Journal of Technology Law & Policy

Volume 11 | Issue 2 Article 4

December 2006

False Positives and Secure Flight Using Dataveillance When Viewed Through the Ever Increasing Likelihood of Identity Theft

Stephen W. Dummer

FALSE POSITIVES AND SECURE FLIGHT USING DATAVEILLANCE WHEN VIEWED THROUGH THE EVER INCREASING LIKELIHOOD OF IDENTITY THEFT

Stephen W. Dummer[*]

* J.D., University of Mississippi School of Law 2006; B.A. *cum laude* with Honors, Phi Beta Kappa, University of Wyoming 2003; A.A. with Honors, Phi Theta Kappa, Northwest College 2000. Stephen W. Dummer was an Executive Articles Editor for the *Mississippi Law Journal* and is currently an associate with the law firm of Allen, Cobb, Hood & Atkinson, P.A. in Gulfport, MS. Before attending law school he was a Sergeant in the U.S. Marine Corps.

Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.[1]

[H]e that filches from me my good name, robs me of that which not enriches him, but makes me poor indeed.[2]

I. INTRODUCTION

On September 11, 2001, 19 terrorists managed to board domestic commercial aircraft despite the current security measures; fly 2 planes into the World Trade Center causing its eventual collapse, and kill approximately 2800 people.[3] The hijackers crashed a third aircraft into the symbolic heart of America's military, the Pentagon, killing another 184 people and injuring dozens more.[4] Yet another plane was crashed into the tranquil Pennsylvania countryside killing 40 more. An unknown fact to many Americans was that the hijackers had been identified as flight risks that very day by airport security but were allowed to board their planes.[5] In response to this great tragedy, Congress descended upon a course of action which will change the face of our country's liberty for years to come.

---

1. Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor*, Nov. 11, 1755, *in* 6 THE PAPERS OF BENJAMIN FRANKLIN 242 (Leonard W. Labaree ed., 1963). This same inscription is located on the base pedestal of the Statute of Liberty.

2. WILLIAM SHAKESPEARE, OTHELLO act 3, scene 3 (7th ed. 1958). Shakespeare, however, failed to recognize the future permutations of identity theft or did not have to deal with its far-reaching repercussions. If he had known what lay ahead, the "great bard" would have spoken about how identity theft can enrich criminals with little to no threat of apprehension and the lasting effects it could have on the victim.

3. The exact number of lives lost at the world trade center is unknown. *See* Rebecca Blackmon Joyner, Note, *An Old Law for a New World? Third-Party Liability for Terrorists Acts-From the Klan to Al Qaeda*, 72 FORDAM L. REV. 427, 461-62 n.281 (2003); Leigh A. Kite, Note, *Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will A Redesigned CAPPS II System Meet the Constitutional Challenge?*, 61 WASH. & LEE L. REV. 1385, 1387 (2004).

4. *See generally* Phil Hirschkorn, *New York Adjusts Terrorist Death Toll Downward*, CNN.COM, Aug. 22, 2002, *available at* http://www.cnn.com/2002/US/08/22/911.toll (referencing death toll at attack sites) (last visited Aug. 24, 2006). Analysts have suggested that the fourth plane also targeted the Pentagon but passengers or crew may have managed to thwart the hijacker's efforts, thereby preventing more deaths. *Id.*

5. The pilot program of Computer-Assisted Passenger Prescreening System (CAPPS) correctly identified the would-be hijackers as threat risks but no legislation was in place whereby passengers could be refused boarding if identified by the CAPPS system. Kite, *supra* note 3, at 1387-88.

America's fear of terrorism had arrived and embedded itself in the mind of every citizen.[6] It has been said that terrorism's goal is to kill "the few," to frighten "the many."[7] The events of September eleventh unmistakably accomplished this goal as the nation became gripped with fear and uncertainty. With so much doubt pervading our modern psyche, citizens cling to their routine to establish order out of chaos. However, once that routine becomes the source of uncertainty as it did after 9/11, inevitably people fight to re-establish order and control. The "fly in the ointment," compounding America's attempt to regain control, is that not all parties are playing by the same set of rules. Now in addition to the ever present threat of terrorism, Americans must face a new threat, having their identity stolen by opportunistic charlatans.[8]

Attempts to find order amongst chaos have led America to some of its darkest hours. Rampant fear has unfortunately flourished into the erosion of civil liberties.[9] American history is fraught with examples of Congress or the courts drastically limiting freedom of expression or civil liberties.[10] Apparently, history has not been America's teacher. America is once again

6. *See* 147 CONG. REC. S9583 (daily ed. Sept. 21, 2001) (senate announcing realization of terrorist threat and illustrating concern that security of airports is a matter of national security).

7. *See generally* CHUCK LAWLISS, THE MARINE BOOK: A PORTRAIT OF AMERICA'S MILITARY ELITE (1992). In contrast, the goal of war is to kill large numbers to force a change in position of the few. *Id.*

8. Criminals are by no means "stupid" in the general sense of the word. Criminals have realized it is safer and more productive to steal someone's identity than to resort to traditional crimes like armed robbery. Chris Osher, *Region Ripe For Identity Thieves*, PITTSBURGH TRIB. REV., July 31, 2005. According to Osher, one deputy sheriff overhead an inmate tell another inmate:

> I walk into a liquor store and stick a gun in a kid's ribs, and I'll get seven to [fifteen] years . . . for $120 bucks and a carton of cigs. . .[but if I find] a way to get a person's name and their Social Security number, the most I'll get is a year. But with that same name and Social Security I can take out $10,000 to $100,000 without even batting an eye.

Id. This new threat, combined with the fear of terrorism, creates an American landscape ripe for fear and uncertainty. How-to-Books are now available to the savvy criminal wishing to learn the trade of identity theft. *See* Alan Sipress, *An Indonesian's Prison Memoir Takes Holy War into Cyberspace*, WASH. POST, Dec. 14, 2004, at A19. Therein, Sipress discusses a chapter written by a cyber-terrorist, Imam Samudra entitled, "Hacking, Why Not?" *Id.* (Samudra describes how to launder money, get away with online credit card scams, manipulate computer language and other useful cyber-techniques).

9. *See generally* DAVID COLE, ENEMY ALIENS: DOUBLE STANDARDS AND CONSTITUTIONAL FREEDOMS IN THE WAR ON TERRORISM (2003); Alan Brinkley, *A Familiar Story: Lessons from Past Assaults on Freedoms*, *in* THE WAR ON OUR FREEDOMS 23 (Richard C. Leone & Greg Anrig, Jr. eds., 2003); Diane P. Wood, *The Rule of Law in Times of Stress*, 70 U. CHI. L. REV. 455, 455 (2003); Kite, *supra* note 3, at 1387.

10. *See, e.g.*, COLE, *supra* note 9; Wood, *supra* note 9, at 455; Kite, *supra* note 3, at 1389.

at a crossroad and leaning toward the well worn path of civil liberty erosion.

After September 11th, legislation was passed which began eroding our civil liberties.[11] The USA PATRIOT Act authorized intrusive surveillance and data reconnaissance targeting citizens and visitors alike.[12] Remembering past wrongs of this country and cautioning the Senate against further erosions of civil liberty, Senator Russ Feingold said, "We will lose [the war on terrorism] without a shot being fired if we [begin] sacrifice[ing] the liberties of the American people in the belief that by doing so we will stop the terrorists."[13] Senator Feingold's plea apparently fell on deaf ears as America charged once again into rash action. America's systemic response was to focus on its physical infrastructure rather than emerging cyber security issues.[14]

Congress proceeded down a path where national security was once again placed before fundamental rights.[15] Congress's passage of the ATSA[16] and the ATSSSA[17] federalized many services and personnel previously exclusively private.[18] While neither the ATSA nor ATSSSA

11. What is now known as the Patriot Act became law on October 26, 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 107 H.R. 3162 (2001) [hereinafter USA PATRIOT Act].

12. *Id.* § 201.

13. 147 CONG. REC. S10, 570 (daily ed. Oct. 11, 2001) (statement by Senator Feingold while discussing the USA PATRIOT Act).

14. John D. Podesta & Raj Goyle, *Perspective: Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World*, 23 YALE L. & POL'Y REV. 509 (2005) (quoting Paul B. Kurtz, a former senior official in the Bush Administration and Executive Director of the Cyber Security Industry Alliance).

