Stanford Legal Clinic

Cyberlaw Clinic

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 724-1900
Fax 650 723-4426

VIA FEDEX

January 19, 2007

David W. Kane, Federal Security Director
Inspector James A. Roberts
Transportation Security Administration
5420 West Southern Avenue, Suite 205
Indianapolis, IN 46241

Re: EIR NUMBER 2007IND0021

Dear TSA,

By way of introduction, we represent Christopher Soghoian, a graduate student in the School of Informatics at Indiana University. On November 28, 2006, you indicated that the TSA was investigating whether Mr. Soghoian violated the Code of Federal Regulations and wrote to give him an opportunity to submit written information regarding the matter.

We have several legal and procedural questions about this investigation which we hope your office can answer. These questions are listed in the final section of this letter. However, we appreciate the opportunity to respond substantively with information demonstrating that Mr. Soghoian has violated no statute or section of the Code of Federal Regulations. Mr. Soghoian never used or attempted to use his boarding pass generator to bypass any airport security measure. As I'm sure you are aware, the FBI dropped its investigation of Mr. Soghoian after interviewing him extensively in and out of the presence of his attorney, our co-counsel, Stephen Braga.

Our client is in the business of studying security. He is neither the first nor the only individual to criticize flaws in the TSA's security procedures nor the only person to describe flaws in the way that boarding passes are created and used. He should not be subjected to civil penalties because he did not violate the Federal Regulations cited in the TSA's letter, because the regulations cannot be enforced against him or other passengers, because the civil damages provision cited in the TSA's letter does not apply to the cited regulations, and because Mr. Soghoian's website is protected by the First Amendment.

I. Critiques of the Boarding Pass Loophole

On August 15, 2003, Bruce Schneier, founder and CTO of network security company BT Counterpane, pointed out in his *Crypto-Gram* newsletter that there was no cooperation between the system that issued boarding passes at the ticket counter and the one that checked them at the security checkpoint:

> It's actually easy to fly on someone else's ticket. Here's how: First, have an upstanding citizen buy an e-ticket. (This also works if you steal someone's identity or credit card.) Second, on the morning of the flight print the boarding pass at home. (Most airlines now offer this convenient feature.) Third, change the name on the e-ticket boarding pass you print out at home to your own. (You can do this with any half-way decent graphics software package.) Fourth, go to the airport, go through security, and get on the airplane. This is a classic example of a security failure because of an interaction between two different systems. There's a system that prints out boarding passes in the name of the person who is in the computer. There's another system that compares the name on the boarding pass to the name on the photo ID. But there's no system to make sure that the name on the photo ID matches the name in the computer. In terms of security, this is no big deal; the photo-ID requirement doesn't provide much security. Identification of passengers doesn't increase security very much. All of the 9/11 terrorists presented photo-IDs, many in their real names…[1]

On February 13, 2005, Senator Charles Schumer of New York "revealed a gaping hole in [airport] security" on his official Senate website.[2] The Senator's website "outlined a situation in which anyone with basic computer skills can print a fake boarding pass and avoid scrutiny by airport security." After decrying the ease with which a terrorist could bypass airline security, Senator Schumer offered a detailed hypothetical description of exactly what "Joe Terror" would need to do to bypass airline security:

> 1. Joe Terror (whose name is on the terrorist watch list) buys a ticket online in the name of Joe Thompson using a stolen credit card. Joe Thompson is not listed on the terrorist watch list.
>
> 2. Joe Terror then prints his "Joe Thompson" boarding pass at home, and then electronically alters it (either by scanning or altering the original image, depending on the airline system and the technology he uses at home) to create a second almost identical boarding pass under the name Joe Terror, his name.

---

[1] http://www.schneier.com/crypto-gram-0308.html#6 (last visited January 16th, 2007). (Exhibit A)
[2] http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/2005/PR4123.aviationsecurity021305.html (last visited January 17th, 2007). (Exhibit B)

> 3. Joe Terror then goes to the airport and goes through security with his real ID and the FAKE boarding pass. The name and face match his real drivers license. The airport employee matches the name and face to the real ID.
>
> 4. The TSA guard at the magnetometer checks to make sure that the boarding pass looks legitimate as Joe Terror goes through. He/she does not scan it into the system, so there is still no hint that the name on the fake boarding pass is not the same as the name on the reservation.
>
> 5. Joe Terror then goes through the gate into his plane using the real Joe Thompson boarding pass for the gate's computer scanner. He is not asked for ID again to match the name on the scanner, so the fact that he does not have an ID with that name does not matter. [Since Joe Thompson doesn't actually exist it does not coincide with a name on the terrorist watch list] Joe Terror boards the plane, no questions asked.

