

September 20, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office at the Department of Homeland Security,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system - but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is considering a similar arrangement to hand over illegal immigrants to the INS. The question is, what else will CAPPS II be used for? Given the potential for abuse of the

information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my constitutional right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPS II should be withdrawn.

Sincerely,

A handwritten signature in black ink, appearing to read 'Patrick Dillon', written over the word 'Sincerely,'.

Patrick Dillon

FILE

September 29, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

ATTENTION:

Dear Privacy Office at the Department of Homeland Security,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system - but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is

considering a similar arrangement to hand over illegal immigrants to the INS. The question is, what else will CAPPS II be used for? Given the potential for abuse of the information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my constitutional right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPS II should be withdrawn.

Sincerely,

Michael Dominijanni

A handwritten signature in black ink, appearing to read 'Michael Dominijanni', with a long horizontal flourish extending to the right.

CEO of the PA Legal Resource Center

September 28, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system - but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

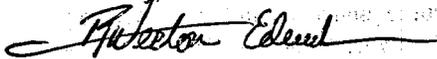
Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is considering a similar arrangement to hand over illegal immigrants to the INS. The question is, what else will CAPPS II be used for? Given the potential for abuse of the information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my constitutional right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPS II should be withdrawn.

Sincerely,



Ryan Edwards



G. Hardy Acree
DIRECTOR OF AIRPORTS

John O'Farrell
ADMINISTRATOR
Community Development &
Neighborhood Assistance Agency

September 26, 2003

Privacy Office
U. S. Department of Homeland Security
Washington, DC 20528

Re: Transportation Security Administration
Docket No. DHS/TSA-2003-1

To Whom It May Concern:

I have reviewed the CAPPs II Privacy Act Federal Register notice and would like to submit the following questions and comments:

1. What measures will TSA put in place to ensure that the commercial data providers do not "permit use of" or "retain" the data for any purpose other than in connection with the CAPPs II program?
2. Will a person become a selectee if there is a change in his/her PNR as compared to what is being stored by TSA? For example, change of address or use of an alternate address.
3. How is this system integrated with the check in kiosks and procedures?
4. How will the list of "crimes" be developed and with whose input? Current SIDA badging procedures do not account for persons whose arrest or conviction records have been expunged, and do not adequately address crimes committed by military personnel processed through the Uniform Code of Military Justice.
5. The proposal states that during the test period that no data will be transmitted to the airport screeners. This implies that after the test period data will go to the screeners. Why is the data going to the screeners? How will they get that information? Since it will require some form of

SACRAMENTO INTERNATIONAL
PHONE: (916) 929-5411
FAX: (916) 874-0636

EXECUTIVE
PHONE: (916) 875-9035
FAX: (916) 428-2173

MATHER
PHONE: (916) 875-7077
FAX: (916) 875-7078

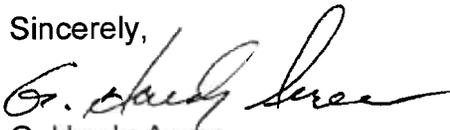
FRANKLIN FIELD
PHONE: (916) 875-9035
FAX: (916) 428-2173

equipment to receive this information, where is this system going to go? How large is this system? Who will have access to it? Who will control it? What will be the penalties for misuse?

6. There is concern with the direction that TSA will not retain "significant" amounts of personnel information. This still allows TSA the flexibility to keep "significant" amounts of personnel information on select individuals without retaining a significant amount of personnel information overall.
7. What contingency plans will be activated when the system becomes non operational?
8. Will random selectees be generated from the passenger lists? If so, what protection is extended to those individuals since they will be viewed as potential terrorists or criminals by other passengers?
9. Arrests are not "guilty verdicts" in this country. No actions should be predicated on arrests. Further, what provisions are being made to purge the data when convictions are vacated by the court or a record is expunged. What ability will a citizen have to review and correct errors in their files?
10. What process is used to determine who is qualified to be designated as a commercial data provider?

If you have questions or require additional information please contact me at (916) 874-0600.

Sincerely,



G. Hardy Acree
Director of Airports
Sacramento County Airport System

Cc: Frances Sherertz, Assistant Director, Operations and Maintenance
Ann LeBlanc, Airport Security Coordinator
Dawn Lucini, Regulatory Affairs

September 28, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system - but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is considering a similar arrangement to hand over illegal immigrants to the INS. The question is, what else will CAPPS II be used for? Given the potential for abuse of the information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my constitutional right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPs II should be withdrawn.

Sincerely,


Charlie Gorichanaz



AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

535 HERNDON PARKWAY □ P.O. BOX 1169 □ HERNDON, VIRGINIA 20172-1169 □ 703-689-2270
888-FLY-ALPA (888-359-2572) □ FAX 703-689-4370

September 30, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, D.C. 20528

Re: Docket Number DHS/TSA-2003-1, Privacy Act of 1974: System of Records

Dear Sir/Madam:

The Air Line Pilots Association (ALPA), which represents 66,000 pilots who fly for 42 airlines in the U.S. and Canada, has reviewed the referenced notice published in the August 1, 2003, Federal Register and offers the following comments.

ALPA staunchly supports all reasonable measures that can be taken to prevent the boarding of persons with criminal intent onto airliners. While it is not possible to accurately predict which passengers of the hundreds of millions boarded each year may intend to engage in criminal misconduct, there are ways to assess passengers' previous actions and historical data as a predictive tool in this regard.

ALPA representatives were involved in and supported the development of the first-generation Computer-Assisted Passenger Prescreening System (CAPPS), which relied on individual airline-collected data. That system had obvious limitations, such as the lack of shared information with other airlines and no capability for searching government data. However, its purpose was to identify those individuals who could be deemed trustworthy, based on information available to the airlines, in order to enable greater allocation of security resources to those individuals about whom less was known or whose background information raised legitimate questions.

Accordingly, ALPA supports the concept of CAPPS II, as it is intended to enhance the earlier version of the system by increasing the amount and variety of data that is examined for each individual. While we wholeheartedly endorse physical security checkpoint screening of passengers, we believe that such screening should be combined with an assessment of risk for each passenger. El Al Airlines has been held up as a model for airline security – it should be noted that this carrier relies heavily on assessing passenger risk through interviews and collecting information on individuals as a means of determining intent. These assessments are performed prior to and during physical screening, and the results are used as a factor in determining how a passenger is processed. ALPA encourages the TSA to develop a cadre of trained interviewers who will be stationed at screening checkpoints to assess the risk of those individuals about whom little is known or whose backgrounds give rise for concern.

CAPPS II will provide some significant benefits to aviation security, which include the following:

- It reduces government intrusion for the vast majority of passengers. Most commercial airline passengers are upstanding citizens who pose no threat to aviation. However, in this country,

each and every passenger is viewed and treated at the screening checkpoint as though they pose a threat. One outcome of this generalization is that security screeners must make very intrusive physical checks of all individuals, including the very aged, the infirmed and the very young, not to mention U.S. Senators and Congressmen. In response to this intrusiveness and inconvenience, many airline passengers are reducing their airline travel frequency and/or finding other ways to travel.

It focuses our finite security resources on those passengers whose background presents an elevated, uncertain, or unknown risk. By treating all passengers as though they pose the same level of risk, the natural outcome is to actually reduce the amount of scrutiny to a level that can sustain moving all passengers through the checkpoint at an acceptable rate. The result is excessive scrutiny on those who pose little or no risk and too little scrutiny on those who pose an elevated, uncertain or unknown risk.

It identifies individuals who are wanted by law enforcement authorities. CAPPS II will be capable of positively identifying criminals who are sought by law enforcement authorities. This capability will act as a deterrent to air travel by such individuals and help authorities locate and arrest these criminals.

It addresses the fact that terrorists do not need to bring weapons with them through the security-screening checkpoint to pose a threat to airline security. Trained terrorists do not need easily detected metal weapons to take over an aircraft. Determining a passenger's intent, or better yet, identifying a known terrorist, prior to boarding is the "ounce of prevention" that airline security needs.

Lastly, ALPA objects to the weakening of the August 1, 2003, CAPPS II proposal as compared to the January 15 version. As modified, the passenger's place of birth will not be identified nor used in the prescreening process, which is a key component of determining identity. TSA also proposes to eliminate its previous use of financial and transactional data and information from law enforcement and intelligence sources. These data sources should be used for passenger prescreening, if the system is to function effectively and efficiently. We recommend that the TSA reinstate the use of such valuable data in CAPPS II.

ALPA appreciates the opportunity to comment on this important initiative.

Sincerely,


Captain Stephen Luckey, Chairman
National Security Committee



AMERICANS FOR TAX REFORM

Grover G. Norquist

President

September 30, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Re: Computer-Assisted Passenger Pre-Screening System 2.