15. Kevin Bankston & Megan E. Gray, *Government Surveillance and Data Privacy Issues: Foundations and Developments*, PRIVACY & INFO L. REP., Apr. 2003, at 1, 3 (arguing that with little to no regard for the disastrous impact on civil liberties the legislature passed the USA PATRIOT Act with almost no debate). The USA PATRIOT Act greatly expands the government's ability to spy upon its own citizens unchecked while weakening oversight which could prevent future abuses. *Id.*; *see* Kite, *supra* note 3, at 1386 n.21. The USA PATRIOT Act enables far-reaching invasion of privacy and monitoring of citizens and suspected terrorists including, but not limited to, planting surveillance devices on electronics and amassing large computer databases containing sensitive private information. *See generally* NAT HENTOFF, THE WAR ON THE BILL OF RIGHTS AND THE GATHERING RESISTANCE (2003).

16. Aviation and Transportation Security Act, Pub. L. No. 107-71 (2001) [hereinafter ATSA].

17. Air Transportation Safety and System Stabilization Act, Pub. L. No. 107-42 (2001) [hereinafter ATSSSA].

18. *See generally* David T. Norton, *Recent Developments in Aviation Law*, 67 J. AIR L. & COM. 1107, 1111-12 (2002).

overtly erode civil liberties CAPPS,[19] CAPPS II[20] and Secure Flight do. Because of staunch opposition CAPPS II was not implemented by the Transportation Security Act (TSA). A revised version known as "Secure Flight" is now ready to be launched in 2006.[21] However, before Secure Flight's activation, TSA must consider and implement procedures addressing the ever growing problem of identity theft.[22]

Part II of this Article will provide a brief history of Secure Flight and its application in passenger surveillance. Part III will then discuss data mining and information utilization. Part IV discusses identity theft and its widespread effects in America. Part V discusses the effects of false positives likely to result from identity theft and the lack of redress procedures used by TSA for those flagged during the check in process.

II. A SHORT ACCOUNT OF COMPUTER AUTOMATED PASSENGER SURVEILLANCE

After the crash of TWA Flight 800 in 1996, the U.S. government formed the Gore Commission which recommended several suggestions to the aviation industry which sought to enhance their security systems and make air travel safer.[23] The Gore Commission used this platform to conceptualize the Computer Automatic Passenger Surveillance (CAPS) and the Computer-Assisted Passenger Prescreening System (CAPPS).[24] CAPPS was originally developed by Northwest Airlines in conjunction with the FAA to integrate the abilities of a computer with available

19. CAPPS was developed by Northwest Airlines with a grant from the Federal Aviation Administration (FAA) as a passenger profiling security mechanism for aviation. Charu A. Chandrasekhar, Comment, *Flying While Brown: Federal Civil Rights Remedies to Post 9/11 Airline Racial Profiling of South Asians*, 10 ASIAN L.J. 215, 221 (2003).

20. Computer-Assisted Passenger Prescreening System II (CAPPS II) was an improved system developed by the Transportation Security Administration (TSA) based on the original platforms of CAPS (Computer Assisted Passenger Screening) and CAPPS. *See id.* at 222-23. CAPS and CAPPS were replaced by the more advanced CAPPS II. Kite, *supra* note 3. CAPPS II was subsequently replaced by Secure Flight. *Id.* at 1401.

21. James X. Dempsey & Lara M. Flint, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA Patriot Act: Surveillance, Records & Computers: Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1468 (2004).

22. House Select Comm. On Homeland Sec.: Hearing Before the Subcomm. on Econ. Sec., Infrastructure Protection, and Cyber Sec.; Hearing on Passenger Pre-Screening, 110th CONG. (2005) (Statement of James Dempsey, Exec. Dir., Ctr. for Democracy and Tech.) (noting that identity theft poses a serious problem to passenger screening and to Secure Flight).

23. Chandrasekhar, *supra* note 19, at 221.

24. White House Comm. on Aviation Safety and Sec., Final Report to Pres. Clinton (1997), *available at* http://www.fas.org/irp/threat/212fin~1.html (last visited Nov. 3, 2005) [hereinafter Gore Commission].

information systems to focus on the growing concerns over aviation safety.[25] The FAA then adapted CAPS into the CAPPS which they offered on a volunteer basis to all major airlines for implementation.[26] CAPPS uses approximately forty pieces of personalized passenger data, retained in secrecy, to detect passengers who fit a "profile" based on previously determined criteria.[27] These data probably included a litany of basic travel information.[28] The Gore Commission maintained that no religious or racial data would be contained in the database but according to Chardrasekhar, Asian advocacy groups have noted that the CAPPS profiling system unfairly targeted them as "increased risk" because of their national or racial identity.[29] Unfortunately, the CAPPS system and its data components were never released before the system was taken offline.[30]

Shortly after September 11th, the ATSA mandated the creation, under section 136, of an improved version of CAPPS to be implemented at all airports in the United States and foreign hubs which service inbound flights to America.[31] CAPPS II had been tested in several airports but heavy resistance precluded its originally scheduled implementation at the end of 2004.[32] CAPPS II, as originally conceived, evaluated all incoming passengers utilizing a process whereby the person's identification was matched with a government linked commercial database to provide a computer generated risk assessment.[33] Civil liberty advocates challenged CAPPS II claiming it treated all incoming passengers as potential terrorists

25. *Id.*

26. Chandrasekhar, *supra* note 19, at 221.

27. *Id.*

28. Information likely included the passenger's address, method of ticket purchase, travel companions, rental status, ticket purchase date, departure date, destination, origin, and whether the ticket was one way or round trip. Chandrasekhar, *supra* note 19, at 221 (citing Air Passenger Profiling: Hearings Before the Aviation Subcomm. of the House Comm. on Transp. and Infrastructure, 107th CONG. (2002)). This writer has been unable to locate any source which can verify what information was actually included in either CAPS or CAPPS.

29. *See id.* at 226; *see generally* Jamie L. Rhee, Comment, *Rational and Constitutional Approaches To Airline Safety in the Face of Terrorist Threats*, 49 DEPAUL L. REV. 847 (2000).

30. Rhee, *supra* note 29, at 865. The components were never made public so academics may only speculate as to what the components were prior to the systems removal. *Id.*

31. Kite, *supra* note 3, at 1387.

32. *See* Press Release, U.S. Dep't of Homeland Sec., Undersecretary Hutchinson's Remarks at a CAPPS II Media Roundtable, *available at* http://www.dhs.gov/dhspublic/display?content=3166 (Feb. 13, 2004) (last visited Aug. 24, 2006). Civil liberty organizations strongly opposed CAPPS II because of fears that people would be accidentally detained without actually catching all terrorists. *See* Kite, *supra* note 3, at 1391-92.

33. Kite, *supra* note 3, at 1391; *see generally* Notice of Status of Sys. of Rec.; Interim Final Notice; Request for Further Comments, 68 Fed. Reg. 45265 (Aug. 1, 2003).

while privacy groups vehemently opposed the use of private information being used against would be passengers.[34]

With CAPPS II, passengers would have been coded one of three ways upon arriving at the terminal. (1) Red, the passenger is "untrustworthy" and therefore a risk to the aircraft, wherein law enforcement would be notified and the person would be arrested. (2) Yellow, the passenger is "potentially untrustworthy" or *may be* a risk, but further investigation is required wherein, depending on the outcome of the investigation, they would be allowed to board the aircraft or precluded from flying. (3) Green, "not *un*trustworthy" or the passenger had been identified as possessing limited risk behavior making them eligible to board the aircraft.[35]

Because of the opposition leveled at CAPPS II, the TSA and the White House revoked the implementation of the program and demanded that it be redesigned to respond to the policy concerns voiced by the opposition. The new system, "Secure Flight" incorporates modifications that presumably changed the risk assessment process and addressed the pervasive privacy concerns which were inherent in the CAPPS II system. Realistically however, Secure Flight has simply eliminated the middle classification of "yellow" and removed certain computer risk assessment algorithms, mined from vast commercial databases, in its verification process.[36] Secure Flight still uses data mining[37] and computer algorithms

---

34. *See* Kite, *supra* note 3, at 1391-92; *see* Leslie Miller, *New Passenger Screening Plan Not Ready to Fly*, CHI. SUN-TIMES, July 14, 2004, at 46; Matthew L. Wald, *Government Is 'Reshaping' Airport Screening System*, N.Y. TIMES, July 14, 2004, at 46.

35. K.A. Taipale, *Technology, Security & Privacy: The Fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd*, 7 YALE SYMP. L. & TECH. 123, *12 (2005) (Taipale explained the program would label flyers as, "untrustworthy and denied access (and there may be false positives), those deemed not-untrustworthy who are in-fact trustworthy and are allowed access (good guys), and those deemed not-untrustworthy who are in-fact untrustworthy but have not been yet identified as such and may be mistakenly allowed access (false negatives)").