This description is still posted on Senator Schumer's official Senate.gov website.

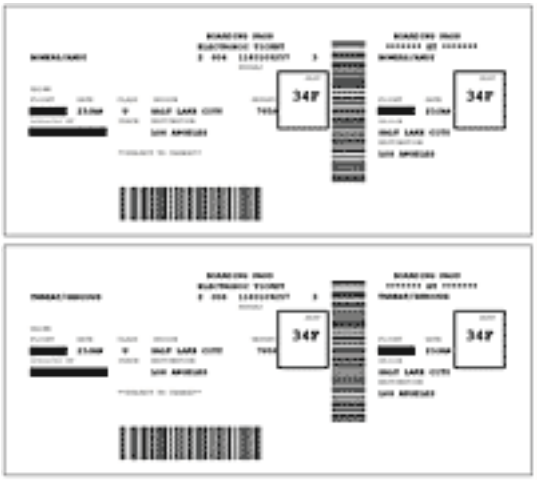
In response to this flaw in airline security, the Senator suggested that boarding passes and identification should be checked at the gate.

On February 7, 2005, Slate.com published a critique by reporter Andy Bowers similar to Senator Schumer's.[3] Bowers wrote that printing boarding passes at home created a "loophole" that makes circumventing airport security disturbingly easy:

> A home-printed boarding pass is generally checked only twice at the airport:
>
> 1) Right before you go through security, a security guard checks your boarding pass against your government-issued ID, making sure the names match. This check *does not include* a scan of the barcode, in part because the same security checkpoints process passengers for multiple airlines with different computer systems. Occasionally a second security guard at the metal detector will double-check the boarding pass, but again, not by scanning it.
>
> 2) Once you get to your boarding gate, the barcode on the printed pass is finally scanned just before you enter the Jetway. However, as the boarding agents remind you over and over, *you no longer need to show your ID at the gate.* (The TSA estimates 80 percent of U.S. airports have done away with ID checks at the boarding gate.) I've noticed that many passengers still have their driver's licenses or passports in hand as they approach, remembering post-9/11 enhanced security. But the agents cheerily tell them to put their IDs away—they're no longer necessary.
>
> Do you see the big flaw? *At no point do you have to prove that the person in whose name the ticket was bought is the same person standing at the airport.*

[3] http://www.slate.com/id/2113157/fr/rss/ (last visited January 17th, 2007). (Exhibit C)

> At stop 1), the name on a home-printed boarding pass is checked against an ID, but *not* against the name stored in the airline's computer. At stop 2), the name on the printed pass is checked against the name in the computer, but *not* against an ID.



Click on image to expand

> So all a terrorist needs to breeze through this loophole are *two different boarding passes*, both printed at home, that are identical except for the name. Check out the mock-up I made on Microsoft Publisher in about 10 minutes, using a real boarding pass I was issued last month. On the first one, you see my real name. On the second, the name has been replaced by that of Mr. Serious Threat, who we will pretend is on the No-Fly List.

(The image is included on the site.)

On May 12, 2005, security researcher Jacob Applebaum again decried the ease with which one could fraudulently enter an airport on his blog, with the heading "***Subvert and exploit pointless security measures at an airport***"[4]*:*

> Let's discuss two possible vectors of subversion, the name and the information presented on the boarding pass.
>
> The possibility to doctor this boarding pass is unlimited and this is partially based on your computing experience and partially based on the checking systems in place at the airport.
>
> Let's explore this in a moment. First I'll assume you're able to do basic image editing, visit the page for your boarding pass and save the document. You can print it if you're unable to find a way to save the document as a file. If you do that, you'll need to scan it in again, doctor the image and then print it a second time. That's a great deal of trouble but it demonstrates that as long as you can print the boarding pass, you can later reprint it any

