하되, 당국이 발한 소환장 또는 영장에 응하여야 함을 규정하고 있다.

80) 메시지서비스는 사용자의 중간에 일시 저장장치가 존재하여 이 장치를 경유하여 통신되는 서비스를 말한다. 일시 저장장치의 기능으로는 store-and-forward, mailbox, message handler(예, 정보편집, 처리, 변환 등) 등이 있다(http://enc.daum.net/dic100/contents.do?query1=11XXXX7718).

뉴욕타임즈가 TFTP의 세부적인 내용을 최초로 폭로하자 마다. 외국 특히 EU 의회는 2006년 7월 6일 그 프로그램이 EU의 데이터보호법과 프라이버시법을 침해한 것이라는 우려를 표명하는 결의를 채택하였다. 그 후 데이터보호와 프라이버시에 관한 독립적인 EU 자문기관인 제29조에 따라 설치된 실무단(Working Party)은 2006년 11월 월 22일에 되어서야 SWIFT의 활동이 EU Data Protection Directive를 위반한 것이라는 결론을 내리고 모든 침해행위를 중지하라는 의견(Opinion 10/2006)을 제시하였다. 이에 따르면 SWIFT는 Data Protection Directive 제2조의 데이터 제어자(data controller)에 해당한다고 판단하였다. 반면에 SWIFT는 자신은 데이터 처리자(data processor)일 뿐이라고 반론을 제기하였다. 동 Directive에 따르면 “controller”라 함은 독자적으로 또는 타인과 공동으로 개인데이터의 처리 목적과 수단을 결정하는 자연인이나 법인, 공공기관, 대행기관 또는 기타 기관”이라고 정의하고 있으며, “processor”라 함은 controller를 위하여 개인데이터를 처리하는 자연인이나 법인, 공공기관, 대행기관 또는 기타 단체”라고 정의하고 있다. 동 Directive상 data processor의 직무는 data controller를 위하여 정보를 처리하는 자이기 때문에 이러한 구분은 대단히 중요한 의미가 있다.

그러나 제29조 실무단은 SWIFT가 그 통상적인 보안메시지서비스와 그 제출요구된 데이터의 처리 두 가지 측면에서 모든 controller의 역할을 하고 있으며 따라서 정보가 미국 당국에 전송되기 전이라 할지라도 controller로서 Directive를 준수할 책임이 있다고 판단하고 SWIFT로 하여금 동 Directive의 침해를 중지하고 합법적인 데이터 처리로 즉각 복귀하도록 요구하였다.

이로 인하여 미국은 TFTP 프로그램을 제한적으로 운영할 수 밖에 없었고 2007년 6월 27일 EU위원회에 TFTP에서 데이터 취급, 이용 및 유포에 대한 통제와 보호를 설명한 일방적인 해명서를 송부하였다.

이 해명서는 SWIFT의 Safe Habor에의 참여 가능성에 대비하여 보낸 것이다 앞서 언급한 바와 같이. Safe Habor Principles는 정부당국에의 데이터 전송에 대해서는 적용되지 아니한다. 그러나, EU 항공사에 의한 미국 DHS에의 PNR 전송과는 달리, 유럽의 SWIFT 처리센터는 상업적 목적을 위한 유럽에서 상업적 목적을 위하여 미국의 SWIFT 지사에 데이터를 전송하고 그 후 미국 당국이 미국에서 이에 접근하게 된다. 그럼에도 불구하고 미국 당국이 데이터에 접근하기 때문에 TFTP에 의거한 미국의 노력은 Safe Harbor Principles를 invoke하며 그 해명서는 미국이 SWIFT 데이터를 편집시에 EU의 데이터보호원칙에 따를 것이라는 것을 보장하고 있다.

그에 대한 답변에서 EU 위원회와 이사회의 대표들은 그러한 해명서의 보장을 환영하고 일단, SWIFT가 금융데이트를 Safe Harbor Principles에 따라 상업적 목적을 위하여 미국에 제공하게 되면, SWIFT(와 그 서비스를 이용하는 금융기관들)는 EU의 데이터보호법에 따라 각각 법적 책임을 지게 될 것이라는 점을 선언하였다.

이에 따라 SWIFT 미국지사는 2007년 7월 16일 Safe Harbor에 참여하였고  EU로 받은 개인데이터를 Safe Harbor Principles에 따라 취급한다는데 동의하였다.

# 제 4 장 국내 프로파일링 도입방안

## 제 1 절 의 의

앞서 살펴본 미국을 비롯한 많은 국가들이 9.11테러이후 각국이 항공테러의 방지를 위한 엄격한 보안절차들 외에도 개선된 프로파일링 도입을 위하여 많은 노력을 기울이고 있다. 보안검색 효율성을 높이기 위해서는 무엇보다도 테러의심 승객을 선별·검색하는 방식이 필요하다.