36. Kite, *supra* note 3, at 1392.

37. Data mining is the process of compiling and aggregating individual data to be used for computational purposes of personal evaluation. K.A. Taipale and Paul Rosenzweig have identified three distinct applications:

> [F]irst, subject-oriented link analysis, that is, automated analysis to learn more about a particular data subject, [their] relationships, associations and actions; [S]econd, "pattern-analysis" (or "data mining" in the narrow sense), that is, automated analysis to develop a descriptive or predictive model based on discovered patterns; and,
>
> [T]hird, "pattern-matching," that is, automated analysis using a descriptive or predictive model (whether [the model] itself developed through automated analysis or not) against [additional datasets] to identify other related (or "like") data subjects (people, places, things, relationships, etc.).

taken from governmental databases of known terrorists compared against huge commercial databases containing private information.[38] To understand the importance of Secure Flight's implementation, a brief analysis of dataveillance and data mining must be undertaken.[39]

III. DATAVEILLANCE, DATA MINING A MODERN REBIRTH OF THE PRIVATE INVESTIGATOR

A. *Forms of Identification Captured*

The different types of information retrieved by data mining, to be used for dataveillance, while complex on its face, is nothing more than a straightforward attempt to accurately identify someone. The identification process can be broken down into three basic forms: Entity, Identity, and Attribute.[40] *Entity resolution* is the "process whereby different identifiers or different identities are resolved [] to the same entity or individual usually through analysis of shared attributes."[41] Simply put, it is a determination, at a certain confidence level, that the person presenting their ID in front of the teller is whom the computer designates.[42]

Identity authentication is the level of confidence with which a computer generated "identifier" is assigned to the correct person. For example, the computer must determine whether "Bill Jones" is the same

---

K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, *13 (2003) (noting that these aggregated data and computer analysis systems are tools to aid in human analytical thinking in order to manage and use the vast amounts of information available); *see also* Paul Rosenzweig, *Proposals for Implementing the Terrorism Information Awareness System*, 2 GEO. J.L. & PUB. POL'Y 169 (2004).

38. Dempsey & Flint, *supra* note 21, at 1468.

39. The term dataveillance, also known as pattern analysis or knowledge extraction, is the process of analyzing aggregated data based on p-values dependent upon a desired level of error. Dempsey & Flint, *supra* note 21, at 1463. That level of error, known as the β is based upon a level of significance known as α. M. ANTHONY SCHORK & RICHARD D. REMINGTON, STATISTICS WITH APPLICATIONS TO THE BIOLOGICAL AND HEALTH SCIENCES 166 (3d ed. 2000) (noting that type I errors are commonly known as α errors and type II errors are known as β errors). That information is then converted into an output based upon a level of confidence to forecast a potential outcome. Taipale, *supra* note 37, at *10. The term "dataveillance," while cleverly combining "surveillance" with "data" analysis is actually more technical than the word suggests. *Id.* Dataveillance uses more than a simple review of data to survey an individual because the amount of data is too vast for an efficient human analysis. *Id.*

40. Taipale, *supra* note 37, at *10-*11.

41. *Id.* at *11.

42. *Id.*

person as William Jones or Will Jones.[43] This identity match can be achieved by incorporating technological evaluation methods like passwords, fingerprint ID, DNA sniffers and retina and iris scanners.[44] Once *entity* and *identity* are assured and the person is properly linked to the information being represented on the computer,[45] *attribute* examination must be completed.[46]

Attribute authentication is the "process of establishing confidence that an attribute [] applies to a specific entity."[47] Once a person is properly identified, their information needs to be used for something practical like assessing risk.[48] Once these three levels of analysis are completed, the ability to match the entity against an authorized watch list is only as useful as the veracity of the watch list or database which provided it.[49]

All these data, warehoused by sources which store it, must not only be useful but also obtained through legal channels. While much of the information collected does not amount to a direct invasion of privacy, the aggregation of information for the explicit purposes of examination and extrapolation does create civil liberty concerns. Dataveillance poses constitutional concerns because it raises privacy issues and utilizes *lawful* activities to "presume" future guilt. Jeffrey Rosen capsulated this concern to a special subcommittee[50] and Congress recently heard testimony requesting a nearly limitless search into people's lives for the sake of security.[51] Serious constitutional issues arise when (1) privacy rights are

43. *Id.* at *10-*11; Dempsey & Flint, *supra* note 21, at 1464-65.

44. Taipale, *supra* note 37, at 11.

45. *Id.*

46. It is appropriate to note that identity theft can cause serious problems at any stage of the passenger prescreening process because the person seeking admittance could be either the thief or the actual person. If it is the actual person presenting themselves for admission, they can be denied access because of the thief's prior activities.

47. Taipale, *supra* note 37, at *11.

48. *Id.*

49. *Id.*; *see generally* BRUCE SCHNEIER, BEYOND FEAR 38-40 (2003).

50. Rosen stated that when the government takes part in, "mass dataveillance to conduct general searches of millions of citizens without cause to believe that a crime has been committed, the searches arguably raise the same dangers in the twenty-first century as the general warrants that the [f]ramers of the Fourth Amendment feared in the eighteenth century." Data Mining: Current Applications and Future Possibilities: Hearing Before the House Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, Comm. on Gov't Reform, 108th CONG. (2003) [hereinafter Rosen] (statement of Jeffrey Rosen, Assoc. Professor, George Washington Univ. Law Sch.), *cited in* Dempsey & Flint, *supra* note 21, at 1465 n.20.

51. Registered Traveler Program Implementation: Hearing Before the House Subcomm. on Econ. Sec., Infrastructure Protection, and Cyber Sec., 110th CONG. (2005) (emphasis added) (statement of Jim Harper, Dir., Info. Pol'y Studies, Cato Institute). Jim Harper testified to a House Select committee that, "The way to do real identity-based security is to do deep, deep background

violated, (2) guilt is assigned before the crime, or (3) the government creates a pretext screening to circumvent the Fourth Amendment.[52]

B. *Background of Dataveillance*

Due process and Fourth Amendment issues are significant problems when using personal data, without consent, to create risk assessments, whereby an individual may be denied civil liberty protections. The federal government, through the Information Analysis and Infrastructure Protection Directorate at the Department of Homeland Security Integration Center, has given the FBI the authority to use data mining with private data warehousing companies.[53] This act permits the U.S. government to circumvent the Privacy and Information Act because the database is not technically a "government database."[54] Current laws allow these commercial databases to be used for investigation of terrorist activities without the hindrance of oversight by applicable privacy laws because they are not *government* databases. Furthermore, privacy laws which would ordinarily give citizens the right to review all their personal information does not apply because the information is "privately maintained."[55]

Government officials have supported their plans and assured privacy groups that their use of the commercial data will be strictly monitored, yet there are no programs in place which exist to oversee the government's actual use of these databases.[56] Moreover, no legislation is in place to control the privately held data, such as the Fair Credit Reporting Act

---

checks into people, *know everything about them*, where were they educated, what do they think about stuff, how many kids do they have." *Id.*

52. For a more complete discussion of these topics, see Stephen W. Dummer, Comment, *Secure Flight and Dataveillance, A New Type Of Civil Liberties Erosion: Stripping Your Rights Even When You Don't Know It*, 75 MISS. L.J. 583 (2005).

53. *See generally* Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask Choicepoint: U.S. Agencies' Growing Use of Outside Data Suppliers Raises Privacy Concerns*, WALL ST. J., Apr. 13, 2001, at A1.

54. 5 U.S.C. § 522a(d) (Records Maintained on individuals). Because the government does not "maintain" the database, citizens would be precluded from exercising the privilege created by the Privacy Act. *See, e.g.*, Dempsey & Flint, *supra* note 21, at 1472.

55. Dempsey & Flint, *supra* note 21, at 1472. The USA PATRIOT Act contains almost no First Amendment safeguards and section 203 allows extensive sharing of information which is not related to terrorist activities without regard to whether the information deals with legal or illegal activities. USA PATRIOT Act, *supra* note 11, § 203(a); Dempsey & Flint, *supra* note 21, at 1483. The USA PATRIOT Act circumvents grand jury powers but with none of the criminal justice system protections. USA PATRIOT Act, *supra* note 11, § 203(a). Moreover, no judicial approval is required for the government's investigative activities nor does the act require disclosure of the information used in identifying the individual. *Id.*

56. Dempsey & Flint, *supra* note 21, at 1471; *see, e.g.*, Fair Credit Reporting Act, 15 U.S.C.A. 1681-1691 (West 1998 & Supp. 2003) [hereinafter FCRA].