To Whom It May Concern:

The USA Transportation Security Administration (TSA), has prepared a new version of the Computer-Assisted Passenger Pre-Screening System also know as CAPPS II.

Americans for Tax Reform (ATR) submits the following comments in opposition to the USA Transportation Security Administration new Computer-Assisted Passenger Pre-Screening System. ATR is a non-partisan coalition of taxpayers and taxpayer groups who oppose all federal and state tax increases.

ATR is concerned with the proposed new CAPPS II program for several reasons. CAPPS-II is the USA government's name for a new system that will be used to identify, profile, and monitor airline travelers. The ultimate goal is the creation and enforcement of a "no-fly list" and other "watch lists" for airline passengers. The CAPPS-II will first be applied to airline passengers on flights to, from, or within the USA, and eventually will be expanded to include other modes of transportation such as trains and busses.

The USA Transportation Security Administration has published two Privacy Act notices describing what CAPPS-II would do. The first version, "CAPPS 2.0", was published in the Federal Register on 15 January 2003. The negative response to the proposed new system was tremendous. Critical comments from members of the public, privacy and consumer advocates, legislators and law enforcement officials, and other individuals and organizations forced the TSA to reexamine the program and revise its original proposal.

CAPPS 2.1 was first outlined in a TSA privacy advocates briefing in March, repeated in subsequent TSA press statements and testimony to Congress, and finally published in the Federal Register on 1 August 2003. Below are several concerns that must be addressed by the TSA before the implementation of the new CAPPS 2.1 program.

The revised program creates a new, unconstitutional requirement for a domestic passport. **This creates a de facto national ID card system by requiring all travelers to carry and display, on**

request, government-issued identity documents. The public, and Congress have routinely opposed the idea of any type of national ID for years.

One of the ways that CAPPs 2.1 is significantly worse than CAPPs 2.0 is that it requires air travelers to provide additional information, including the date of birth, home phone number, and home address of each traveler to the airline, travel agent, or travel arranger. (CAPPs 2.0 would have relied on information already entered in reservations.) In addition, the program requires the collected information to be entered into a computerized reservation system (CRS).

Because none of the information is currently required or collected, and airlines and CRS's don't even have fields in their databases to record it, CAPPs 2.1 would require hundreds of millions of taxpayers' dollars to modify the data storage. Therefore, implementing this outlandish mandate will place an unneeded financial burden onto either consumers or taxpayers.

Additionally, the program enlists travel agents, airline employees, corporate travel managers, and other individuals as surveillance agents, collecting and recording information to be forwarded on to the federal government.

As I stated above, the CAPPs 2.1 requires travelers to provide additional information, which would be recorded in their reservations, passed on to the government, and retained by travel companies. While the TSA claims that it will purge the data on most travelers after their flights, there are no specific requirements that they do so. Moreover, because there is no federal law protecting general data privacy law, and since neither CAPPs 2.1 nor any other federal law or regulation restricts using travel data by private companies, travel companies may retain this additional information and use it, rent it, or sell it without travelers' knowledge or permission.

This worse case scenario where a travel company uses a travelers' personal information for profit, constitutes an improper and unconstitutional theft of personal informational property without compensation.

Until the TSA can address these concerns and provides the necessary safe guards for personal information, ATR will oppose any efforts to implement any type of Computer-Assisted Passenger Pre-Screening System.

Sincerely;



Grover G. Norquist
President

September 21, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

The current proposed rules enable the Transportation Security Administration to gather personal information about me from both government and commercial databases. I believe this to be an unquestionable violation of my personal privacy. Furthermore, the TSA is going to be using this information to rank my so-called threat level, ultimately deciding if I am allowed to board the flight or not. I am concerned that the quality and accuracy of the information contained in these databases is highly dubious.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem I see with the TSA acquiring their information from these databases is the possibility of computer trespass and identity theft. Much of this information may have considerable market value; and hence be a very appealing target to criminal intruders. I have seen virtually no assurances from the TSA that the information retrieved is going to be secure and un-comprisable.

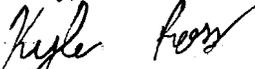
And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is considering a similar arrangement to hand over illegal immigrants to the INS. The question is, what else will CAPPS II be used for? Given the potential for abuse of the information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel is basic to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

For these reasons and others, the proposed rules regarding CAPPS II should be withdrawn.

Sincerely,


Kyle Ross

Henry Grady Beard

September 26, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office at the Department of Homeland Security,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's August 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system – but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is considering a similar arrangement to hand over illegal immigrants to the INS. So what else will CAPPS II be used for?

Given the potential for abuse of the information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel, first enunciated in the Magna Carta, is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPS II *should be withdrawn*.

Sincerely,

A handwritten signature in cursive script that reads "Henry G. Beard". The signature is written in dark ink and is positioned above the printed name.

Henry G. Beard

September 22, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be withdrawn.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system - but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

Finally, CAPPS II is already exhibiting "mission creep." The proposed rules expand CAPPS II beyond its originally stated purpose of identifying possible terrorists. For instance, TSA plans to share information gathered by CAPPS II about those who have outstanding arrest warrants for violent crimes with law enforcement, and is considering a similar arrangement to hand over illegal immigrants to the INS. The question is, what else will CAPPS II be used for? Given the potential for abuse of the information that is collected, this may be the most important question that we ask about CAPPS II.

The right to travel is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my constitutional right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPS II should be withdrawn.

Sincerely,

A handwritten signature in black ink, appearing to read "John Harrold". The signature is written in a cursive style with a large, stylized initial "J".

John Harrold

4



VIA FIRST-CLASS MAIL & E-MAIL DELIVERY

September 30, 2003

Privacy Office
U.S. Dept. of Homeland Security
Washington, DC 20528

Re: Docket No. DHS/TSA-2003-1

Dear Sir or Madam:

On behalf of People For the American Way (PFAW) and its more than 600,000 members and supporters, I write in response to the request for comments on the proposed records system titled "the Passenger and Aviation Security Screening Records," Docket No. DHS/TSA-2003-1, established to support the Computer Assisted Passenger Prescreening System known as "CAPPS II."

While CAPPS II was conceived with the worthwhile goal of "minimiz[ing] threats to passenger and aviation security," the two-pronged records system of authentication and risk assessment is seriously flawed, does little to ensure greater safety in American air travel and threatens to subvert fundamental civil liberties and civil rights. As explained further below, we urge you to halt implementation of the proposed system on either a trial or permanent basis and begin the process of identifying other more effective ways of increasing aviation security without undermining privacy and other freedoms.

In seeking to verify the identity of each and every airline passenger, CAPPS II's authentication prong offends individual privacy by the collection and possible improper use and sharing of personal information. The collection of each passenger's name, birth date, address, telephone number and travel itinerary cross-checked with information obtained from government and public databases, even without the use of credit reports and medical records, is essentially the creation of a personal dossier on each and every U.S. air passenger. Although the TSA claims that the dossiers will be destroyed at an unknown fixed number of days after the passenger's flight, there is no mention of who will have access to them before they are destroyed, when they will be shared with other federal agencies or private companies, for how long and for what purposes.¹

Moreover, most of the information compiled in the dossiers, also known as "Passenger Name Records" ("PNR"), will be forever inaccessible to the passengers themselves, though all of the information will be accessible to "contractors, grantees, experts, or consultants" working on the CAPPS II program. In particular, the PNRs will

DHS/TSA 010, Routine Uses 1-6; Retention and Disposal.

be transmitted to commercial data providers who will use the information to generate an authentication score that translates to a certain level of confidence in the passenger's identity.² While these entities are not authorized to use or permanently retain the data for any purpose other than in connection with the CAPPs II program, there simply is no way to guarantee that the compiled information will not be improperly or mistakenly misused and disseminated, resulting in unwarranted intrusions of privacy.

This is precisely what occurred in a Department of Defense military security project that similarly involved the compilation of passenger information for risk assessment. As recently reported, JetBlue Airways released information about 5 million passengers (including names, addresses, telephone numbers and travel itineraries) to a technology company, which was operating as a Defense Department subcontractor on a non-airline security project aimed at enhancing security on military bases, ostensibly for use in demonstrating the predictability of the company's algorithms.³ Similar to the proposed system in CAPPs II, the technology company reportedly used JetBlue's passenger information, cross-referenced it with information purchased from commercial databases to perform a risk assessment of the airline's passengers and released the results in a report that, incredibly, was distributed at a technology conference and accessible online. After numerous complaints from the airline's passengers about the public release of certain personal information, the CEO of JetBlue publicly apologized, calling the airline's actions a "mistake."⁴

Significantly, the airline claimed that the subcontracted technology company also used the passenger information in ways that were not authorized by JetBlue or, presumably, the Defense Department. According to a report prepared by the company for a Department of Homeland Security symposium in February 2003, the technology company combined the identifying passenger information with information purchased from other commercial databases in order to obtain passenger Social Security numbers, travel histories and household incomes, again without the knowledge or consent of the individual passengers. This is exactly the type of impermissible invasion of privacy that could well occur as a result of the authentication process in CAPPs II, and the DHS should accordingly halt implementation of the system in its current form.