우리나라의 경우 매뉴얼 프로파일링과 시스템 프로파일링의 장점을 취한 혼합식 프로파일링의 도입이 합리적으로 1차적으로 인권침해 논란이 비교적 적은 시스템 프로파일링을 도입한 후 순차적으로 법적 근거 마련 및 전문인력 양성 등의 준비를 거쳐 매뉴얼 프로파일링을 실시하는 것이 바람직한 것으로 본다. 테러취약노선, 위험국가인물 정보와 여권 비자 정보, 항공권 예약정보, 탑승과정에서 나타난 데이터를 시스템으로 연계, 분석을 통하여 항공편, 노선, 승객별 의심승객을 검색하는 방법을 도입하여 보안검색의 정확성을 높이고 비용을 최소화하는 방안을 마련하여야 할 것이다. 또한 이를 구체적으로 시행함에 있어서는 공항당국과 정부기관, 항공사 등의 공동 노력이 필요함을 두말할 여지가 없다. 승객의 예약, 탑승정보 등을 이용한 승객프로파일링 기법도입을 위해서는 항공사로부터 승객정보를 제공받아 분석해야 함에 따라 이러한 승객 정보를 입수, 활용할 수 있어야 하는 바, 이는 법적 뒷받침이 있어야 한다.

## 제 2 절 항공프로파일링에 대한 종합적인 평가

### 1. 혼합적 프로파일링의 필요성

CAPPS가 9.11테러주의자 19명중 10명을 가려내었다는 사실은 프로파일링과 그에 수반되는 약간의 여행과 프라이버시의 권리에 대한 침해를 정당화하고 있다. 테러주의자들의 수하물은 그들이 항공기에 탑승할 때까지도 아무런 저지도 받지 아니하였다. 이러한 현상은 프로파일링 자체의 결함이라기 보다는 그 시행상의 결함을 노출한 것이다. 보안요원들이 사람이 아닌 폭탄에 초점을 맞춤으로써 프로파일링 시스템을 효과적으로 이용하지 못하였던 것이다. 반면에 이스라엘 항공보안요원들은 오랫동안 승객 자체에 초점을 맞추어왔다. 그들은 승객 개개인에 대해서 검색을 하여왔다. 예컨대, 1986년 런던에서 텔 아비브로 가는 항공편에 탑승하려는 임신부를 EL AL이 추가적 검색을 받도록 하였는바, 보안요원들은 임신부가 혼자 여행하는 것을 수상히 여겼던 것이다. 그녀의 요르단 남자 친구가 그녀가 탑승한 항공기상의 375명을 죽일 수 있는 폭탄을 그녀의 휴대용 가방에 장치하였던 것이다. 이스라엘에서는 이러한 보안절차를 통하여 이스라엘 공항에서 한 번도 항공기 납치기도가 성공하지 못하였다. 이러한 시간소모적인 절차는 미국에서는 9.11테러 이전에는 표준절차도 아니었고 환영받지도 못하였다. 9.11테러 사건 발생 후 1주일도 못되어, 미국에서도 승객의 행동(behavior)에 대한 분석을 하는 요원들이 “Screening Passengers by Observation Technique”(SPOT)라는 프로그램에 따라 활동하기 시작하였다.

한편으로 행동 프로파일링(behavioral profiling)도 결함을 가지고 있다. 그러한 미숙한 항공요원을 속일 수도 있는 것이다. 사실 인간이 프로파일링을 담당하는 경우에는 “false positives”의 가능성이 더 커질

수 있다. 물론 컴퓨터가 프로토콜(protocol)밖에 있는 세부적 사항에 대해서는 둔감하기 때문에 false positives를 초래할 수도 있는 경우에는 관찰에 토대를 둔 프로파일링이 자칫하면 엉뚱한 자를 테러리스트로 혼동하는 주관적이고 차별적인 판단을 내리게 된다. 말하자면, 비행과 관련하여 긴장하여 손바닥에 땀이 나고 신경이 날카로운 움직임을 보이는 승객 모두가 테러리스트는 아니다.[81]