(FCRA), which was passed to protect consumers from disclosure of inaccurate information held by consumer credit reporting agencies.[57] Thus, private warehouses could dispense harmful errors with impunity to Secure Flight. To make matters worse, the information held within these commercial databases is absolutely secret.[58] According to the TSA and the Department of Homeland Security, if this information were released it could permit would-be-terrorists to circumvent the system.[59] Understandably, there are important competing interests between national security and notifying the public, however, at what cost should America's safety come to its citizens?[60]

C. *Constitutional Issues for the Fourth Amendment and Dataveillance*

The Fourth Amendment protects citizens from unreasonable searches and seizures.[61] According to Rosen, the U.S. Constitution's original Framers were expressly concerned with investigations which delve into a person's private life.[62] While it is unlikely that the Framers could envision mass private commercial databases being used by the government's "thinking machines" or algorithmic risk assessment on people boarding "flying machines," the Fourth Amendment likely applies. The Constitution was drafted in such a manner as to provide for unseen contingencies and technological advances. Now that emerging technologies are being used, the American court system must apply all available resources to ensure the Framers' intent is respected and that civil liberties are protected. Dataveillance, at its heart, investigates a person who has yet to commit a crime and then determines their proclivity for criminal behavior based on unrelated past actions. While this seemingly Orwellian example may

57. Dempsey & Flint, *supra* note 21, at 1471. Unfortunately, the FCRA has done little to spare victims from the wages of damage wrought by identity thieves. The FCRA only provides avenues for victims to learn about the theft but does nothing itself to help fix a victim's destroyed credit. The victim is left to spend hundreds of hours making calls and thousands of dollars to fix their credit. Maria Bartiromo, *Nik Deogun & Ed Mierzwinski Discuss Identity Theft*, WALL ST. J. REP., July 17, 2005, at A1 ("It can take victims anywhere from 60 to 600 hours to undo the damage. And the cost, well anywhere from $1,200 to $16,000 if you factor in such expenses as legal fees, higher interest rates and lost wages."); Tom Zeller, Jr., *Identity Crises*, N.Y. TIMES, Oct. 1, 2005, at B1 (noting that victim devoted forty hours a week for several months to clear up his credit). Moreover, the FCRA does nothing to help victims who have had their criminal histories corrupted by criminals. Catherine Pastrikos, Comment, *Identity Theft Statutes: Which Will Protect Americans the Most?* 67 ALB. L. REV. 1137, 1138 (2004).

58. Pastrikos, *supra* note 57, at 1137; Kite, *supra* note 3, at 1425.

59. Dempsey & Flint, *supra* note 21, at 1489.

60. *See id.* at 1489-90.

61. U.S. CONST. amend IV.

62. Dempsey & Flint, *supra* note 21, at 1467 n.20.

appear to exaggerate the present dataveillance capabilities; the reality of Secure Flight is not too far removed from George Orwell's post war novel, *Nineteen Eighty-Four*, and its frightening concept of "thought crime"[63]

Compelling reasons exist to prevent persons from hijacking aircraft. However, the error rate for Secure Flight could incorrectly flag nearly 800 to 1200 persons a day as "flight risks."[64] That means approximately one thousand innocent persons per day could be denied their fundamental right to travel because a data output suggested they *may* pose a flight risk.[65] Unfortunately, a detailed discussion of these constitutional dilemmas is beyond the scope of this Article.[66] More important for our purposes is a discussion of the exacerbating effects of identity theft on Secure Flight.

IV. IDENTITY THEFT: THE EVER EXPANDING THREAT DESTROYING AMERICA'S CONFIDENCE

A. *New Flies in the Old Ointment*

Life in America is stressful enough considering the increasing workload, diminishing amounts of free time along with the ever present push for technological advancement and the necessity to "keep up to speed" or risk losing your job, spouse, or home. Along with these blossoming stress factors, criminals have graciously provided Americans with yet another compounding factor to make our lives even more complicated, stealing our identities for their own pecuniary gain.[67] Innocent activities subject Americans to months or years of effort and

63. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1st Am. ed. 1949).

64. *Id.* at 1421; *see also* Sara Kehaulani Goo, *Fliers to Be Rated for Risk Level: New System Will Scrutinize Each Passenger, Assign Color Code*, WASH. POST, Sept. 9, 2003, at A01 (stating that security system will incorrectly identify two percent of passengers as flight risks). *See infra* Parts V.A-B (discussing error rates).

65. While seeming far fetched now, this could be something as innocuous as buying oatmeal on a Tuesday with your local retail bonus card and then accessing a flagged web site the next day. Because no explanation has been given to the types of information or the algorithms used, it is possible that completely lawful activities, when combined, could end up identifying a passenger as a potential terrorist.

66. For a discussion of the *Mathews* Factors and Secure Flights Redress Procedures as they apply to a constitutional review, see Dummer, *supra* note 52. *See also* KATHLEEN M. SULLIVAN & GERALD GUNTHER, CONSTITUTIONAL LAW (14th ed. 2001); William D. Anderson, Jr., *Investigation and Police Practice: Overview of the Fourth Amendment*, 82 GEO. L.J. 597 (1994).

67. *See* Michael Higgins, *Identity Thieves*, 84 A.B.A. J. 42, 45 (1998). Higgins notes: "[I]dentity theft victims . . . are left trying to explain [the problem] to creditors and collection agencies, who often suspect the victim of being the imposter . . . when [the creditors] never bothered to ask [the thief] to prove who [they were]." *Id.*

thousands of dollars to clean up their credit and good names.[68] ID thieves can expose citizens to the humiliation, anger and frustration of being labeled a criminal.[69] Moreover, with the implementation of Secure Flight, identity theft victims will likely be denied the right to board aircraft if their identities have been used in a manner which flags them as a "threat."[70]

Beyond antiquated methods of stealing one's identity, modern thieves may harvest identities with new scams like: phishing, hooking, web diverting, fraudulent Internet auctions, international modem dialing, pretexting, skimming, and web cramming, to name only a few.[71] Americans must now be ever vigilant to protect themselves from identity theft. Sadly, many American's identities are stolen through no fault of their own.[72] Some thefts occur because businesses fail to take appropriate care of customer files or information.[73] Some thefts occur because

68. FEDERAL TRADE COMMISSION, TAKE CHARGE: FIGHTING BACK AGAINST IDENTITY THEFT 1-2 (2005) [hereinafter FTC, FIGHTING BACK]; *see also* FEDERAL TRADE COMMISSION, ID THEFT: WHAT IT'S ALL ABOUT 1-3 (2005) [hereinafter FTC, ID THEFT]. The FTC noted that activities entered into everyday like: writing checks, renting cars, mailing tax returns, changing service providers or even applying for another credit card exposes citizens to identity theft. In fact, something as simple as an e-mail or instant message on the Internet can expose victims to numerous types of identity theft. *See generally* High-Technology Crime Prosecutor/Investigator Resource CD-ROM: *The Internet, Email and Internet Chat Investigations: A Guide for Prosecutors and Investigators*, pts. II & III (Sept. 2004). This is especially relevant because studies project that by 2007 people will engage in approximately 1,380 billion instant messages per day and even more e-mails. *Id.*

69. FTC, ID THEFT, *supra* note 68, at 1; Kristin Davis, *But, Officer, That Isn't Me*, KIPLINGER'S PERSONAL FIN., Oct. 2005, at A1. The Better Business Bureau suggests that about 4% of the 9.3 million identity theft victims each year will have their names given to law enforcement by the criminals to escape punishment, thereby wrongly labeling the victim a "criminal." *Id.*

70. Privacy Laws & Data Broker Servs.: Hearing Before the Senate Commerce, Sci., & Transp. Comm., 110th CONG. (2005) (statement of Marc Rotenberg, President & Exec. Dir. Elec. Privacy Info. Ctr.) (noting that identity theft exacerbates homeland security risk with the central role that identity verification procedures like Secure Flight will play in passenger screening).

71. *See generally* FEDERAL TRADE COMMISSION, FTC CONSUMER ALERT, SPYWARE (July 2005); FEDERAL TRADE COMMISSION, TRAPPED IN THE TANGLED WEB: WEB SCHEME DIVERTS CONSUMERS FROM THEIR INTENDED SITES (Oct. 2001); FEDERAL TRADE COMMISSION, DOT CONS-FACTS FOR CONSUMERS (Oct. 2000); *see also* Alan Stafford, *Privacy in Peril*, P.C. WORLD (Sept. 30, 2005), *available at* http://msn.pcworld.com/news/article/0,aid,122498,00.asp (last visited Nov. 8, 2005) (describing how easily thieves can obtain your information and use it to make thousands of dollars at a victim's expense); OnGuard Online.gov, Phishing (Sept. 2005) (on file with author).