[4] http://ioerror.livejournal.com/192472.html (last visited January 17th, 2007). (Exhibit D)

> way you'd like.
>
> Either way, open the image in an image editor. Now that you've got your image loaded into your favorite image editor, let's doctor it. Let's assume you've sold your ticket to someone else, let's call them A. Nonymous. Edit the image by first matching the font of your name and simply replace it with A. Nonymous. Obviously you'll want to match the order, first name first or last name first, whichever is the case.
>
> Print it.
>
> You've just subverted the name based credentials that you're flying with. You can now present a valid ID for A. Nonymous at the airport and no one will be the wiser. If A. Nonymous was on a flight restriction, you've just effectively lifted the ban. The only people that check your boarding pass against your ID are just above minimum wage federal employees guiding you into your security line. No one else checks your ID and no one verifies the validity of the ticket until you attempt to board.
>
> This is a very simple and well known flaw in entire boarding pass security system. There's nothing special or interesting about this beyond the fact that **you** *can do this*. This so called "security" was actually designed at the behest of the airline companies who wanted to solve the problem of people reselling their tickets. So in a way, this doesn't actually subvert anything interesting beyond being able to resell your ticket.

(Emphasis in original.) Mr. Applebaum then expressed his hope that the TSA would correct this problem.

Christopher Soghoian is a Ph.D. Candidate at the University of Indiana in Bloomington, Indiana. His academic study focuses on Security Informatics.[5] He received a B.S. in Computer Science from James Madison University and a Masters in Security Informatics from the Information Security Institute of Johns Hopkins University in May 2005. During various internships throughout his career, Mr. Soghoian has designed anti-phishing devices, designed account verification for cell phones, studied click-fraud, explored network vulnerabilities, and developed network security systems. He has received grants and scholarships from the Hispanic College Fund and the JHU Information Security Institute, as well as a GEM Graduate Engineering Fellowship and a Usenix Security Student stipend.

Through his academic work, he studies anonymity preserving networks, anti-phishing technology, click-fraud defense, ethical hacking and penetration testing, network security, and protocol/application security analysis, as well as airport and transportation security.

On October 25, 2006, Mr. Soghoian created a posting for his webpage critiquing TSA's use of readily alterable boarding passes as a security measure. His criticism was no different

[5] http://informatics.indiana.edu/ (last visited January 17th, 2006). (Exhibit E)

than that of Senator Schumer, Mr. Schneier, Slate.com, Mr. Applebaum or any number of other citizens interested in improving airport security. His webpage included a sample altered boarding pass, as did the Slate.com article, but this sample was interactive and allowed a reader to input a different name. His site called for a fix to the security hole.

On October 27, 2006, the FBI questioned Soghoian about his webpage. Soghoian explained his intention to point out the drastic and unremedied security flaw in the TSA's use of boarding passes as credentials for entering the secured areas of airports. He explained to the FBI that the website was created in a class and linked to a professor's work group at that professor's request. The website related to a research paper Soghoian is currently writing about securing airline boarding passes.

Mr. Soghoian cooperated entirely with the FBI, talking to them until after 10:00 PM. The FBI gave Mr. Soghoian a cease-and-desist letter from TSA at that time and told him to take the website down. However, Mr. Soghoian's Internet Service Provider had taken the website down by the time Mr. Soghoian returned from the questioning. Mr. Soghoian truthfully reported that he had never used an altered boarding pass, nor did he know of anyone who had generated and used one from his website.

After this encounter, on October 28, 2006, the FBI obtained a search warrant, entered and searched Mr. Soghoian's home, and seized much of his computer equipment.

The FBI interviewed Mr. Soghoian again with his attorney Stephen Braga present on November 14, 2006. Agents had reviewed the computer hard drives and other equipment seized from Mr. Soghoian and returned some of them at the November 14th interview. Following this thorough investigation, the FBI informed Soghoian that they would not pursue charges against him and that the investigation was over. The rest of Mr. Soghoian's equipment was returned around December 5, 2006, after the FBI erased Mr. Soghoian's hard drives with Mr. Soghoian's permission. The FBI investigation is closed.