In addition, CAPPs II's risk assessment process, which ultimately assigns each passenger a security score (green- passenger can freely board, yellow - passenger needs additional screening at checkpoint, red - detention and law enforcement notified), offends the Due Process Clause in that it is prone to inaccuracies that can lead to unlawful deprivations of constitutional protections.

Instead of being narrowly directed, the proposed "risk assessment" process extends beyond air safety by, for example, barring air travel to passengers who are

² DHS/TSA-2003-1, "Notice of Status of System of Records," Sources of Information Contained in the CAPPs II System; Process Flow.

³ "Responding to Privacy Concerns, JetBlue Emails an Explanation," Susan Carey and Stephen Power, *Wall Street Journal*, Sept. 22, 2003.

⁴ *Id.*

believed to have outstanding local or federal arrest warrants. To accomplish this task, the process will rely on existing law enforcement and government databases, some of which are of questionable reliability. For example, the FBI's National Criminal Information Center ("NCIC"), the federal database used by law enforcement all over the country, has been the subject of numerous complaints about wrong information. Indeed, in March 2003, the Justice Department lifted a requirement that the FBI ensure the accuracy and timeliness of the information in the database for that very reason.⁵

Reliance upon such factors will certainly lead to false positives and system errors. Some "red" passengers may be wrongly prevented from flying and unlawfully arrested not because of any connection to terrorism or other criminal activity but because of an outdated police database or because they have the same name as known fugitives. In Florida, one man has reportedly been detained and handcuffed by customs officials in airports repeatedly between 1996 and 2003 because he shared the same name as a fugitive listed on the NCIC and the Treasury Enforcement Communications System. Despite a letter from the U.S. Customs Office written in 1996 stating that he is not the suspect of record in the databases, which he was directed to carry with him at all times, he continues to be stopped and interrogated at airports on a routine basis.⁶

Other passengers who simply have bad credit or no credit and are relocating to another state may be falsely categorized as "of undetermined risk," given a "yellow" code, interrogated or worse. Meanwhile, nothing in the proposed system addresses or prevents the very real possibility that a terrorist may be able to escape detection through identity theft, be mistakenly coded as "green," waved through security and have an easier time boarding a plane under the new system than under the present one. Even putting aside the constitutional violations that will occur, the consequences of error are simply too dire to allow testing and implementation of the system to go forward.

Finally, because of the sheer number of people that the PASSR system will affect, it is potentially one of the most pervasive – and overwhelming - threats to fundamental civil rights and civil liberties in this country's history. An estimated 2 million people travel to, from, or within the United States each day and 730 million do so annually. The Transportation Security Administration ("TSA") expects that up to 90% of domestic travelers will be assigned a green code and allowed to freely board, while up to 8% will be coded yellow and 1-2% coded red. According to the TSA's estimates, this means that each day approximately 160,000 passengers will be delayed and interrogated while 20,000 to 40,000 people will be detained while law enforcement is notified. Even assuming an accuracy rate of 99.9 %, under the proposed CAPPS II, 2,000 innocent passengers per day and 730,000 annually could be wrongly delayed or unlawfully arrested.

The dire consequences and the public outcry that will inevitably result is demonstrated by the constitutional violations occurring as a result of the administration's

⁵ "Limits lifted on fugitive, terrorist data in FBI criminal database," Tom Bridis, *Associated Press*, March 24, 2003.

⁶ "Sharing a name produces hassles," Elinor J. Brecher, *Knight Ridder Newspapers*, August 17, 2003.

war on terrorism and the public's reaction to them. As has been widely reported, Attorney General John Ashcroft embarked on the mass detention of hundreds of people in the weeks and months following the September 11 attacks with the similar goal of identifying and thwarting persons with ties to terrorists or terrorist organizations. In that effort, an estimated 1,400 people since the 9/11 attacks have been arrested and detained.

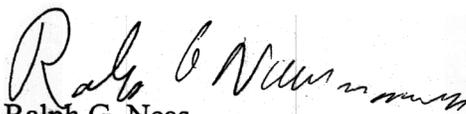
The attorney general set in place a classification and clearance process wherein detainees were designated by the FBI as "high interest," "of interest," or "of undetermined interest," comparable to the proposed records system's risk assessment prong. In a stunning indictment of the attorney general, the Justice Department's Inspector General issued a report in April 2003 finding that the classification process was seriously flawed and randomly applied, resulting in the detention of hundreds of people for months on end in maximum security federal prisons who had no connection to terrorism.

In response, the attorney general has been assailed by Congress, the media and the American people for the countless constitutional violations and deprivations of due process that have occurred in his prolonged detention of innocent people. So far, over 173 cities, towns, and counties and three state legislatures have passed resolutions condemning certain anti-terrorism tactics of the government that have the potential to undermine constitutional protections.⁷ In its present form, CAPPS II threatens to do the same but on a much larger scale.

As America passes the second anniversary of the terrorist attacks that brought vast changes in our idea of national security, it is important to address the dangers that face us now and in the years ahead. Our nation must utilize all the tools at its disposal to fight terrorism, but in doing so, it must be equally vigilant in protecting the promise of freedom for our citizens and visitors. The compilation of largely classified and unreliable information for use in assigning secret security scores that can result in the interrogation or formal arrest of innocent people, does nothing to advance aviation security and runs counter to the values and the rights afforded by the Constitution, which are central to the American way of life.

For these reasons, CAPPS II should not go forward in its present form.

Very truly yours,



Ralph G. Neas

President

People for the American Way

RGN/dl

⁷ Bill of Rights Defense Committee website, 9/23/03.



BOB BARR

Member of Congress, 1995 – 2003

September 30, 2003

Privacy Officer
Department of Homeland Security
Washington, DC 20518

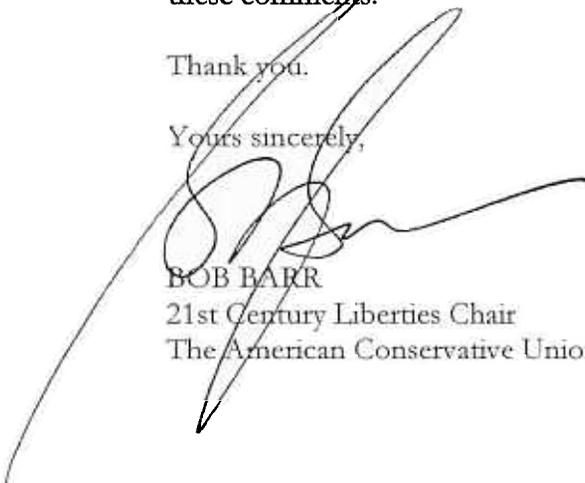
IN RE: Comments Regarding CAPPs II Proposal, Docket No. DHS/TSA-2003-1

Dear Sir or Madam:

Enclosed are two originals of comments I am hereby submitting to the Department's proposed CAPPs II, pursuant to previous notice published in the *Federal Register*, Docket Number DHS/TSA-2003-1. Concurrently herewith, I am submitting the comments by fax (202/772-9738) and by e-mail (privacy@dhs.gov), and am enclosing a self-addressed postcard in order to receive confirmation the Department received these comments.

Thank you.

Yours sincerely,



BOB BARR
21st Century Liberties Chair
The American Conservative Union

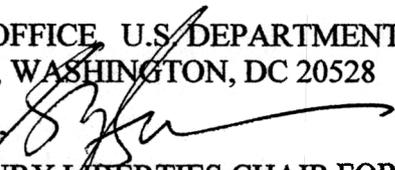


OFFICE OF BOB BARR

MEMBER OF CONGRESS, 1995-2003

MEMO

TO PRIVACY OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC 20528

FROM BOB BARR, 
21ST CENTURY LIBERTIES CHAIR FOR PRIVACY AND FREEDOM, THE AMERICAN CONSERVATIVE UNION

SUBJECT COMMENTS ON PROPOSED CAPPS II AIRLINE PROFILING SYSTEM, PUBLISHED AUGUST 1, 2003, 68 FED REG. 45,265, DOCKET NUMBER DHS/TSA-2003-1

DATE SEPTEMBER 30, 2003

The latest version of the Computer Assisted Passenger Prescreening System (CAPPS II), published by the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) in the Federal Register on August 1, 2003 (68 Fed. Reg. 45,265), Docket Number DHS/TSA-2003-1, is a bad idea whose time hopefully will never come. As proposed, it not only constitutes a highly-intrusive and unconstitutional evidence-gathering system on law-abiding citizens, but it is neither an effective nor cost-efficient way to identify terrorists attempting to use the airlines to carry out terrorist acts. It should be scrapped.