72. Thieves can obtain the first seven digits of a victim's Social Security number from a service called "People Finder" and then combine those digits with the remaining four digits obtained from LexisNexis. Ken Buford, FDIC Investigative Examiner, Address at the University of Mississippi Advanced Cyber Crime Training Conference: Advanced Training on Identity Theft Symposium, *Account Hijacking* (Nov. 2, 2005) [hereinafter Buford Address].

73. *Id.* FTC investigators discovered that Ashley Furniture was discarding reams of old credit applications in their dumpsters. *Id.* Thieves would then drive around to local Ashley Furniture

businesses themselves are being "scammed" by highly organized con-artists.[74]

Thieves typically target the elderly, children, and immigrants.[75] However, no one is free from risk.[76] In fact, Jeff Kurtz with the Social Security Administration, stated that "there is nothing we can do . . . it is epidemic and it will hit most everyone sometime in the future."[77] Kurtz admitted that the current situation stems from the commonplace use of the Social Security Number (SSN) as a means of personal identification. Kurtz explained that the SSN was never intended to be used for anything other than a governmental identification match for Social Security benefits. Sadly, even Kurtz acknowledged that identity theft is at the bottom of their priority list.[78] Unfortunately, even if a person proves they are a victim of identity theft, the Social Security Office will not even flag their account as "compromised."[79] The Social Security Office will only act if fraud is

---

dealers to "dumpster dive" to collect this information. *Id.* According to Buford, Ashley Furniture's negligence made identity theft so easy and efficient that thieves had a filing system on victims organized according to credit score. *Id.*

74. Robert O'Harrow, Jr., *Choice Point Data Cache Became a Powder Keg: Identity Thief's Ability to Get Information Puts Heat on Firm*, WASH. POST, Mar. 5, 2005, at A01 (noting that at least 145,000 people had their identities sold to a con man in the Los Angeles area by one of America's largest information brokers). According to Michael Sivy ChoicePoint lost data on 145,000 customers, LexisNexis lost data on 310,000 Americans, Time Warner lost close to 600,000 citizens' personal information and Bank of America released nearly 1.2 million individuals' files to hackers. Michael Sivy et al., *What No One is Telling You about Identity Theft*, MONEY, July 2005, at 94.

75. Jeff Kurtz, Office of the Inspector General for the Social Security Administration, Address at the University of Mississippi Advanced Cyber Crime Training Conference: Advanced Training on Identity Theft Symposium, *Protections for Social Security Numbers* (Nov. 2, 2005) [hereinafter Kurtz Address].

76. *Id.* Kurtz explained that the elderly and children in particular are prime targets because thieves can exploit their identities for an extended period of time before the victim realizes what is happening. Moreover, these victims often do not have the political or financial means available to them to adequately repair the situation. *Id.*

77. *Id.* This shocking statement fails to provide much hope that the government is taking adequate steps to curb the growing exploitation of identity theft. *Contra* Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 264-68 (2004) (noting that the U.S. Congress has taken steps by expanding the definition of identity theft, granting jurisdiction to prosecute the crimes in federal court and increasing the penalties, however, there is still far to go before Americans will be safe from the crime of the "new millennium.") (citing the Identity Theft & Assumption Deterrence Act of 1998, the Internet False Identification Prevention Act of 2000, the Federal SAFE ID Act and the Federal Fair and Accurate Credit Transactions Act of 2003 which are all codified under 18 U.S.C. § 1028 (2000 & Supp. 2003)).

78. Kurtz Address, *supra* note 75.

79. *Id.*

perpetrated for benefits correlating with a SSN.[80] The apparent ease at which identity theft can occur is not nearly as shocking as the resulting damage.

B. *Effects of Identity Theft on Americans*

The effects of identity theft are both far-reaching and devastating. Last year a "reported" 10 million Americans were victims of identity theft with approximately 160,000 of those being classified as "severe victims."[81] Thieves can obtain new credit cards in the victim's name, divert mail to a different address, run up charges and ultimately leave the victim with the bill. They can open bank accounts in the victim's name, write bad checks or counterfeit checks or authorize electronic transfers in the victim's name.[82] Thieves can file false tax returns to obtain advances or file for bankruptcy under the victim's name, thereby destroying the victim's credit.[83] They can purchase large items like homes, cars or businesses in the victim's names leaving the victim to deal with the balance.[84] Thieves have also been known to sell the victim's identities to illegal immigrants thereby increasing the number of people using the victim's identity.[85] To prolong the scheme thieves may, for a short time, file tax returns and pay bills until the balances get too high or they wish to move onto a new victim's identity.[86]

---

80. *Id.* When Kurtz was asked what could be done, he conceded that his office lacks any power to tell a business to stop using Social Security numbers. Kurtz advised citizens to only give out their Social Security number when absolutely necessary and to question any business's need for it. If the business fails to provide a satisfactory response, citizens should either not shop there or refuse to provide the SSN. *Id.*

81. Bartiromo, *supra* note 57, at A1; *contra* Davis, *supra* note 69 (noting only 9.3 million victims). According to Bartiromo, a "severe victim" is one where criminal(s) actually assume the victim's identity, buys homes, gets a job, and lives as "the victim." The remaining 9.8 million are considered only routine victims, which translates to "minor cases" such as damaged credit or outstanding debt. *Id.* The problem is likely much worse because those statistics reflect only the number of "reported victims" who actually contacted a law enforcement agency. It is highly likely that more victims exist who simply have not learned of the crime or lack the education to ascertain this information or know how to report it. Sivy et al., *supra* note 74 (noting that only 2.6% of Americans fall victim to a burglary while 4.25% fall prey to identity theft). Other victims may be too ashamed or reluctant to report the crime.

82. FTC, FIGHTING BACK, *supra* note 68, at 3.

83. *Id.*

84. *Id.*

85. Richard Hamp, Assistant Attorney General of Utah, Address at the University of Mississippi Advanced Cyber Crime Training Conference: Advanced Training on Identity Theft Symposium, *Investigating and Prosecuting State ID Theft Cases* (Nov. 2, 2005) [hereinafter Hamp Address].

86. *Id.*

As a result of this theft, victims are often left with enormous bills, past due notices, and overdrawn accounts. Victims often do not know they are victims for years. Many victims do not suspect anything until they are finally denied credit. Upon their denial, victims often discover they have a long history of bad credit, except for one important fact; it is not theirs. One victim had his American Express Card declined when trying to rent a tuxedo for his sister's wedding and soon discovered that he had nearly $500,000 of bogus debt attached to his name.[87] The victim, Mr. Fairchild, began dedicating forty hours a week and thousands of dollars to clear up his credit. Upon discovering his damaged credit, Fairchild's legitimate credit accounts, which had never been delinquent, began raising his interest rates and withdrawing credit.[88]

More shocking to Fairchild was the types of services and debts now permanently attached to his "good name."[89] Fairchild was now the *not-so-proud* owner, proprietor and defaulted debt holder of Ebony Passions, an ethnic-metro based escort service based in a city he had never visited. Fairchild explained that he was most upset by the fact that he and his family had "gone without" for so many years because they could not afford expensive things, yet the culprit treated himself to $750 shoes, exotic cars and other lavish expenses.[90]

Nearly two years later, after hundreds of phone calls to creditors, Fairchild still gets an occasional call from a collection agency looking for money and the process starts over again.[91] If these nightmares were not sufficient to create fear and apprehension, thieves also use their victim's identity while committing crimes, thereby providing the victim an undeserved criminal history.[92]

---

87. Zeller, *supra* note 57, at B1.

88. *Id.* Further exacerbating this situation is the emotional battle victims must endure when trying to fix their credit. Timothy O'Brien writes:

> Some victims, after enduring the slow torture of mending their credit histories, say they know exactly whom to blame. "My anger at my perpetrator quickly transferred to the credit-granting community itself . . . They don't care what this does to victims because they don't have to care . . . [it is the] companies that are too loose with consumer and employee information."

Timothy L. O'Brien, *Gone in 60 Seconds*, N.Y. TIMES, Oct. 24, 2004, at 1.