On October 27, 2006, Congressman Edward Markey of Massachusetts criticized the website and called for Mr. Soghoian's arrest. Two days later, and after the FBI searched Soghoian's home, Congressman Markey announced publicly[6] that he had been hasty and agreed with Soghoian that it was too easy to create fake boarding passes:

> On Friday I urged the Bush Administration to 'apprehend' and shut down whoever had created a new website that enabled persons without a plane ticket to easily fake a boarding pass and use it to clear security, gain access to the boarding area and potentially to the cabin of a passenger plane. Subsequently I learned that the person responsible was a student at Indiana University, Christopher Soghoian, who intended no harm but, rather, intended to provide a public service by warning that this long-standing loophole could be easily exploited. The website has now apparently been shut down.

[6] http://blog.wired.com/27bstroke6/2006/10/congressman_res.html (last visited January 17th, 2007). (Exhibit F)

> Under the circumstances, any legal consequences for this student must take into account his intent to perform a public service, to publicize a problem as a way of getting it fixed. He picked a lousy way of doing it, but he should not go to jail for his bad judgment. Better yet, the Department of Homeland Security should put him to work showing public officials how easily our security can be compromised.
>
> It remains a fact that fake boarding passes can be easily created and the integration of terrorist watch lists with boarding security is still woefully inadequate. The best outcome of Mr. Soghoian's ill-considered demonstration would be for the Department of Homeland Security to close these loopholes immediately.[7]

After Congressman Markey's change of heart, an article in the *Washington Post* on November 1, 2006 chronicled the incident and included a statement by a TSA spokesperson claiming that Mr. Soghoian's boarding passes could not help anyone circumvent airline security:

> Amy Kudwa, a spokeswoman for the TSA, declined to say whether the agency was considering changing check-in procedures because of the incident. She said that while the fake boarding pass generator "had the potential to promote illegal activity, it will not aid anyone in circumventing airport security."
>
> She added: "The TSA assures that every person is thoroughly screened at the checkpoint for dangerous weapons or explosives. There are many layers of security at the nation's airports, including many methods that are not obvious to the casual observer."[8]

Boarding pass generation pages like Mr. Soghoian's are up and running on the internet today. For example, at http://j0hn4d4m5.bravehost.com/, an anonymous user has posted a generator, an example of the generator file, instructions for using the generator, and a plea to mirror the generator in other internet locations.[9] Wikinews states that "fake boarding passes are quite easy to create in Microsoft Word,"[10] a popular word processing program.

Discussion of this flaw in airline security and criticism of the current practice still pepper the internet. Mr. Soghoian did not provide the first, the only, the most detailed, or the simplest instructions for how one could exploit the problem with boarding passes.

---

[7] See http://blog.wired.com/27bstroke6/2006/10/congressman_res.html (last visited January 17th, 2006). (Exhibit F)
[8] http://www.washingtonpost.com/wp-dyn/content/article/2006/10/31/AR2006103101313.html (last visited January 18th, 2006). (Exhibit G)
[9] Last visited January 18th, 2006. (Exhibit H).
[10] http://en.wikinews.org/wiki/FBI_raids_creator_of_fake_boarding_pass_Generator (last visited January 17th, 2006). (Exhibit I)

II. Christopher Soghoian did not Violate the Statutes Cited in the TSA letter

Christopher Soghoian never "attempted to circumvent an established civil aviation security program." He has never used a fake boarding pass to enter the secure area of an airport. He has never created a boarding pass in an attempt to circumvent a civil aviation security program. His intentions were honorable and well in-line with his academic field of study and his research agenda at Indiana University. He wanted to improve airport security by dramatically pointing out an obvious flaw that he believes TSA officials are addressing inadequately.

Your November 28th letter cites sections 49 C.F.R. 1540.103(c), 49 C.F.R 1540.105 (a)(1), and 49 C.F.R 1540.105(a)(2). These regulations state that "no person may make, or cause to be made any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access medium, or identification medium issued under this subchapter,"[11] that "No person may tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under [subchapter C],"[12] and that "no person may enter, or be present within, a secured area, AOA, SIDA, or Sterile Area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas."[13]

Mr. Soghoian did not violate sections 1540.105 (a)(1), and 1540.105(a)(2). Mr. Soghoian never circumvented or attempted to circumvent any airport security measures. During all of Mr. Soghoian's travels, he has used his real name, used only airline-issued boarding passes, and used only his government-issued ID to verify his identity. The FBI found no evidence of wrongdoing of this nature during their thorough investigation. There is absolutely no evidence that could lead TSA to conclude otherwise.