## 2. 프로파일링의 과학적 기준의 확립 필요성

프로파일링은 컴퓨터에 의한 것이든 사람에 의한 것이든 간에 테러리스트를 확인하는 이론이 때로는 특정성(specificity)과 이를 뒷받침하는 데이터가 부족하기 때문에 효과가 없을 수도 있다는 점에 주목할 필요가 있다. 심리학적으로 테러리스트는 정신질환을 겪고 있다는 개인병리학적 명제(personal pathology thesis)는 큰 지지를 얻고 있지 못하다. 테러리스트는 신체이형장애(bodydysmorphic disorder)를[82] 가진 식욕부진한 사람과 같이 과대한 어떠한 과대망상적인 가치에 사로잡힌 반사회적이고 정신질환이 있고 광신적인 사람이라는 이론도 지지를 받고 있는 것으로 보이지 아니한다. 테러리스트가 정신질환적 자기도취증(narcissism), 과대망상증(paranoia) 또는 권위주의적 인격을 가

81) Bob Barr, “Post-9/11 Electronic Surveillance Severely Undermining Freedom”, Val. U. L. Rev.,Vol.41(2007), pp.1383-85; Bennie G. Thompson, “The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy”, PGH. J. Tech. L. & Pol'y, Vol.10(2006), p.1.

82) 강박증의 일종. 정상적인 외모를 가진 사람이 상상적인 신체적 결점에 지나치게 집착할 때 발병. 또한 결점이 매우 작은데도 유난히 크게 그것을 부각하고 과장하여 생각할 때는 의심해야 한다. 발병률은 28%로 생각보다 높으며 자존심, 전반적인 자기가치감이 낮고 우울증이나 자살로 이어진다. 모든 사람들이 항상 나를 보며 모른척한다고 생각하며 다른 강박장애와 다른 점은 본인들이 조금 인정한다는 것이다. 사회적 직업적 문제는 물론 결혼생활에도 어려움을 겪는다. 증세가 심하면 머리 자르는데 8시간이 걸리거나 털을 확대경으로 보는 등의 증상이 있다. 성형하는 사람들의 2%정도가 신체이형장애로 고통 받는 것으로 추정되며 신체이형장애 환자중 11%는 사회공포증, 8%는 강박장애, 2%는 공황장애를 앓는다.

진다는 명제도 경험상의 지지를 그다지 받지 못하고 있다. 어린 시절의 데이터가 있는 61인의 테러리스트들중 불과 4명만이 반사회적 인격장애가 있다는 증거가 있을 뿐이다. 이들 중 2명은 기독교로부터 개종하였다. 테러리스트들이 자살을 두려워하지 아니한다는 사실은 정신질환보다는 순교라는 문화적인 맥락에서 설명될 수 있다. 결론적으로 프로파일링은 예컨대, 전세계의 모든 살라피 무자헤딘(Salafi mujahedin)은 공통 프로파일을 갖게 되며 따라서 모든 무자헤딘집단들마다 각기 그에 상응하는 프로파일을 갖게 되기 때문에 실제적용상에는 많은 오류를 초래할 수 있다.

마지막으로 프로파일링 시스템이 과연 법적인 문제로서 과학적으로 신뢰할 만한 것인가에 대한 의문도 제기된다. 프로파일링시스템은 법집행에 대한 거짓말 탐지기의 유용성이 법원에서 빈번히 인정할 수 없는 기술이라는 결론이 내려지고 있다는 점에서 거짓말 탐지기와 마찬가지이다. Dubert v. Merrell Dow Pharmaceuticals, Inc.사건에서는 기술이 과학적인가의 여부는 다음과 같은 몇 가지 고려에 입각하여 판단하여야 한다고 판시한 바 있다. 즉, 기술이 시험가능하고 또한 시험을 거쳤는지의 여부, 알려진 또는 잠재적인 에러율, 기술이 전문가집단의 상호심사(peer review)를 받은 것인지의 여부, 사용된 기술이 일반적으로 인정을 받았는지의 여부 등이다.

앞서 언급한 바와 같이 항공기승객프로파일을 구성하는 기준은 공개적으로 알려진 바가 없으며 따라서 투명하게 테스트할 수 없다. 사실상, 정부의 항공업계와의 협력에 의한 프로파일링 테스트는 소송을 초래하였다. 폐쇄적인 정보(intelligence) 분야가 하나의 기술로서의 프로파일링을 어떠한 집단을 통하여 평가하고 있는지 알 수가 없다. 더구나, 프로파일링은 일반적으로 인정되는 기술도 아니고 에러율이 알려져 있거나 만족스러운 과정도 아니다. 그러므로 프로파일링이 상업적 항공을 보호하기 위하여 필요하다고 추론한다 할지라도 테러리스

트를 확인하기 위한 항공기 승객프로파일을 구성하는 일련의 명확한 특징들은 존재하지 아니한다.