89. O'Brien, *supra* note 88, at 1.

90. Zeller, *supra* note 57, at B1.

91. *Id.*

92. *See generally* United States v. Morgan, 54 Fed. Appx. 421, 422 (6th Cir. 2002); United States v. Karro, 257 F.3d 112, 114 (2d Cir. 2001); Beard v. City of Northglenn, 24 F.3d 110 (10th Cir. 1994); United States v. Montejo, 353 F. Supp. 2d 643 (E.D. Va. 2005); United States v. Morris, 2005 U.S. Dist. LEXIS 418 (Conn. 2005); United States v. Morehouse, 345 F. Supp. 2d 3 (Me.

C. *Ramifications Extend Beyond Simple Damaged Credit*

Imagine for a moment being pulled over for a minor infraction but rather than receiving a small fine, you are arrested, booked, and sent to jail on several outstanding warrants. While protesting the false arrest the police officer explains they are only "following procedure" and it is the prosecutor's job to determine guilt. The police officer's reluctance to release is not surprising considering that nearly all criminals protest their "wrongful arrest."[93] However, what happens when the arrested person *is actually* innocent?[94]

Jack Greene explained that the clash between identity theft and law enforcement leaves many questions unanswered because enforcement agencies often do not share information and police officers have no way to verify a person's identity.[95] One identity theft victim spent fifty-four days in jail even though he repeatedly showed officials a photo of the actual fugitive who stole his identity.[96] More than one victim has been arrested numerous times regardless of the fact that he carries, and has constantly presented, an affidavit from the court proclaiming his innocence.[97] Considering the damage possible, the casual observer would be shocked to learn that there are minimal penalties dealt to criminals who wreak havoc with people's lives.[98]

2004); Johnson v. Scotts Bluff County Sheriff's Dep't, 245 F. Supp. 2d 1056 (Neb. 2003); Neville v. Classic Gardens, 141 F. Supp. 2d 1377 (S.D. Ga. 2001). False criminal histories resulting from identity theft will be addressed later in the Article. *See infra* Part IV.C.

93. *See* Davis, *supra* note 69, at *2. Police officers often call these arrestees "toddi or soddi" for "the/some other dude did it." *Id.* Davis notes that this "phrase captures the 'culture of mistrust around efforts to clear a criminal record.' . . ." *Id.*

94. One identity theft victim realized that the "onus is on you to persuade authorities that you're not the alleged offender and then to fix your record . . . [regardless] your name may remain as a known alias . . . because the oft-arrested imposter [will] continue to give [the victim's] name to law enforcement." *Id.*

95. Robert Perez, *ID Theft Puts Victims in Jams with Law*, ORLANDO SENTINEL, Aug. 15, 2005, at A1 (quoting Jack Greene, Dean of the College of Criminal Justice at Northeastern Univ. of Boston).

96. *Id.* Other victims have been pulled over for speeding and ended up being jailed, strip searched, and detained for days simply because law enforcement agencies would not listen to claims of innocence and identity theft. *Id.*

97. Bartiromo, *supra* note 57, at A1.

98. Mari J. Frank notes that identity theft is a "crime [for] which you can get a lot of money, and have a very low probability of ever getting caught" and minimal penalties if convicted. Zeller, *supra* note 57, at B1. According to Frank, criminals now realize that it is safer to switch to identity theft from traditional crimes. *See id.* After one victim spent five years fixing numerous warrants, lost her job and her home because of identity theft the perpetrator was sentenced to a two month "work furlough" program. Michael Higgins, *Identity Theft is Huge and Growing*, A.B.A. J., Oct.

Victims of identity theft have little recourse against those who perpetrate the crime. While the law provides civil redress, criminals rarely have sufficient funds to cover the amount of damages that might be awarded through a judgment. Moreover, it is highly likely that the thieves are either in prison or have "disappeared" so that victims are precluded from even filing suit.[99] Purists would retort that falsely arrested or detained victims could seek redress through a section 1983 suit against the "wrong doers."[100] This option too lacks appeal because the success rate, even for egregious violations, is dismal.[101]

To make matters even more complicated, identity thieves have contrived several activities to keep police off balance. Identity thieves have learned that if they call the police and claim that the actual victim is stealing their identity, the police will begin investigating the "innocent

---

1998. More shocking to the victim was that the perpetrator showed up to her "work furlough" program still driving the red mustang she bought with the victim's credit. *Id.*

99. Beth Givens noted that police have little incentive to go after identity thieves because the crimes are often extremely complex, typical extend beyond their jurisdiction and "by the time the victim catches on [or the police are notified] the perp is often long gone. Rubin Sabrina, *She Stole My Identity!*, COSMO., Aug. 1, 1999, at *2.

100. Section 1983 suits are civil suits against government bodies, or their agents, for damages resulting from deprivation of rights, privileges, or immunities guaranteed by the U.S. Constitution. 42 U.S.C. § 1983 (1979). Success rates for section 1983 claims are dismal and courts have been extremely reluctant to grant relief at the cost of tying the hands of law enforcement agencies. *See generally* JAMES J. TOMKOVICZ & WELSH S. WHITE, CRIMINAL PROCEDURE: CONSTITUTIONAL CONSTRAINTS UPON INVESTIGATION AND PROOF (4th ed. 2001) (scholars have seriously questioned the effectiveness of 1983 suits as well as tort remedies for civil rights violations).

101. One victim was repeatedly arrested and put in jail even though the office of the prosecutor had information that she was innocent of the crimes. This "knowledge" was found not sufficient to award damages even though the victim spent needless months in jail awaiting release. Neville v. Classic Gardens, 141 F. Supp. 2d 1377, 1378-79 (S.D. Ga. 2001) (victim filed suit against prosecutor because they continuously delayed her release for four to five months at a time even though they had information that she was a identity theft victim). Ultimately, the district court noted that prosecutors exercise formidable and easily abusable power, however, absolute immunity is more important for prosecutors to do their job. *Id.* at 1387. Therefore, the victim's section 1983 suit was dismissed. *Id.* at 1385. The Tenth Circuit also denied a victims redress through section 1983 because the victim failed to prove the prosecutors "knowingly" arrested and detained him. *See* Beard v. City of Northglenn, 24 F.3d 110, 117-18 (10th Cir. 1994). Requiring such a finding nearly precludes the possibility of providing redress unless a prosecutor is absurd enough to admit they knowingly kept an innocent victim in jail. A Nebraska court, when faced with a similar section 1983 suit, found that the "Constitution does not guarantee that *only the guilty* will be arrested." Johnson v. Scotts Bluff County Sheriff's Dep't, 245 F. Supp. 2d. 1056, 1059-60 (Neb. 2003) (citing Baker v. McCollan, 443 U.S. 137 (1979)) (emphasis added). The Nebraska court reasoned that it would be an undue burden on police to require them to determine whether the arrestee was actually guilty of the crime during the arrest and detention. *Id.* The Nebraska court concluded that identity theft victims will likely be unable to use section 1983 for false arrests. *Id.*

person" rather than the *actual perpetrator*.[102] This provides the criminal a chance to move away or escape before they themselves are arrested.[103] Criminals have also legally changed their names to the "victim's name" shortly before trial to confuse the judge and jury.[104] While these activities are occurring, it is not uncommon for the thief to sell or give the false identification to someone else, thereby forcing police to expand their search yet again.[105]

Even if a person learns they have a false criminal record there is little remedy available.[106] This writer has been unable to find one jurisdiction that would fully expunge prior convictions attached to an identity number or name.[107] Police departments and legal jurisdictions maintain that a crime has occurred and it is attached to an identification number, namely a Social Security Number. Prosecutors retort that a person with name X and Social Security Number Y *was* convicted of the crime. They, as prosecutors, can not *now* erase a conviction attached to a SSN because another person with that name or SSN claims they did *not* commit the crime.

Victims undergoing these problems often suffer adverse reactions because of these faux histories even though enforcement agencies recognize and admit they were victims of identity theft. Victims have been fired from their jobs for "lying about their past" or not hired because of the appearance of *having* a felony conviction.[108] Some states provide affidavits

---

102. Todd Lawson, Assistant Attorney General of Arizona, Address at the University of Mississippi Advanced Cyber Crime Training Conference: Advanced Training on Identity Theft Symposium, *Investigating and Prosecuting State ID Theft Cases* (Nov. 2, 2005) [hereinafter Lawson Address].

103. Sabrina, *supra* note 99, at *1.

104. Lawson Address, *supra* note 102. The effect of this treachery is yet another crime placed on the innocent victim's record because the guilty party used the victim's name as theirs for the trial. *Id.*

105. *Id.*; Bob Sullivan, *The Secret List of ID Theft Victims*, MSNBC, Jan. 25, 2005 (noting that identify theft is increasingly used by illegal immigrants).