Fourth Amendment Problems

An appropriate starting point for analysis of the proposed CAPPS II system, is, and ought to be, the Constitution of the United States of America, and, specifically, of the Fourth Amendment thereto which, more than any other, defines the relationship of the People to the government.

The Fourth Amendment, which speaks in terms of “probable cause” as the prerequisite for government to search and gather evidence on individuals, and of protecting We the People against “unreasonable searches and seizures,” essentially defines the notion of *privacy*: government cannot gather evidence against individuals absent reasonable basis for believing the person probably committed a crime.

Prior to recent law and government programs such as the proposed CAPPs II, the Fourth Amendment stood as a bulwark against the government gathering, compiling and using evidence against individuals, *absent a good and articulable reason to believe the individuals had violated the law*. CAPPs II as proposed to be implemented by the DHS and TSA, essentially throws this vital and principled protection out the window.

If this system of compiling, analyzing and utilizing this “system of records” – that is, *evidence* – is implemented, then our nation will have adopted the unconstitutional premise that the government can gather evidence, to be used in any number of ways, including against the individuals on whom the evidence is collected, with no basis in fact to believe that such persons have committed a crime. The only basis for the gathering of such evidence would be that the individuals chose to seek to travel commercially by air.

The individual traveler would have no way of ever knowing what evidence is being or has been collected on them; whether it is accurate; how it is used; how it is disseminated; or how to correct it. In short, any person who seeks to travel by air (one of some 2.5 *million* air travelers per day who so travel within the United States, or into or out of our country), is treated as a criminal in that the government gathers evidence on them and can use it *against* that person.

Fourteenth Amendment Problems

The proposed CAPPs II system is fraught with constitutional infirmities, over and above the above-cited fundamental, Fourth Amendment defect. As configured in the proposal, it raises serious equal protection concerns (XIV Amend., U.S. Const.), in that, for example, while most persons who seek to travel by air, would be subject to the CAPPs II system of evidence-gathering and -analysis, some, “preferred” persons such as government bureaucrats, would not be. Further equal protection arguments would be raised by the system’s application only to certain categories of travelers and not others. (Of course, the government’s solution would likely be to *expand* CAPPs II to *all* forms of travel, not just travel by commercial air carrier.)

Due process concerns (XIV Amend., U.S. Const.) abound in the CAPPs II proposal. Arbitrarily taking away a person’s ability to travel by air would, in virtually every instance, subject that person to loss of liberty, frequently to loss of property, and in some cases, even to loss of life; all in violation of the Fourteenth Amendment (*id.*). The simple and inescapable fact is that the system affords no *process*, much less *due process*, whereby the aggrieved person could have recourse against being denied the right to travel or charges being lodged against him or her initially.

What would be contained in the “black box,” the database against which all air travelers would be subject to electronic review? Who knows? This is not a rhetorical question. Certainly the individual traveler would have no way of knowing. Even TSA, the federal agency tasked with administering the system, would not know! Due process and equal protection arguments aside for a moment, such a system would be grossly unfair.

Federalism Problems

Federalism concerns are raised, in the sense that, as proposed, CAPPs II would include in its database, state and possibly local warrants. How this aspect of the system would work in practice is unclear – would the ticket agent be deputized to arrest or detain a traveler against whom the CAPPs II “black box” triggers a red flag because of a supposedly outstanding state warrant? Regardless of how this power would be carried out, it is decidedly *not* the job of private business persons – airline ticket agents, travel agents, or whoever – to be arresting or detaining air travelers because some federal computer system says a person has an old state warrant against them. Moreover, a person whose only “crime” is seeking an airline ticket, should not be subject to scrutiny and detention for a non-federal warrant, by or on behalf of federal authorities.

Second Amendment Concerns

Moreover, and of additional fundamental importance in considering what would be contained in the “black box,” is the distinct possibility -- hollow assurances by various government officials to the contrary notwithstanding -- that impermissible information would be contained in the “black box,” simply because some bureaucrat or agency of the government decided such information might be “useful” in developing a “profile” of a possible terrorist. Information regarding a person’s tax history, or firearms purchases, for example, comes readily to mind. Such information has proved in the past to be irresistible to some federal agencies which, despite legal prohibitions to the contrary, have compiled information on such purchases. That the Second Amendment is potentially subject to infringement by the CAPPs II system, is a very real and reasonable concern (II Amend., U.S. Const.).

Overly Broad and Ambiguous Terms

One of the premises on which the CAPPs II would rest, would be links to “foreign and domestic terrorist organizations.” However, like so many other terms employed in the CAPPs II proposal, such terms are not defined. Furthermore, the broad and vague definitions of such terms in other federal laws and programs, such as the USA PATRIOT Act, leave one with no sense of assurance that such terms would not be applied or defined far more broadly than historic concepts of due process and equal protection allowed.

Operative terms in the very language of the CAPPs II proposal – such as “significant amounts of personal information,” “records of travel,” “persistent link,” “appropriate action,” “additional information,” “pertinent to the detection of terrorists,” “detection of serious criminal violations,” “individual health records,” and others – create open-ended avenues for government abuse.

Dissemination of Data Problems

The virtually unlimited number of persons and agencies, including *international or foreign agencies*, to which evidence and other data compiled and used by CAPPs II pursuant to the authorities outlined in the proposal could be disseminated, is alarming in the extreme for every member of the traveling public, whether U.S. citizen or not.

If a person happens to be involved in litigation, evidence compiled by CAPPs II can be used against them in litigation! In other words, nothing is sacred; everything the government compiles pursuant to CAPPs II is fair game to be distributed and used by other federal, state, local, foreign and international agencies.

Error Rates and Corrections

In addition to the constitutional and legal problems – many glaring and others more subtle – contained within the parameters of the CAPPs II proposal, there are very real and serious *practical* problems. Error rates, for example, or redress of errors.

Experts have established that error rates in large, commercial databases, can frequently approach and even exceed 25% to 30%. Even if one assumes an unrealistically much lower error rate by the government in administering CAPPs II, given the fact some 2.5 million passengers would be subject to its intrusions each and every day, one does not have to be a rocket scientist to conclude that tens – and more realistically, hundreds – of thousands of errors would occur each day. Each one of those errors is not a theory; it will be a *real* person.

Oh, by the way, the CAPPs II proposal contains a method for a person against who information has erroneously prevented them from traveling (or worse, perhaps, subjecting them to arrest), to seek redress: they can . . . write a letter to the CAPPs II “Passenger Advocate” with a further appeal to a . . . “DHS Privacy Office.” This is a laughable fig leaf. Anyone who has studied problems encountered by individuals against who the government has compiled erroneous evidence or information, or reached an erroneous conclusion, knows this proposed mechanism is not even a serious stab at a meaningful correction mechanism.

The bottom line is, the proposed CAPPs II system contains no meaningful way for the aggrieved person to correct the record contained in the system's "black box."

Ineffective Method of Identifying Terrorists

All this might be justified by some – not by this writer – if in fact the CAPPs II system as proposed, constituted a system that realistically would identify true terrorists. In fact, it won't.

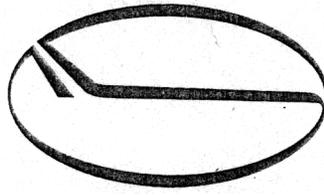
The question is very well to be asked, "what is the value in compiling vast quantities of data on law-abiding citizens and other individuals, in an effort to identify terrorists who, by the very nature of their acts, go to great lengths to *avoid* being profiled?" (A pre-9/11 study in 2001 by the government, asked this very question, and reportedly concluded the answer was that such profiling exercises would *not* yield identities or profiles of terrorists.)

Would not the huge sums of money, expenditure of energy, and growth of government that will necessarily be occasioned by the development and implementation of CAPPs II, be better spent on improving our nation's intelligence gathering, compilation, analysis, coordination and dissemination, via terrorist and terrorist-associates watch lists? Against which sensibly and reasonably, the names of travelers could be matched, without violating fundamental constitutional principles and dramatically changing – for the worse – the relationship of trust that has heretofore existed between Americans and government officials and those acting on their behalf?

Would it not make more sense to arm airline pilots (a process mandated by law but which the Administration has apparently deliberately slowed)? Better enforce immigration laws? And laws and procedures designed to prevent illegal aliens from obtaining and using false identification? Or from obtaining access to prohibited areas, such as airports, planes, and flight schools?

Conclusion

Apparently, and unfortunately, the government has concluded it's easier to profile and gather evidence on law-abiding citizens and other persons. CAPPs II is far from the best way to solve the problem of terrorist acts. In fact, it's a terrible approach. It should be abandoned before it takes further hold, and the resources put into other, constitutional programs that will have a much higher likelihood of ultimate success.