## 3. 프로파일링과 인권의 조화 필요성

9.11테러 발생 수 4개월 동안 시행된 미국 정부의 “Civil Liberties Survey”에서 조사대상이 된 미국 시민들은 시민적 권리를 개인의 안전과 보안의 강화와 교환할 용의가 있다는 응답을 표명한 비율이 상대적으로 높았다. 그렇지만 이러한 교환을 감내한다는 결정은 그 이면을 들여다보면 복합적인 요소들을 많이 내포하고 있다. 개인적인 인종과 종족, 교육, 연령, 교류울타리와 더불어 독단적 태도(즉 폐쇄적인 마음), 사람에 대한 신뢰정도, 국가에 대한 긍지와 애국심 등 자신의 사회적·심리적 상황이 반영된 것이라 할 수 있다. 9.11테러후 미국인들은 실제 상황에서보다는 추상적인 상황에서 안보보다는 시민권을 더 중시여기는 것으로 보였다.

프라이버시와 개인의 권리 보다는 보안을 우선시하는 국민들의 충동적인 감정은 9.11이후 차츰 사라지고 있다. 시민들은 다시 9.11 이전의 일상생활로 돌아갔으며 현재는 점차 미국인들이 정부의 조치의 점진적인 확대에 대한 우려와 기술에 대한 두려움으로 인하여 생활속에 침투하는 정부의 보안조치를 테러방지조치에 대한 반감(anti-anti-terrorism)을 가지고 바라보고 있다.

일부 시민들은 정부 당국의 남용 가능성을 실제 남용과 동일시하고 있으며 그러한 조치의 잠재적인 혜택에도 불구하고 얻게 되는 혜택보다 권한 남용의 가능성 더 크다고 판단하기 때문에 정부의 보안조치 확대에 항의를 하고 있다. 이러한 상황에서 CAPPS, CAPPSⅡ 및 Secure Flight와 같은 프로파일링시스템에 의한 과실을 구제하겠다는 TSA의 약속은 많은 미국들에게 확신을 심어주지 못하고 있다. 또

한 프라이버시 옹호론자들이나 시민권자들은 연방정부 또는 민간업체들이 Registered Traveler와 같은 시스템을 통하여 개인데이터와 생체인식 데이터에 대한 접근권을 가지는 것은 허용할 수 없다고 판단하고 있다.

CAPPSⅡ에 대한 주된 반대 이유는 프라이버시 옹호론자들은 이 시스템이 불법적으로 프라이버시를 침해할 뿐만 아니라 데이터베이스 착오시 무고한 승객에게 누명을 씌울 수 있다는 것이었다. 또한 필요 이상의 많은 개인정보가 필요이상의 기간 동안 보관되는 것은 합리성이 결여되어 있으며, CAPPSⅡ시스템이 정부 건물과 공공장소 및 배, 기차, 버스와 같은 모든 운송수단에의 접근을 통제하기 위하여 배치될 수 있을 것이라고 우려하였던 것이다.[83]

## 제 3 절 관세청 APIS 제도

관세청은 테러, 마약 등 우범여행자의 효과적인 선별을 위하여 우범여행자를 선별하여 정밀검색하는 APIS 제도를 전국 공항에서 실시하고 있다. 2001년 3월 인천공항 개항과 더불어 APIS 제도를 도입하여 2002년 5월 김해, 제주공항, 2003년 김포공항으로 확대하고 2005년 9월부터 전국 공항만에 확대하여 실시하고 있다. 관세청의 APIS 제도라 함은 Advance Passenger Information System으로서 항공기 도착전 항공사로부터 여객명부를 전자적 수단으로 입수, 분석하여 우범성이 높은 소수의 여행자를 선별, 검사하는 제도이다. 1988년 미국이 도입한 이래, 주요 국가들이 이를 시행하고 있다.[84]

관세청은 개항초기 여행자정보 사전 입수율이 11%에 불과한데다 EDI로 여행자 정보를 전송하는 항공사는 대한항공, 아시아나 2개 국

83) 김장환・강자영, “미국의 항공보안정책 적용과 프라이버시 문제점”, 한국항공운항학회지, 제13권 제3호(2005), p.155.
84) 황호원・이규황, op.cit., p.166.