106. Christopher P. Couch, *Forcing the Choice Between Commerce and Consumers: Application of the FCRA to Identity Theft*, 53 ALA. L. REV. 583 (2002); Pastrikos, *supra* note 57, at 1137-38.

107. Sabrina, *supra* note 99, at *2; *contra* Teresa Anderson, AM. SOC'Y FOR INDUS. SEC. MGMT., Jan. 1, 2005, at 95 (noting that some Colorado courts have "flagged" victims criminal records noting that they "may" reflect fraud); Davis, *supra* note 69, at *3 (noting that a new California law allows identity theft victims to put their name on a "watch list" that police and prosecutors can "pull up" to verify if the name or SSN has been associated with a previous identity theft).

108. Couch, *supra* note 106, at 586. Rubin Sabrina wrote:

> Almost a year and a half [after being falsely arrested] [the victim] is still trying to fix the mess. Her driver's license has been suspended due to her "warrants." Her "criminal" past has kept her from getting jobs. Worst of all, police don't seem

to victims explaining the "mis-leading criminal history" but that is of little consolation considering that prejudices often rear their head in pretext dismissals regardless of the affidavit. It appears that businesses would rather play it safe than hire someone who "might" have a felony conviction.[109]

Destroyed credit, false arrests and humiliation aside, the effects of these false criminal histories can have ramifications beyond those already discussed.[110] Now that the innocent victim has a "criminal record" they can be flagged as "threats," across the United States.[111] This factor is of grave concern with the upcoming implementation of Secure Flight.[112] It is now likely that identity theft victims may be precluded from flying because of false criminal histories.[113]

> interested in helping her correct the situation. Her life has become so impossible that she's considering changing her name. "When this woman gets out of jail, there's nothing to keep her from using my name again."

Sabrina, *supra* note 99, at *1.

109. Businesses and prosecutors alike also question the effectiveness of these affidavits because there is no way to validate the affidavit or ensure that it is not actually a criminal presenting a false document. The uncertainty about an affidavit's validity is the reason why many police officers will not release a person who presents one. The real victims are stuck between the proverbial rock and the hard place because even documents proclaiming their innocence can be forged by criminals and used for illicit purposes. Davis, *supra* note 69.

110. Julia Malone, *Air Flight Database Project Hits Snag; GAO Sides with Critics of TSA's Prescreening*, ATLANTA J., Apr. 29, 2005, at 5C.

111. Even worse is the disheartening fact that identity thieves frequently sell "stolen identities" to crime syndicates around the globe. Sivy et al., *supra* note 74. These syndicates then sell the ID's to local criminals who use them when committing various crimes. *Id.* Thus, American citizens may have criminal histories spanning the globe with no way of knowing until it is too late. *Id.* A more severe problem arises when one of those Americans travels abroad and is arrested because of their "criminal record." An American citizen might spend months or years in a foreign prison before they can reach the American consulate to clear up the confusion. It is difficult to imagine a worse scenario then being arrested in Thailand, Nigeria, or Shri-lanka on vacation; being denied any inalienable rights or privileges of due process; pleading your innocence to a potentially uncaring or corrupt judicial system; becoming a "guest" to the country's prison for the rest of your life; and never understanding how you even got into the situation.

112. Fenton Johnson, *Instead of Security, Chaos & Blanket Excuses*, SUN SENTINEL, Aug. 11, 2005, at 19A.

113. Pam Fessler, *Use of Terrorists Watch Lists at American Airports*, NPR, Apr. 26, 2005 (noting that identity theft is a definite problem with the system but lawmakers have chosen to go ahead because they consider "national safety concerns" more important than the fear of false positives). *See infra* Part V.B.

V. FALSE POSITIVES FROM IDENTITY THEFT EXACERBATE SECURE FLIGHT'S EFFECTIVENESS

A. *What is Next for the American Flyer*

When passengers arrive at airport gates and present their tickets and identification, Secure Flight springs into action by searching vast private databases and government maintained watch lists of suspected terrorists.[114] Sources predict that potential error rates for this process could be as high as thirty percent while others claim the system will have an error rate of *no lower* than two percent.[115] Even TSA has acknowledged that there is a significant potential for high numbers of falsely red-coded passengers and they "ha[ve] no indication of the accuracy of [the] information contained in [the] government databases."[116] This means statistically that between 400 to 1200 innocent people per year, who have committed *no crime*, will be coded red, handcuffed and led away by security for being a suspected terrorist when they reach the airport check-in counter.[117] Not even the program's advocates can reach a consensus about whether the figure of falsely labeled "terrorists" will decrease or *increase* over time.[118]

Current legislative policy in the United States has done little to curb the growing problem of identity theft.[119] This means that Secure Flight's

---

114. *See* U.S. GENERAL ACCOUNTING OFFICE, REPORT TO CONGRESSIONAL COMMITTEES, AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES, GAO-04-385, at 6 (Feb. 2004), *available at* http://www.gao.gov/new.items/d04385.pdf (last visited Nov. 7, 2005) [hereinafter GAO Report].

115. *See, e.g.*, Lane County Bill of Rights Defense Committee, CAPPS II, *available at* http://www.lanerights.org/ capps.htm (last visited Nov. 3, 2005); *contra* Goo, *supra* note 64, at A01 (stating that Secure Flight will likely incorrectly identify two percent of passengers as flight risks); Audrey Hudson, *Airline Profiling System Defended*, WASH. TIMES, Feb. 13, 2004, at A11.

116. GAO Report, *supra* note 114, at 15.

117. Kite, *supra* note 3, at 1421; Goo, *supra* note 64, at A01. These figures are based on a one million person per day average.

118. Kite, *supra* note 3, at 1421; Ann Davis, *Boarding Impasse: Why a 'No Fly List' Aimed at Terrorists Often Delays Others*, WALL ST. J., Apr. 22, 2003, at A1.

119. Pastrikos, *supra* note 57, at 1442 (stating that identity theft results in harms to "the individual's reputation or credit rating, inconvenience, and other difficulties resulting from the offense" (citing Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1432 (2001); Liz Pulliam Weston, *Blame Lenders, Not Thieves for Identity Theft*, CNBC MONEY MATTERS, *at* http://moneycentral.msn.com/content/Banking/ Financial Privacy/P48173.asp?GT1=6239 (stating that because of two fraudulent entries in the LexisNexis and Choicepoint consumer databases, nearly 145,000 people had their identities stolen from that database) (last visited Nov. 17, 2005)). Constant refusal by lenders to work within policy complicates the issue and victims are left without anywhere to turn to fix their problem. *Id.* Lenders refuse to abide by search warrants or requests for information from out of state courts and refuse to speak with police investigating complaints because they make more money by using lax

defects will be compounded by this country's increasing identity crisis.[120] Identity thefts combined with the already excessive error rates projected by experts, strongly suggests significant issues for the public at large.[121]

People living in this country have learned to deal with the ever increasing security which pervades our daily existence. We cope on a day to day basis with the implicit accusations from automated security systems and lurking cameras.[122] In addition to the degradation from cashiers failing to properly deactivate sensor strips at your local retailer,[123] citizens and visitors can now look forward to possibly being falsely labeled a "terrorist" at their local airport by an unseen accuser.[124] Passengers may

---

application procedures. *Id.* Consumer databases, and the lenders who use them, have hardly any oversight and use it to their advantage. *Id.* Recently a subsidiary of LexisNexis had its customer database hacked and over 310,000 people had their social security numbers, drivers licenses, and addresses stolen and the company did not even know it until they happened upon it accidentally. Associated Press, *LexisNexis ID Theft Much Worse Than Thought*, MSNBC NEWS, *at* http://www.msnbc.msn.com/id/7475594/ (stating that Reed Elsevier's database located in Boca Raton, Florida provides data for Matrix) (last visited Nov. 11, 2005). Reed Elsevier's Matrix contract is one of the U.S. anti-terrorism database contracts that is currently used by TSA and will be utilized by Secure Flight. *See id.* Perhaps the theft of over 300,000 identities in a database used by Secure Flight will prompt congressional review because of the great potential for error and abuse in dataveillance.

120. After people have realized that someone else has been using their identity, they have been unable to fix it because States refuse to delete records created by the identity thief. Many of these victims must carry documents for the rest of their lives explaining they are not felons, child molesters, or insolvent. With the current Secure Flight system, this "carry-around documentation" would not alleviate the problem because the government will posit that these documents could easily be forged or presented by actual terrorists. Moreover, while these identity theft victims try to explain their dilemma to the arresting officer, their flight will be leaving with their families or friends on board or even worse causing the entire family to miss their vacation, wedding, or other "once in a lifetime" event. Davis, *supra* note 69, at *3.