Air Transport Association

James L. Casey
Vice President & Deputy General Counsel

October 1, 2003

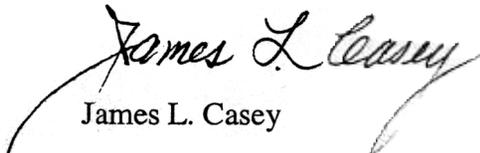
Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Re: Docket No. DHS/TSA-2003-1

Dear Sir or Madam:

Enclosed are the comments that the Air Transport Association of America electronically submitted yesterday to the Department responding to the Transportation Security Administration's request for comments about its interim final Privacy Act notice concerning the Passenger and Aviation Security Records system, Docket DHS/TSA-2003-1.

Sincerely,


James L. Casey

air transportation and to authenticate their identity. TSA will apply CAPPs II to both domestic and international flights. *Id.* at 45266.

The airline industry has repeatedly expressed support for the development of measures that will improve the ability of TSA to evaluate from a security standpoint those who present themselves for transportation on air carrier aircraft. All concerned want this to occur with appropriate protection of the privacy interests of airline customers. More particularly, airline customers are expressing increasing interest in privacy protection issues. Public comments about TSA's January CAPPs II Privacy Act notice are but one indication of that heightened attention. 68 Fed. Reg. 2002 (Jan. 15, 2003). These consumer concerns must be responded to. Consequently, development of responsive data protection policies is essential for the successful introduction of CAPPs II.

Public acceptance of CAPPs II will depend in large measure on the government generating public confidence, both in the United States and overseas, about the adequacy of the System's personal data protection practices. Public acceptance will also depend on avoiding CAPPs II-related delays during the reservation and airport check-in processes. Achieving both of these objectives is imperative. If customers are not confident about personal data privacy or they experience long waits at airports as they provide CAPPs II mandated information, the very real risk is that a substantial segment of the traveling public will forgo air transportation.

Passengers must be confident about the propriety of the government's access to, handling of and disposition of personal information that will be used in

evaluating them. Public comments reacting to TSA's January 15th Privacy Act notice emphasized this point. See Department of Transportation Docket OST-1996-1347, *accessible at* <http://dms.dot.gov>. TSA has responded to those comments by clarifying its intentions about CAPPS II and modifying several of the System's routine uses. See 68 Fed. Reg. 45267-68.

Even with these modifications, airline customers will still sacrifice an appreciable amount of privacy if they are to use air transportation. If passengers are not comfortable with the government's application of CAPPS II, public acceptance of the System could be imperiled. Were that to occur, air travel would suffer because passengers would regard the privacy demands of CAPPS II as personally too costly to justify traveling by air. Thus, the government's provision of personal data privacy protections for CAPPS II should be thorough and its explanation of those measures should be clear.

Airline customers must be comfortable that the surrender of some elements of their privacy is efficacious. This means that customers need to view CAPPS II as useful and conclude that their relinquishment of some aspects of their privacy will make civil air transportation appreciably more secure. As CAPPS II advances in its development, these matters can be more thoroughly addressed in the next Privacy Act notice that TSA anticipates issuing. See *generally* *id.* at 45266.

Furthermore, the traveling public needs to be confident that the government will carefully superintend access to and use of personal information. This is the basic privacy consideration with respect to CAPPS II. We will all

suffer if CAPPs II does not enjoy this confidence. We believe that several matters associated with this consideration should be discussed in more detail in the next Privacy Act notice to enhance that confidence.

First, a clearer explanation to the public of who within the CAPPs II program will have access to passenger information and for what purposes would be helpful. Such a description would allay concern about whether the scope of an authorized individual's access to and use of information will be as limited as practicable and directly tied to her or his aviation security responsibilities. This predictable concern is likely to be more pronounced because of the involvement of commercial data providers in the CAPPs II passenger authentication process. *See generally* id. at 45266.

Second, the interim final notice does not explain how governmental authorities will oversee access to and use of passenger information and what penalties will be imposed for unauthorized access to or misuse of that information. Again, this is a significant issue that is likely to rise in importance because of the involvement of commercial entities in CAPPs II. A description of compliance and enforcement policies would enhance confidence in a program that, by its nature, will have virtually no public transparency.

There is an important international component of the CAPPs II data privacy issues. The Department of Homeland Security and the Department of State have met with European Commission data protection officials to discuss privacy issues associated with the Bureau of Customs and Border Protection's access to passenger name record data for customers on flights to the United

States. Those discussions, which are ongoing, have highlighted European concerns about the adequacy of U.S. data privacy protection practices. European authorities have expressed those same concerns about CAPPs II. We hope that U.S. and EC officials can agree in their current discussions about data protection principles that will be applicable to CAPPs II when it is introduced and thereby eliminate the need in the future for U.S. and European authorities to revisit passenger privacy protection issues.

Finally, implementation and application of CAPPs II will impose substantial new requirements on passengers and airlines. As we have noted in previous conversations with TSA officials, passenger name records do not contain all the categories of information that TSA contemplates will be available for CAPPs II. See *generally* id. at 45268 ("Categories of Records in the System"). Moreover, some current PNR categories are not mandatory. CAPPs II will consequently require airlines to change significantly their practices for acquiring information from customers. This will create substantial new resource demands on airlines.

The essential implications about the anticipated CAPPs II passenger information collection requirements are:

- Airlines will have to obtain the required CAPPs II information from every passenger. This will be more intrusive for the passenger and far more resource intensive for the airline than is the case today.
- Airlines do not control third parties, such as travel agents and online booking entities, through which the majority of air

transportation is purchased. Any failure of such a party to obtain mandated information will have to be remedied at the airport, which will delay passenger processing and inconvenience customers.

- Information in many instances will be obtained from passengers orally and entered manually into reservations systems. This will not only impose greatly expanded resource demands on airlines, it will also place demands on the time of customers.

As indicated above, airlines will need to reprogram their reservation systems to accommodate the mandatory collection of the expanded information categories. In addition, reservation call "talk time" will increase markedly, affecting the length of time a consumer is on a reservation call and the cost of such calls to air carriers. Furthermore, because the majority of reservations are made through third parties, most notably travel agents, airlines often do not have direct contact with the passenger until he or she arrives at the airport. This means that airlines cannot assure that information is collected from such customers at the time of reservation. Any CAPPs II rule must recognize this fundamental characteristic of airline distribution and mandate that third parties collect needed information at the time of their first contact with the customer. The failure to do so will result in serious delays for airline passengers at airport check-in, where airline customer service agents will have to collect from them the information that is necessary for CAPPs II

The foregoing is not meant to be an exhaustive explanation of the implications of the mandatory collection of CAPPs II passenger information. It is

intended, instead, to underscore that changes in the reservation and passenger processing environments will have substantial consequences, including added expenses and the likelihood of increased customer processing times.

The ultimate cost to the U.S. airline industry is unclear because the exact requirements of CAPPS II are unknown, as is the likely level of third-party provision of the required passenger information. With those caveats, the reprogramming and transaction costs of CAPPS II could generate tens of millions of dollars of costs for the aviation industry. This would be a very substantial burden for the airline industry, which is struggling to recover from unprecedented financial losses.

+++++

We have offered these comments because we believe that consumer acceptance, both in the United States and overseas, of CAPPS II depends on the government's assurance of suitable privacy protections and passengers' understanding of them. We also believe that the implementation and operational issues associated with CAPPS II need to be clearly recognized. These are indispensable considerations in the development of CAPPS II. Lingering customer concerns about CAPPS II would undermine the attractiveness of air transportation and the efforts of the U.S. airline industry to recover from its recent enormous financial losses.

Respectfully submitted,

A handwritten signature in black ink that reads "James L. Casey". The signature is written in a cursive style and is positioned above the typed name.

James L. Casey
Vice President and Deputy General Counsel
Air Transport Association of America, Inc.
1301 Pennsylvania Ave., NW
Washington, DC 20004
202.626.4211
jcasey@airlines.org

September 30, 2003

September 20, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Re: Comments on DHS/TSA-2003-1

Privacy Office:

I am writing to urge you to stop the CAPPS II program. I am deeply concerned that this program will put the government on a path toward ever-more intrusive background checks, and hinder the security at our nation's airports.

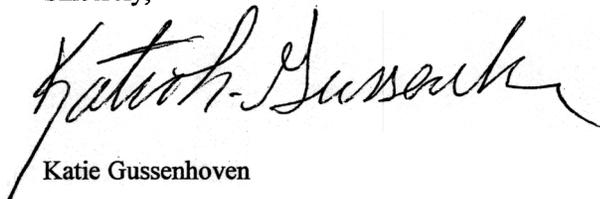
I have read that innocent people have already been stopped and banned from flying because their name appeared on government "no fly" lists -- and have been unable to clear their names in the federal bureaucracy. This national system would only increase the delays and blacklist even more innocent Americans - regular people traveling for work or vacations.