적항공사에 불과하였고 국적 항공사도 성명을 기준으로 한 여행자 정보 전송율은 60% 수준이지만 이름외에 여권번호, 생년월일 등 APIS 선별에 필수적인 여행자 상세정보 제공율은 20%에 수준에 불고하였으며 외국적 항공사의 경우 EDI 전송시스템 자체가 구축되지 아니하여 종전과 같이 인편 또는 FAX로 여객 명단을 제출하는 사례도 초기에는 많았다.[85]

이와 같이 여행자정보 입수율이 저조함에 따라 APIS 운영실적도 저조 2001년 4월-8월 APIS 검사자는 전체 입국여객의 0.1%에 불과하였으며 대부분의 승객은 종전과 같이 X 레이 검색과 인력에 의존하여 검사대상자을 선별하였다. 이는 APIS를 항공사 자율사항으로 함에 따라 입수율 제고에 한계에 다다르자 2002년 APIS 전송을 의무화하도록 한 관세법 제135조 제2항에 '선박 또는 항공기가 소속된 선박회사 또는 항공사(그 업무를 대행하는 자를 포함한다)로 하여금 제1항에 규정된 여객명부, 적하목록 등을 입항하기 전에 제출하도록 할 수 있다고 규정함으로써 항공사가 항공기 도착전 성명, 국적, 생년월일, 여권번호 등 여행자 상제정보를 기재한 EDI 여객명부 전송을 의무화하였으며 이를 위반한 때에는 벌금을 부과하도록 하는 관세법 개정안을 제출하여 2003년 1월부터 시행하고 있다.

한편 제137조의2 (승객예약자료의 요청)은 세관장은 세관업무와 관련하여 선박회사 또는 항공사가 운영하는 예약정보시스템의 승객예약자료를 제출하도록 요구할 수 있으며 열람할 수 있는 자를 관세청장이 지정하는 세관공무원에 한하고(제3항) 직무상 알게 된 승객예약자료를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니하도록 하고 있다(제4항). 그러한 승객예약자료는 1. 국적・성명・생년월일・여권번호 및 예약번호, 2. 주소 및 전화번호, 3. 예약 및 탑승수속 시점, 4. 항공권 또는 승선

85) Ibid., p.167.

표의 번호・발권일・발권도시 및 대금결제방법, 5. 여행경로 및 여행사, 6. 동반탑승자 및 좌석번호 및 7. 수하물자료로 한정하고 있다(제2항). 또한 선박 및 항공기의 PNRs(승객예약자료)의 제공 및 이용에 관한 고시(2006년 4월 26일)를 통하여 승객예약자료를 사전 제출받아 세관감시업무의 효율적 수행과 입출국 여행자의 신속한 통관을 도모하기 위함이었다. 따라서 이러한 규정은 테러의 방지와 직접적인 관련이 되어 있는 것은 아니지만, 항공프로파일링의 구축을 위한 데이터로도 활용될 수 있을 것이다.

## 제 4 절 법무부 사전승객분석시스템(APIS)

법무부는 테러, 국제범죄 등 위해인물의 입국을 차단하기 위한 노력의 일환으로 APIS 제도를 시행하고 있다. 법무부 APIS는 1988년 미국에서 최초로 시행되었으며 처음에는 항공사들의 비협조로 운영이 지지부진하였으나 9.11테러 사건을 계기로 강력한 법개정을 통하여 미국 취항 항공사에 APIS 전송 필수항목 지정 및 처벌강화 후 모든 항공사가 승객정보를 전송하고 있다. 우리나라의 경우는 2005년 5월 1일부터 시험운영을 거쳐 2005년 9월 25일 개정 출입국관리법 시행일에 맞추어 본격적으로 운영하고 있으며 2007년 현재 86개 항공사 승객정보를 전송받아 활용하고 있는데, 미국, 호주, 뉴질랜드, 캐나다, 일본, 싱가폴, 홍콩, 영국, 태국, 필리핀, 말레이시아, 아랍에미레이트 등 13개국이 운영중에 있거나 시험가동중에 있다.[86]

법무무는 항공사들에게 승객정보 전송을 의무화하기 위하여 2005년 3월 24일 출입국 관리법을 개정하였다. 제73조(운수사업자 등의 일반적 의무 등) 신설을 통하여 출입국 관리공무원이 항공사가 운영하는 예약정보시스템의 자료를 받아 열람할 수 있고 항공사로부터 승객의 국적 및 주소, 예약 및 탑승수속 시점, 여행경로 및 여행사, 동반탑승

86) Ibid., p.168.

자  좌석번호, 수하물, 항공권 구입대금 결재방법 등에 관한 자료를 운수업자에게 요청할 수 있도록 하고 제75조(보고의 의무)를 신설하여 승무원 명부 및 승객명부를 출입국사무소에 제출하도록 하였다.[87]

한편, 동법 시행령 제87조는 법 제75조 제1항의 출입항보고서중 운수업자가 제출하여야 하는 승객명부 및 승무원명부에 국적, 여권에 기재된 성명, 생년월일, 성별, 여행문서의 종류 및 번호, 환승객인지의 여부(승객의 경우에 한한다)를 기재하도록 규정하고 있으며 운수업자가 제출하여야 하는 항공기에 관한 정보에는 항공기의 종류, 등록기호 및 명칭, 국적, 출항지 및 출항시간, 경유지 및 경유시간, 입항지 및 입항시간, 승무원·승객·환승객의 수 등을 기재하도록 하고 있다.