121. Kite, *supra* note 3, at 1421; Goo, *supra* note 64, at A01; Davis, *supra* note 118; Hudson, *supra* note 115.

122. *See generally* Jamie James, *Why I Don't Live in America*, AM. SCHOLAR, Autumn 2004, at 109 (author explaining her reasons, one of which was a pervasive feeling of too little trust, for leaving America to live in Indonesia). Pastrikos notes that, "[c]omplications from identity theft may also require embarrassing explanations if employers or law enforcement officials perform a background check on a victim." Pastrikos, *supra* note 57, at 1154.

123. *See, e.g.*, Deseriee A. Kennedy, *Processing Civil Rights Summary Judgment and Consumer Discrimination Claims*, 53 DEPAUL L. REV. 989 (2004); *see generally* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1 (2005); *see* Amanda G. Main, Note, *Racial Profiling in Places of Public Accommodation: Theories of Recovery and Relief*, 39 BRANDEIS L.J. 289, 296 (2001).

124. Once this fear becomes a reality our society moves one step closer to Orwell's government controlled dominance of its citizens. "[Computer] data processing creates a potential for suppressing a capacity for free choice. The more that is known about an individual, the easier it is to force his obedience . . . the state and private organizations can [then] transform themselves into omnipotent parents." Daniel J. Solove, *Privacy and Power: Computer Databases and*

now worry that they might be led away in handcuffs because a computer has misdiagnosed a personal preference, commercial purchase, or entity authentication.

Due to the level of inconvenience and embarrassment that the system might cause, most people would expect an effective oversight system to exist which could mitigate the possible damage that Secure Flight could cause. Considering the risk, it seems quite reasonable that the government would place a high value on "fixing" whatever led the computer to falsely red-code the passenger in the first place. Much to this author's dismay, almost no procedures exist whereby an aggrieved passenger can get help, or for that matter even find out exactly why they were flagged as a potential terrorist in the first place.[125] This security veneer exists, according to the TSA and the Department of Homeland Security, to prevent aggrieved passengers from ever knowing why they were coded "red" for security reasons.[126] To make matters worse, red-coded persons may only bring complaints based on information they obtained from their *own* records[127] thereby making it nearly impossible to effectively contest a Secure Flight assessment.[128]

This means that passengers can only access the information that they provided personally when they bought the tickets. This type of information would include their name, address, telephone number, credit card number, date of birth and any other distinguishing factors.[129] These factors are known as the Passenger Name Record (PNR).[130] At check-in the PNR is automatically cross checked with Secure Flight to determine how the potential flier with be coded. None of the *relevant* or disputable information which flagged the passenger will be disclosed and they will

---

Metaphors for Information Privacy, 53 STAN. L. REV. 1393, 1396 (2001) (alteration in original) (citing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 39 (1996)).

125. It is important to note that once a passenger has been red-coded and denied boarding the damage has been done because they have been denied their liberty interest without due process of law. Dummer, *supra* note 52. TSA fails to address this issue when outlining its redress procedures. *Id.* If a person's liberty or property interest is infringed without due process that, by itself, is a violation of a fundamental right provided by the U.S. Constitution. *Id.* Further discussion of this topic should be undertaken by academics and Congress before Secure Flight, or future permutations of the system, are implemented.

126. Kite, *supra* note 3, at 1424.

127. *Id.* at 1425.

128. According to a GAO Report, "TSA officials stated that passengers will not have access to any government data used to generate a passenger risk score due to the national security concerns." GAO Report, *supra* note 114, at 26.

129. *Id.* at 26; Kite, *supra* note 3, at 1425.

130. Steven Roberts, *Big Brother is Watching*, 26 NAT'L L.J. 62, 63 (2004).

receive no explanation about why they were denied passage.[131] In spite of the paradigm the United States Congress exists within, it is this writer's belief that the modern law still requires that evidence be presented against the accused *before* they can be punished.[132] Secure Flight and TSA apparently have chosen to disregard these requirements as aggrieved passengers are told nothing about why they were flagged "red."

Little could be more discouraging than being detained and escorted away by security, leaving friends and loved ones standing at the terminal gate while being told by security that the only information they can provide to you is your own name, birth date and telephone number.[133] To further exacerbate the situation, the passenger information which "red-coded" you will be kept for only a limited period of time before it is deleted from Secure Flight.[134]

B. *Affecting Victims Beyond Intent*

Considering the precarious nature of dataveillance and the uncertainties discussed above, the implementation of Secure Flight, and future versions based on the same concept, as a pre-screening system for air travel in America, will likely create numerous problems for identity theft victims. Considering the lack of empathy with which Secure Flight and TSA designed their enforcement measures, victims of identity theft will likely suffer great inconveniences because of their destroyed credit, false histories and suspect purchases. Because TSA has admitted the lack of oversight of private data collection agencies and recognized the fallibility of the information kept in those databases, it is not unreasonable to assume that identity theft poses severe concerns for persons wishing to fly. TSA and current watch groups already question the enormous error rates expected to falsely flag innocent flyers as threats, and the situation will likely be made worse by the ten million instances of reported identity thefts each year. Moreover, considering the 160,000 reported instances of

131. GAO Report, *supra* note 114, at 26; Kite, *supra* note 3, at 1426. Although it is possible that a terrorist might declare their true intentions while purchasing their ticket, it is extremely unlikely.

132. *See* Karen Cunningham, *"A Spanish Heart in an English Body": The Ralegh Treason Trial and the Poetics of Proof*, 22 J. MEDIEVAL & RENAISSANCE STUD. 327 (1992); Mark Nicholls, *Sir Walter Ralegh's Treason: A Prosecution Document*, 110 ENG. HIST. REV. 902 (1995).

133. Implicit in this scenario is the issue of false imprisonment and lack of probable cause, however, discussion of this expansive topic is beyond the scope of this Article but should be noted when considering the potential impact of Secure Flight on passengers and their constitutional rights. *See generally* Dummer, *supra* note 52.

134. Press Release, U.S. Dep't of Homeland Security, CAPPS II: Myths and Facts (Feb. 13, 2003), *available at* http://www.dhs.gov/dhspublic/display?content=3163 (last visited Nov. 11, 2005).

"severe identity thefts" within the United States, it is highly likely that at least some of the 160,000 Americans will be denied the ability to fly because of the activities of criminals.

VI. CONCLUSION

Air travel as a means of transportation has lost its luster and is now about as pleasant as a crowded subway ride.[135] Travelers are told to arrive at airports hours ahead of time to allow for long security lines. Then, rather than being welcomed by cheery smiles, flyers are subjected to potential unconstitutional searches and investigations before being allowed to board. Passengers are now confronted with unpleasant experiences for the sake of security and the situation does not seem to be getting better.[136] The financial losses faced by the airline industry suggest that these issues will need to be addressed or else passengers may no longer consider flying a viable mode of travel. These problems, compounded with the ever present threat of having your identity stolen or misused, illustrate that America and its citizens are at an impasse that must be addressed quickly or even more Americans will see their rights being removed with little to no redress available to them.

A non-partisan congressional review board must be developed to bridge the gap between flyers and TSA officials. The board should function as an intermediary between the system's victims and TSA while balancing citizen grievances against national security needs. To accomplish their task the board must have access to all secret procedures and types of data mined so they can better determine what is necessary when viewed against the nation's best interests. Additionally, TSA must modify Secure Flight to address the increasing problem of identity theft. These actions must be taken before Secure Flight is implemented or another injustice may be visited upon the American people.

---

135. *Delays Warning in U.S. Air Security Crackdown: Fingerprints and Photos to be Taken as Anti-Terrorist Rules Tightened*, SCOT. NEWSPAPERS LTD., Sept. 29, 2004 (noting that 33,000 people coming into the United States will be affected every day and this will result in even longer wait times and delays). *See also* Brian Bennett, *Air Safety: Extending the No-Fly Zone*, TIME, Apr. 17, 2005, http://www.time.com/time/magazine/article/0,9171,1050224,00.html (noting that No-Fly lists expansion to 31,000 names may begin to impede over-flight rights closely guarded within international treaties).

136. *See* Lauren Bayne Anderson, *It's Time to Ditch Your Bics at Airport*, ST. PETERSBURG TIMES, Apr. 13, 2005 (recent reports show that airport safety has not improved since 9/11).