Terrorists will learn how to circumvent the system. Identity thieves could easily sidestep this check by presenting a false driver's license or passport, undercutting the system's entire mission. And the constant false alarms might divert the attention of airport security officers from legitimate threats to security.

I have also read that, if adopted, the most intrusive and dangerous element of the program - the construction of an infrastructure for conducting background checks on people who fly - would depend on shadowy intelligence/law enforcement databases of questionable reliability. The use of these secret databases would remove meaningful public oversight and control over these un-American background checks.

Once again, I urge you to stop this invasive and untrustworthy system.

Sincerely,



Katie Gussenhoven

12:
00}

JAY KINGWILL

9/20/03

Privacy Office
U.S. Department of Homeland Security
Washington, D.C. 20528

Re: DHS/TSA-2003-1

To whom it may concern:

If ever there were a strong argument against the proposed provisions of the so-called CAPPS II system, the article by Philip Shenon on the front page of today's (9/20/03) New York Times (in which there is a description of the malfeasance caused by the sharing of passenger information by JetBlue with Torch Concepts) is proof positive of this argument. And, this was accomplished by the apparent collection of less information than CAPPS II calls for.

CAPPS II will in no way make people safer on airplanes, since a terrorist could easily falsify information, and could indeed endanger passengers by diverting the attention of security officers from actual terrorists. What we care about is what people might do on an airplane. What will make people safer on planes is thorough screening of all passengers' carry-on luggage and checked luggage, and most importantly, all cargo shipped on passenger airplanes, items which at this point are not inspected.

Further, the information is purportedly to be deleted within a "set number of days", a so far undefined amount of time. This is directly akin to "foxes guarding the henhouse". Given the record of truth telling of the current administration, I have trouble believing that the information would be destroyed.

This system should be, must be, discarded.

Sincerely,



Jay Kingwill

cc. Senator Edward Kennedy

Senator John Kerry

Congressman William Delahunt

DOCKET No: DHS/TSA-2003-1

HERBERT A. LYON

PHONE:
[REDACTED]

FAX:
[REDACTED]

EMAIL:
[REDACTED]

Thursday, September 25, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528-0001

Dear Sir or Madam:

I am making these comments as a registered Professional Engineer (Texas 40700). I have over thirty years of professional experience in System Engineering of computer based systems. The vast majority of this knowledge is the design of large scale Government and Military Systems.

My areas of technical knowledge are.

- System Engineering
- Command and Control Systems
- Computer Systems, Programming, Data Base Management, Simulation
- Air Traffic Control
- Physical Security Systems
- Communications,
- Electronic Warfare

The Computer Aided Passenger Prescreening System (CAPPS) system must be designed to “Exclude” persons that have no history of any act that could remotely construed as being terrorist, not just to “Include” people because of some perceived notion of what actions constitute a threat.

As I understand the CAPPS, the system determines a score based on a very extensive database, which includes almost all data ever collected on the subject passenger by government agencies, and other commercial data sources. I have been involved with the design and uses of large-scale database systems, since 1964, all have flaws, when they are installed.

It is not unusual to run a detailed listing of errors in at database and find that the size of the printout of errors exceeds the size of the printout of the database.

To identify a potential terrorist on a passenger list an algorithm must be developed. These algorithms are in my experience extremely error prone, and require months of testing with constant manual review of the results. I developed one of the earliest Natural English Like Query Languages.

I understand that system will tend to error on the side of caution toward "INCLUDING" more travelers for intense screening, and not worrying about offending, delaying, and denying boarding to totally innocent passengers. In engineering terms getting a very high Probability of Detection, without worrying about the False Alarm Rate.

In my case, I have a number of things that probably tend to raise my probability of being intensely screened, or denied boarding:

- a. I have traveled extensively, on both business and pleasure, in the Middle East.
- b. I probably have a negative dossier with the Israeli Security Service, because I have traveled and done business in Egypt and Saudi Arabia.
- c. I have number of friends and business contacts that are of the Moslem Faith.
- d. My cousin, who has the same name as I do, "Herbert Lyon", has lived and taught in "Moslem" countries.

On the reverse side of the issue, there are a number of reasons for "EXCLUDING" me from intense screening of passengers:

- A. I held a U. S. Government Security Clearance for approximately 41 years (1952 to 1993); this included at least two Extensive Background Investigations. For a period of time my home was authorized for storage of classified material.
- B. I have never been arrested in my life, let alone charged with a felony. If my memory serves me right, my last traffic citation was in 1963.
- C. I volunteered for Active Duty and served in the United State Navy, during the Korean War.
- D. As a government contractor employee, I made a significant contribution to the wining of the Cold War, and to improvements to the Air Traffic Control System of the United States.
- E. As the Project Engineer for the Sinai Field Mission, I made a contribution to peace in the Middle East, at some peril to my personal safety.
- F. I own significant Real Estate, in Tampa, Florida, which I would not jeopardize by an illegal act.
- G. My business in the Middle East was centered on the recovery of Military Aid to Egypt, under the Camp David accords, for the United States Defense Industry.

I feel that any reasonable person would find the reasons for "EXCLUDING" far out weigh the reasons for "INCLUDING" for the intense screening or denied boarding.

Amendment IV to the Constitution of the United States reads as follows:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. I realize that the courts have suspended the Constitution in the case of transportation searches, but I feel that when the reasons for EXCLUSION far out weigh the reasons for INCLUSION, the Government must use due diligence in the exercise of that exception from the Constitution.

Each American Citizen must have the right to review his or her individual data in the CAPPS to identify errors. A means of corrections errors must be provided.

Each American Citizen must have the right to determine in advance there or not he of she is on the "Do Not Fly" list. If a person in on the "Do Not Fly" list a means of appeal must be provided.

Because of the intense Screening that I received on my trip in October of 2002, I feel that I may be on the "Do Not Fly" list. One of my interests and my greatest pleasures is international travel. There are several trips that I would like to take. However, these trips require extensive planning and up front expense. If I arrive at the airport and find that I cannot board the aircraft, I would out be hundreds to thousands of dollars in non-refundable airline tickets, tour bookings, and hotel reservations.

The Declaration of Independence states: *We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.* International Travel is my version of Happiness. If I cannot travel because I am correctly or incorrectly identified as by the TSA system, I don't think that any reasonable person would conclude that I have **Liberty** as envisioned by the framers of the declaration of Independence. If I cannot travel for required medical treatment in another location, my right to **Life** is being jeopardized. My father before me, in World War II, and I, in the Korean War, served in Armed Services of the United States to defend the principals and rights expressed in the Declaration of Independence and the Constitution of the United States.

It is only reasonable and proper that if I, a natural born citizen and veteran, have been deprived of my version of the *pursuit of Happiness* that a I be informed of suspension of that right. If the determination was made in spite of overwhelming evidence to the contrary, that I should be able to challenge the decision.

The **Tampa Tribune**, August 30, 2003, on Page 16, in the NATION/WORLD Section carried the quotation in an article:

In 2000, 83 percent of all leisure trips were taken by car, according to the Falls Church, Va., travel research firm D.K. Shifflet & Associates (7115 Leesburg Pike · Suite 300 Falls Church, Virginia 22043). In 2002, that number rose to 84.9 percent.

This means that travel, by modes for which TSA handles security, had decreased by almost 12 percent in two years.

Another article in a trade publication made the following statement: **New Lodging Construction Hits Record Low In 2Q03** *The pipeline for new hotel construction in the second quarter of the year was at an all-time low, according to research released last month by Portsmouth, N.H.-based hospitality tracking firm Lodging Econometrics. Business Travel News, Aug. 25, 2003*

My opinion is that TSA overly oppressive security policies and extremely long delays caused by security regulations have significantly contributed to these impacts to the Nation's Economy and the structure of society, in the Untied States of America.

As a security professional, I feel that these oppressive security measures do very little to lessen the probability of an aircraft hijacking. I feel the root cause of the events of 9/11 was the lack of sharing of intelligence information, which has been a problem, since 1962, in my personal experience. I encountered that problem, during my entire professional career in the design of military and government systems.

Because of Political Correctness, the government does not feel that it can use profiling. As a result, in my experience, terrorize innocent members of the traveling public with the most intrusive searches.

A friend of mine, who is a recent widow and a retired law enforcement officer, took her son on a trip to get him out of the house after the death of his policeman father. The 6 year old was removed from his mother, and searched in a most invasive way. The child, already traumatized by the death of his father, was further traumatized by the search away from his mother.

My niece's 14-year-old daughter must fly between her divorced parents. Every time, she travels by air, she is searched. It has reached the point that my sister-in-law must drive her between her parents.

At Tampa International, last fall I witnessed the terrorization of a heavyset handicapped woman in a wheel chair at the gate. She was searched in a most offensive way at the boarding gate. Obviously, this lady was not a threat to hijack an aircraft. If she were part of any conspiracy to hijack, she would have passed any contraband to a confederate prior to reaching the boarding area.