또한 표준전자문서로 제출된 출입항보고서에 승객명부 또는 승무원명부중 누락한 자가 있는 등 보완할 사항이 있는 경우에는 지체 없이 보완하여 제출하도록 할 수 있으며, 출입항보고서의 제출시기를 입항의 경우에는 출발국에서 출발한 후 20분이내에 또는 국내 입항 2시간 이전으로 하며, 출항의 경우에는 출항준비가 완료되는 즉시로 하는 등 제출시기도 규정하고 있다(시행령 제87조 제4항 및 제5항).

최초 항공사들의 승객정보 제공이 지지부진하자 APIS 활성화를 위하여 벌칙조항을 신설, 정당한 사유 없이 보고서를 제출하지 아니하거나 허위로 제출한 자에 대해 1천만원 이하의 벌금을 부과할 수 있으며 과실로 보고하지 아니한 경우에도 200만원 이하의 과태료를 부과할 수 있도록 하였다.

---

87) 제73조 제2항: 출입국관리공무원은 다음 각 호의 어느 하나에 해당하는 업무를 수행하기 위하여 필요한 때에는 미리 사무소장 또는 출장소장 승인을 얻어 운수업자가 운영하는 예약정보시스템의 자료를 정보통신망을 통하여 열람하거나 문서로 제출하여 줄 것을 운수업자에게 요청할 수 있다. 이 경우 운수업자는 이에 응하여야 한다.

제73조 제3항: 제2항의 규정에 의하여 열람하거나 문서로 제출받을 수 있는 자료의 범위는 다음 각 호에 한한다. 1. 국적 및 주소, 2. 예약 및 탑승수속 시점 3. 여행경로 및 항공사, 4. 동반 탑승자 및 좌석번호, 5. 수하물 6. 항공권 구입대금 결제방법.

한편 우리나라의 항공사들은 지난 2006년 후반기에 국제선 전 노선에 대해 사전승객정보(APIS) 데이터가 입력되지 않거나 누락된 경우 공항 탑승수속시 아예 탑승권 발급이 불가능하도록 하는 새로운 제한기능을 도입하여 시행하고 있다. 2006년 8월 이후 출국신고서 제출제도 폐지와 함께 법무부가 APIS 제도를 본격화하면서 항공사들은 모든 승객의 성명, 성별, 국적, 여권번호, 생년월일 등 APIS 데이터를 법무부에 전송해야 한다.

## 제 5 절 항공보안프로파일링 법제화

앞서 언급한 관세청 APIS 제도는 그 목적상 항공프로파일링은 아니다. 또한 출입국관리법상의 사전승객정보제도로는 현재의 항공테러에 적극적으로 대처하기 어렵다. 프로파일링은 일부 선별된 승객과 수하물에 대해 보다 정밀한 보안검색을 실시하게 됨에 따라 대상자의 반발이나 불만이 생겨날 수 있으므로 시행의 법적 근거가 필요하다. 그러나, 앞서 언급한 봐와 같이 프라이버시의 보호 및 개인정보의 보호와 같은 민감한 문제와의 조화가 필요하다. 우리나라의 경우에도 미국의 CAPPS Ⅰ 또는 CAPPSⅡ와 같이 이미 폐지된 제도를 도입하기 보다는 미국의 Secure Flight이나 Registered Traveller와 같은 프로그램을 도입하는 것도 고려할 필요가 있을 것이다. 또한 출입국관리법의 사전승객정보제도를 강화하는 방향의 개정이 필요할 것이다. 또한 항공안전 및 보안에 관한 법률에 그러한 제도를 명문화하는 근거를 마련하여야 할 필요가 있다. 한편 화물에 초점을 맞추어온 기존의 프로파일링제도와 더불어 승객 자체에 대한 감시시스템을 구축하기 위하여 미국 등 외국과의 협력 및 국제적인 협력체제의 구축에도 참여할 필요가 있다고 판단된다.

# 제 5 장 결 론

9.11테러 사태이후 미국 정부는 자국 영토를 출입하는 항공기 승객 및 승무원의 개인 정보를 미 행정부에 제출하도록 요구하는 다양한 법령들을 제정하였는 바, 특히 항공사는 미 세관 및 국경보안국(CBP)이 passenger Name Records(PNRs: 항공기 승객기록)에 내장된 탑승객 정보에 접근할 수 있도록 허락하여야 하고 이를 위반할 경우 벌금부과, 착륙금지, 도착지연 등의 불이익을 당할 수 있다고 명시하고 있다.