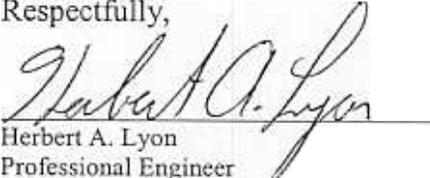
These are just three examples of the terrorization of the innocent traveling public by the TSA, but I am sure that thousands occur each day. So we have countered the "Terrorist Threat" by instituting terrorism by government and airline employees.

To emphasize the point that I made earlier, The CAPPS system is being used to INCLUDE into, rather than EXCULDE people for intense scrutiny. After all the publicity, on the CAPPS system and other totally invasive data bases true terrorists will not be used, if they have negatives in their public histories.

I would be pleased to sit down with you or your designated representative, to discuss any of the numerous issues that I have brought up in this letter. However, any meeting will have to be in the Tampa, Florida area, since I am not comfortable with using public transportation until my status in the CAPPS system is clarified.

The stated goal of al-Qa'eda is to disrupt the fabric of the American Society and Government. The fact that a Native Born Navy Veteran has to write this letter arguably demonstrates that al-Qa'eda has achieved their goal.

Respectfully,



Herbert A. Lyon
Professional Engineer

Sept 16 2003

Main Identity

From:
To: <privacy@dhs.gov>
Sent: Tuesday, September 16, 2003 11:05 AM
Subject: Re: DHS/TSA-2003-1

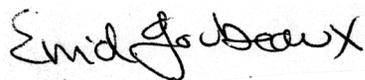
To the Privacy Office, U.S. Dept. of Homeland Security:

I wish to comment on the proposed Computer Assisted Passenger Prescreening II.

I agree with Bob Barr that this proposal could bring great harm to innocent Americans trying to fly. They could be defamed by mistake with no means of correcting the error, or of even knowing what triggered such treatment.

If you want to make air travel safer, I suggest making the airlines secure the cockpit doors (not in the flimsy manner now permitted); arm pilots; and start screening air cargo which is now unexamined due to the actions of an Alaska congressman.

Thank you.





ASSOCIATION OF
CORPORATE TRAVEL
EXECUTIVES

Asia-Pacific Canada EMEA United States

September 26, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

**RE: Docket Number DHS/TSA-2003-1
Comments from the Association of Corporate Travel Executives (ACTE)**

The Association of Corporate Travel Executives (ACTE) is a member driven, international organization comprised of over 2,500 corporate travel executives and suppliers of business travel products and services. Our members represent over \$150 Billion in annual spending on corporate travel and entertainment. By providing the highest quality education on industry issues and creating a platform for open discussion of all sides of issues, ACTE is dedicated to driving the business travel industry toward consensus, resulting in positive change and advancement. It is in this spirit that we offer our comments on the modifications to the proposed CAPPS II system and the CAPPS II Privacy Act notice published in the Federal Register on August 1, 2003.

Travel is one of the major engines of the global economy. It is an integral part of how we interact and how we conduct business. The health of the travel industry is crucial to a sustainable economic recovery. There is no doubt that assuring the highest possible levels of traveler safety and security is a top requirement for the future health and growth of the travel industry and the economy in general. Yet, equally as important is the assurance that this security is achieved efficiently, with minimal impact to the business traveler, and with no loss of personal privacy.

In general, ACTE views the recent modifications to the proposed CAPPS II system and the initial Privacy Act notice as a positive step toward balancing strengthened security with personal privacy. However, according to a recent member survey, support for CAPPS II is still divided with 52% of members supporting CAPPS II with the recent modifications and 48% either opposing the program or lacking enough information to either support or oppose.

ACTE strongly believes that further disclosure and modifications are necessary to ensure the accuracy and effectiveness of the system, to facilitate the movement of business travelers through the system, and to protect the privacy rights of individuals.

1. Disclosure of additional information

To date very little information has been made available about CAPPS II and how the system will work. This void of information has created a 'cloak of uncertainty' around the CAPPS II system, which limits the public's ability to provide constructive input to TSA. Specifically, TSA must be more forthcoming with following information:

Which commercial databases will be accessed in authenticating a passenger's identity?
What is the accuracy of the data in these commercial databases? And, what steps will TSA take to improve the data accuracy?
Given the accuracy of the data, what is TSA's anticipated percentage of false identifications?
What steps can a traveler take *prior* to travel to assure his/her data is accurate and thereby avoid a false identification?
Explain how false identifications will be resolved at the time of travel?
What specific passenger data will be used by the CAPPS II system? Is the full Passenger Name Record (PNR) sent to the commercial data providers or just specific data elements, which elements?

Our member survey indicated that:

78% believe that the issue of data quality in commercial databases needs additional work or has yet to be addressed by TSA.
74% feel that more needs to be done to reduce the risks and consequences of false positives due to data inaccuracies.
87% see a need for improvement to the process to correct inaccurate data.

2. Compliance with all privacy laws and regulations.

ACTE acknowledges that the recent modifications result in a scaling back of the scope and uses of information intended to be collected on passengers. However, in the management of corporate travel programs, corporations must assure that all transfers of data protect the ownership of both company and employee information. Our member survey indicated that 78% are still not comfortable that the manner in which CAPPS II handles PNR's does not violate corporate information policies. In order to assure that CAPPS II provides these safeguards, ACTE urges TSA to complete and publish a full CAPPS II privacy impact analysis prior to CAPPS II activation.

The current inconsistencies between U.S. and EU privacy regulations have put the airlines in a position where, in order to implement CAPPS II, they may have to violate at least one set of laws and in turn, could be subject to penalties. As the U.S. and EU work toward a bilateral agreement to reconcile these laws, ACTE supports some form of immunity for the airlines until a permanent resolution is reached.

3. Consideration of impact on business travel.

Any enhancements to the security screening process that expedite business travelers translate into increased productivity. Conversely, any changes that deter or delay the business traveler decrease productivity and, if significant could have a negative impact on the amount of business travel. As currently described by TSA, the proposed CAPPS II system does not distinguish between the frequent business traveler and the periodic, leisure traveler. While ACTE does not advocate discriminatory treatment of types of travelers, we do recommend that TSA take the following proactive steps to minimize the impact of CAPPS II on corporate travel:

- Provide corporate travel managers with information and actions to advise their company's travelers about how to assure the accuracy of their personal data used by the CAPPS II system.
- Provide a special TSA support desk to assist corporate travel managers in facilitating their corporate travelers through the CAPPS II security screening and resolving traveler identification issues.
- Provide corporate travel managers with the ability to pre-clear their corporate travelers through CAPPS II at the time of ticketing so any discrepancies could be resolved prior to airport check-in.

Given the impact that corporate travel has on the health of our economy, ACTE urges TSA to give increased consideration of the potential impact of systems such as CAPPS II on corporate travel. As experts in corporate travel, ACTE stands willing to work with TSA to provide this insight.

4. Implementation of a Registered Traveler Program

ACTE strongly supports the implementation of a voluntary Registered Traveler program to further facilitate the movement of business travelers through security screening. Reducing the 'hassle factor' at airport security through a Registered Traveler program will help to bring back the short-haul air traffic were airlines have been negatively impacted. Without such a program, business travelers will continue to utilize other means of travel, such as driving or rail, and travel alternatives, such as video and teleconferencing, in lieu of air travel.

By allowing passengers to voluntarily submit to background checks and pre-clearance and thereby receive expedited processing at airports limited security resources could be freed up to focus on higher-risk passengers.

ACTE has conducted member research on a Registered Traveler Program showing strong member support for the program. Our initial survey in September 2002 showed that 55% of our members supported the implementation of a Registered Traveler Program. Survey results reported in September 2003 show member support for this program increasing to 87%. This information has been shared with both TSA and the General Accounting Office. In subsequent discussions with TSA, ACTE has expressed our willingness to work jointly with TSA to further develop this program and participate in or administer a pilot program. We are eager to continue these efforts.

5. Efficient use of existing systems

ACTE encourages TSA, wherever possible, to leverage the investment in existing systems in the development of new or enhanced security systems. Systems, such as, Passport and INSPASS, already contain many of the capabilities and processes required to support a Registered Traveler Program. We request that TSA investigate the use of these and other existing system as a basis for a future Registered Traveler Program.

In conclusion ACTE is unequivocally in favor of taking proactive steps to create terrorist free skies but strongly advises TSA to consider the comments made herein prior to any activation of the CAPPS II system. Implementation of a system with the potential to negatively impact travel would be detrimental to our industry and would clearly hurt the general economy.

ACTE stands ready to work with TSA on the future development of both CAPPS II and the Registered Traveler program. We encourage TSA to use ACTE as a vehicle to provide more information and education on the positive impacts of these programs on the safety and security of air travel.