테러에 맞선 이러한 대응은 민주사회의 필수 불가결한 요소임에는 틀림없지만, 이 과정에서 기본권 및 자유(프라이버시 및 정보보호권리 등)도 존중되어야 한다. 상업적 용도로 수집되어 항공사 데이터베이스 및 관련 예약시스템에 저당된 개인정보를 공공기관이 접근하도록 허락하는 행위는 전세계적으로 전례가 없는 경우일 뿐만 아니라 정보보호 기본원칙에도 어긋난다. 프로파일링은 보안이라는 명분하에 승객의 불편과 공항당국 및 항공사의 부담을 무한정 가중시킬 수도 없는 현실에서 한정된 보안자원을 이용하여 선량한 승객에 대한 검색노력을 줄이고 반면에 보다 위험가능성이 높은 승객과 수하물에 보안역량을 집중시킴으로써 승객이 보안검색을 위해 대기하여야 하는 시간을 단축하고 공항보안을 효율적으로 강화하는데 그 목적이 있다.[88]

우리나라에 대한 직간접적인 테러위협이 증가하고 있는 가운데 인천국제공항 개항이후 지속적인 여행증가에 비례하여 위해물품의 적발 건수가 늘어나고 있어 검색장비의 첨단화, 검색요원의 전문화 및 숙련화에 따른 대책외에도 프로파일링과 같은 새로운 선진보안기법의 개발 및 도입필요성에 대한 공감대가 형성되어 가고 있다. 이미, 테

88) 황호원・이규황, op.cit., p.171.

러, 국제범죄 혐의자 등 국익위해자의 입국을 사전 차단하고 마약밀수 등 우범자들을 선별해냄으로써 다수의 선량한 승객의 신속, 편리한 출입국이 가능하도록 한 법무부와 관세청의 승객사전정보분석시스템(APIS)에서 보듯이 승객의 예약정보를 이용하여 프로파일링한다는 것은 승객의 여행정보를 수집할 수 있는 정당한 권한이 있어야 하며 법적인 근거가 있어야 한다. 또한 프로파일링 기법 실시국에서 인권침해의 논란이 제기된 점을 고려하여 인권침해를 최소화하는 방안에 대한 충분한 사전검토가 선행되어야 할 것이다.[89]

우리나라의 경우 현재 국내법에서는 수하물에 대해 프로파일링할 수 있는 실시규정을 마련되어 있으나 승객에 대한 프로파일링을 실시할 수 있는 법적 뒷받침이 부족하다. 이에 따라 동제도의 국내도입을 위해서는 항공안전 및 보안에 관한 법률 등 관련법규를 검토, 명확한 시행 근거를 마련할 필요가 있다.

89) Ibid., p.172.

# 참 고 문 헌

황호원・이규황, “항공보안에서의 프로파일링 연구”, 항공우주법 학회지, 제22권 2호 (2007).

김장환・강자영, “미국의 항공보안정책 적용과 프라이버시 문제점”, 한국항공운항학회지, 제13권 제3호(2005).

Addie S. Ries, “Comment, America's Anti-Hijacking Campaign - Will It Conform to Our Constitution?”, N.C. J.L. & Tech., Vol.3 (2001).

Agent Infiltrated Terror Cell, U.S. Says, CNN.com, Aug. 11, 2006, http://www.cnn.com/2006/US/08/10/US.security/index.html.

Allen Shoenberger, “Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead”, Ind. Int'l & Comp. L. Rev., Vol.17 (2007).

Anita Ramasastry, “Lost in Translation? Data Mining, National Security and the “Adverse Inference” Problem”, Santa Clara Computer & High Tech. L.J., Vol.22(2006).

Bennie G. Thompson, “The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy”, PGH. J. Tech. L. & Pol'y, Vol.10(2006).

Bob Barr, “Post-9/11 Electronic Surveillance Severely Undermining Freedom”, Val. U. L. Rev.,Vol.41(2007).

Chris Jay Hoofnagle, “Big Brother's Little Helpers: How Choice Point

and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement", N.C. J. Int'l L. & Com. Reg., Vol.29(2004).

Daniel J. Solove, "Reconstructing Electronic Surveillance Law", Geo. Wash. L. Rev., Vol.72(2004).

Daniel J. Steinbock, "Designating the Dangerous: From Blacklists to Watch Lists", Seattle U. L. Rev., Vol.30(2006).

Daniel W. Sutherland, "Homeland Security and Civil Liberties: Protecting America's Way of Life", Notre Dame J. L. Ethics & Pub. Pol'y, vol.19(2005).

Darren W. Davis & Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", Am. J. Pol. Sci., Vol.48(2004).

Deborah von Rochow-Leuschner, "CAPPS II and the Fourth Amendment: Does It Fly?", J. Air L. & Com., Vol.69(2004).

Dempsey & Lara M. Flint, "Commercial Data and National Security", Geo. Wash. L. Rev., Vol.72(2004).

Drew Shenkman, "Comment, 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", Alb. L.J. Sci. & Tech., Vol.17(2007).

Edward C. Harris, "Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers", Am. U. Int'l L. Rev., Vol.22(2007).

Eric P. Haas, “Comment, Back to the Future? The Use of Biometrics, Its Impact on Airport Security, and How This Technology Should Be Governed”, J. Air L. & Com., Vol.69(2004).

Francesca Bignami, “European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining”, B.C. L. Rev., Vol.48(2007).

Gehan Gunasekara, “The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows”, Int'l J.L. & Info. Tech., Vol.15(2007).

Humphrey G. Dawson, “Civil Aviation, Hijacking and International Terrorism: An Historical and Legal Review”, Int'l Bus. Law, Vol.15(1987).

Jack H. Daniel III, “Comment, Reform in Airport Security: Panic or Precaution?”, Mercer L. Rev., Vol.53(2002).

Jamie L. Rhee, “Comment, Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats”, Depaul L. Rev., Vol.49(2000).

Joanna L. Geraghty, Christopher G. Kelly & Judith R. Nemsick, “District Court Dismissal of In re JetBlue Airways Corp. Privacy Litigation Moves to the Forefront of Courts Dismissing Privacy Claims Against Air Carriers”, Air & Space Lawyer, Vol.20(2005).

K. A. Taipale, Technology, “Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd”, Yale J.L. & Tech., Vol.7(2004-2005).

Matthew R. Van Wasshnova, “Note: Data Protection Conflicts Between

the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange", Case W. Res. J. Int'l L., Vol.39 (2007-2008).

Michael J. DeGrave, "Note, Airline Passenger Profiling and the Fourth Amendment: Will CAPPS II Be Cleared for Takeoff ?", B.U. J. Sci. & Tech. L., Vol.10(2004).

Paul Rosenzweig, "Civil Liberty and the Response to Terrorism", Duq. L. Rev., Vol.42(2004).

Peter M. Shane, "The Bureaucratic Due Process of Government Watch Lists", Geo. Wash. L. Rev., Vol.75(2007).

Phillip A. Karber, "Re-Constructing Global Aviation in an Era of the Civil Aircraft as a Weapon of Destruction", Harv. J.L. & Pub. Pol'y, Vol.25(2002).

R.I.R. Abeyratne, "The Effects of Unlawful Interference with Civil Aviation on World Peace and the Social Order", Transp. L.J., Vol.22(1995).

Richard Sobel & John A. Fennel, "Troubles with Hiibel: How the Court Inverted the Relationship Between Citizens and the State", S. Tex. L. Rev., Vol.48(2007).

Richard W. Bloom, Commentary on the Motivational Psychology of Terrorism Against Transportation Systems: Implications for Airline Safety and Transportation Law, Transp. L.J., Vol.25 (1998).

Robert Crandall, “Security for the Future: Let's Get Our Airlines Flying, Address at the Freedom Versus Fear: The Future of Air Travel Conference (Oct. 29, 2001)”, J. Air L. & Com., Vol.67(2002).

Ruwantissa Abeyratne, “Attacks on America - Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada”, J. Air L. & Com., Vol.67(2002).

Ryan L. Bangert, “Comment, When Airlines Profile Based on Race: Are Claims Brought Against Airlines Under State Anti-Discrimination Laws Preempted by the Airline Deregulation Act?”, J. Air L. & Com., Vol.68(2003).

Stephen W. Dummer, “Comment, Secure Flight and Data Veillance, a New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It”, Miss. L.J., Vol.75(2006).

Stephen W. Dummer, “False Positives and Secure Flight Using Dataveillance When Viewed Through the Ever Increasing Likelihood of Identity Theft”, J. Tech. L. & Pol'y, Vol.11 (2006).

Timony M., Ravich, “Is Airline Passenger Profiling Necessary”, U. Miami L. Rev., Vol.62(2007).

Transp. Sec. Admin., Prepare for Takeoff: Permitted and Prohibited Items, available at http://www.tsa.gov/assets/pdf/Prohibited%20 and%20Permitted%20Items printerfriendly 3-16- 07.pdf.

Yousri Omar, “ote, Plane Harassment: The Transportation Security Administration's Indifference to the Constitution in Administering

the Government's Watch Lists” Wash. & Lee J. C.R. & Soc. Just., Vol.12(2006).