Respectfully submitted,

Mark Williams, President, ACTE
(Director, Travel and Meeting Management, PricewaterhouseCoopers)

Angela Naegele, Chairperson, ACTE TSA-CAPPS II Task Force
(Global Procurement Director, AT&T)

Nancy Holtzman, Executive Director, ACTE

Association of Corporate Travel Executives
515 King Street, Suite 340
Alexandria, VA 22314
703-683-5322
www.acte.org

September 8, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Re: Comments on DHS/TSA-2003-1

Privacy Office:

I am writing to express my dissatisfaction with the CAPPS II program. I am deeply concerned that this intrusive program will put the government on a path toward deeper invasions of privacy involving background checks, and further hinder security at our airports.

I have read that innocent people have already been stopped and banned from flying because their name appeared on government "no fly" lists -- and have been unable to clear their names in the federal bureaucracy. This national system would only increase the delays and blacklist even more innocent Americans - regular people traveling for work or vacations. I am reminded that a similar situation existed in this country in the 1950s only in that case it was a "red" list.

Terrorists will learn how to circumvent the system. Identity thieves could easily sidestep this check by presenting a false driver's license or passport, undercutting the system's entire mission. And the constant false alarms might divert the attention of airport security officers from legitimate threats to security.

I have also read that, if adopted, the most intrusive and dangerous element of the program - the construction of an infrastructure for conducting background checks on people who fly - would depend on shadowy intelligence/law enforcement databases of questionable reliability. The use of these secret databases would remove meaningful public oversight and control over these un-American background checks.

Once again, I urge you to stop this invasive and untrustworthy system and let's not repeat the same hysterics committed when McCarthyism held sway.

Sincerely,



Mr. Dean W. Koonts

September 23, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Dear Privacy Office,

I write to express my opposition to the testing and possible implementation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). As described in your department's Aug. 1, 2003 Federal Register notice, 68 Fed. Reg. 45,265, CAPPS II will violate the privacy and civil liberties of myself and every other air traveler and should be re-evaluated.

Under the proposed rules, the Transportation Security Administration (TSA) will have the power to gather personal information about me from both government and commercial databases, and to use this information to "tag" me if it appears that I may pose a threat to those aboard a flight. Not only is this an unquestionable violation of my privacy, the quality and accuracy of the information in these databases is very much in doubt. TSA claims that commercial databases will have to meet a "high standard" to be used in the execution of the CAPPS II system - but whether or not that turns out to be the case, CAPPS II also uses government databases, which are notoriously unreliable.

It is also unclear whether the TSA will use sensitive financial or medical information in building passenger profiles. While the supplementary information section of the Privacy Act Notice about CAPPS II says that this type of information will not be used, there is no such claim in the Notice itself. If the final regulations will be drafted from the Notice, why aren't these important privacy protections included?

Another problem is that the TSA leaves entirely unaddressed the issue of computer trespass and identity theft. Considering the "market value" of this type of information and the sophistication with which criminal intruders work, this is a grave oversight. Before the TSA begins to collect sensitive information, it must first provide the public with a strong assurance that the information is secure and cannot be compromised.

And what happens when the TSA makes the inevitable mistakes? Business travelers on their way to appointments and families on vacation will be unfairly subjected to detention, invasive searches and unwarranted background checks - but they will be in no position to do anything about this unjust treatment. Recourse for wrongfully targeted passengers is still almost non-existent, and the TSA has yet to propose any sensible solution for addressing the problem of such "false positives."

The right to travel is fundamental to a free society, and encroachments on that constitutional right - like requiring air travelers to provide personal information to the government in order to be allowed to fly - must be clearly justified. However, the TSA has presented no evidence that CAPPS II will protect me from terrorism any more than a properly implemented screening of passengers and baggage for weapons and explosives.

Further, CAPPS II violates my constitutional right to privacy. Any burden on that right must also be justified, but TSA has yet to show compelling evidence that giving up my privacy is necessary to protect against terrorism. Instead, CAPPS II would force all of us to sacrifice our privacy today, based on unsupported speculation that it will increase security tomorrow.

For these reasons and others, the proposed rules regarding CAPPS II should be withdrawn.

Sincerely,

A handwritten signature in black ink, appearing to read "David Norman", written in a cursive style.

David Norman

Re: Comments on DHS/TSA-2003-1

I am writing to urge you to stop the CAPPS II program. I am deeply concerned that this program will put the government on a path toward ever-more intrusive background checks, and it actually will hinder the security at our nation's airports.

Innocent people are now being stopped and banned from flying because their name are on government "not fly" lists. Moreover, they have been unable to clear their names in the federal bureaucracy. Without doubt this national system will increase delays and result in even more innocent Americans being blacklisted.

Terrorists will learn how to circumvent the system and identity thieves can easily undercut the system's entire mission by presenting false driver licenses or passports. The constant false alarms will likely divert the attention of airport security officers from legitimate threats of security.

The most intrusive and dangerous element of the program – the construction of an infrastructure for conducting background checks on people who fly – will depend on shadowy intelligence and law enforcement databases of questionable reliability. The use of these secret databases will remove meaningful public oversight and control over these un-American background checks.

I urge you to stop this invasive and untrustworthy system.

Sincerely,

Lucretia Bondish

A number of postcards were received as well. Each was pre-printed with the above comments. Following are the front surfaces of each card.

To: Privacy Office
U.S. Dept. of Homeland Security

From: *LaBeth Pondish*

Subj: **Opposition to CAPPS II Program**

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528

To: Privacy Office
U.S. Dept. of Homeland Security

From: *Sandra Anderson*

Subj: **Opposition to CAPPS II Program**

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528

To: Privacy Office
U.S. Dept. of Homeland Security

From: *Terry Butterworth*



Subj: **Opposition to CAPPS II Program**

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528



To: Privacy Office
U.S. Dept. of Homeland Security

From: *Terrix Anderson*



Subj: **Opposition to CAPPS II Program**

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528



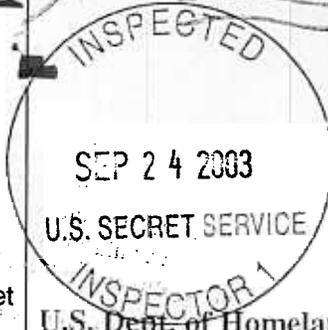
To: Privacy Office
U.S. Dept. of Homeland Security

From: **DOUG PETERSON**

Subj: Opposition to CAPPS II Program

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security

Privacy Office

Washington, D.C. 20528

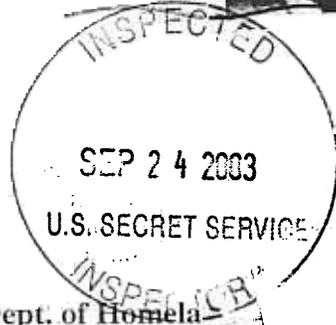
To: Privacy Office
U.S. Dept. of Homeland Security

From: **CHRIS ROSE**

Subj: Opposition to CAPPS II Program

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security

Privacy Office

Washington, D.C. 20528

To: Privacy Office
U.S. Dept. of Homeland Security

From: David BUTTERWORTH

Subj: **Opposition to CAPPS II Program**

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528

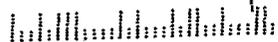
To: Privacy Office
U.S. Dept. of Homeland Security

From: Grace Martinez

Subj: **Opposition to CAPPS II Program**

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528

To: Privacy Office
U.S. Dept. of Homeland Security

From: *Fran Valenzuela*

Subj: Opposition to CAPPS II
Program

The program is a huge threat to
American's right to privacy, and
it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528



To: Privacy Office
U.S. Dept. of Homeland Security

From: *Marcus Aguirre*

Subj: Opposition to CAPPS II
Program

The program is a huge threat to
American's right to privacy, and
it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528



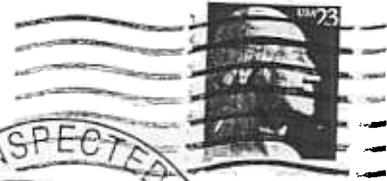
To: Privacy Office
U.S. Dept. of Homeland Security

From: Dave Coa 12 SEP PM

Subj: Opposition to CAPPS II Program

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528

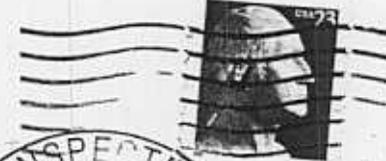
To: Privacy Office
U.S. Dept. of Homeland Security

From: MARGARET TYLER 12 SEP PM

Subj: Opposition to CAPPS II Program

The program is a huge threat to American's right to privacy, and it must be stopped because:

- Americans will be judged in secret
- The system will not make Americans safer
- The data base will delve into sensitive, private data
- There are no notification, appeal or correction processes
- Great potential for discriminatory impact



U.S. Dept. of Homeland Security
Privacy Office
Washington, D.C. 20528