Nor did Mr. Soghoian violate 49 C.F.R. 1540.103. We assume that TSA alleges that a boarding pass is a "report, record, security program, access medium, or identification medium issued under this subchapter." We would appreciate citation to any authority that supports this proposition, as we have found none. Even so, Mr. Soghoian did not alter any boarding pass with a fraudulent purpose. The purpose of his website and of the boarding pass generator was to draw attention to the TSA's failure to deal with the security problem cited by Senator Schumer and others. The website was related to Mr. Soghoian's graduate studies, supported by his academic advisor and department, and wholly honorable.

The website, including the boarding pass generator, did not break any law. The generator was part and parcel of Soghoian's critique of TSA procedures. All the generator did was allow readers to edit the name fields of a boarding pass. The generator was no more illegal than any

[11] 49 C.F.R. §1540.103(c).
[12] 49 C.F.R. §1540.105(a)(1).
[13] 49 C.F.R. §1540.105(a)(2).

image editor or graphics software, such as Photoshop or Microsoft Word, which can perform the same task.

III. Christopher Soghoian's actions are protected by the First Amendment

Mr. Soghoian created his website to critique on a flaw in Federal Aviation security procedures. The site included a subheading claiming that "The TSA Emperor has no Clothes." Its' stated purpose was "to demonstrate that the TSA Boarding Pass/ID check is useless"— it even added two humorous purposes for satirical effect. It then offered suggestions on how to "fix this glaring security hole." This kind of political commentary is strongly protected by the First Amendment.

The website did not advocate or encourage illegal activity in any manner. In *Brandenburg v. Ohio*, the Supreme Court struck down a regulation that criminalized "mere advocacy" where that statute did not distinguish between incitement and imminent lawless action.[14] The Supreme Court ruled that advocacy of illegal action is unprotected by the First Amendment *only* when it is 1) *directed to* inciting 2) imminent illegal action 3) and is likely to produce such action (emphasis added).[15] Soghoian's website doesn't come close to the Brandenburg standard for unprotected speech because it described rather than advocated illegal action and because it was not directed to inciting lawless action. Further, the TSA itself admits that Mr. Soghoian's website was not likely to produce imminent lawless action. In a November 1, 2006 *Washington Post* article, spokesperson Amy Kudwa stated that "while the fake boarding pass generator 'had the potential to promote illegal activity, it will not aid anyone in circumventing airport security.'"

Mr. Soghoian's boarding pass generator was on the same webpage as a suggestion on how to repair a security flaw. Mr. Soghoian's blog[16] and the accompanying comments discuss the need to repair the flaw and the government's previous unwillingness to do so. Posts on the blog continue to support Mr. Soghoian's critical purpose and suggest that the TSA should correct the security flaw. The generator was a demonstration of the ease with which one could fake a boarding pass. It was one section of the message presented by the site: airport security is too easy to bypass.

Computer code is speech protected by the First Amendment: "Communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code."[17] Soghoian's publication is protected by the First Amendment even though it also contained a boarding pass generator.

---

[14] *Id*.
[15] *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
[16] http://slightparanoia.blogspot.com/2006/10/bit-of-good-news.html (last visited January 17th, 2006).
[17] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 445 (2nd Cir. 2001). (Exhibit J)

IV. Christopher Soghoian Should Not Be Fined

If, against all evidence and law, the TSA decides Soghoian violated the referenced sections of the Code of Federal Regulations, he should not be fined.

A fine of $11,000 is contrary to law. The November 28th letter cites a civil penalty of $11,000 per violation. However, 49 U.S.C. 46301, the section the letter cites as authority for imposition of the fine**,** imposes a $10,000 cap for individuals. The TSA's "Enforcement Sanction Guidance Policy" (ESGP)[18] confirms that the sanction against individuals for violating TSA security requirements is capped at $10,000.

The ESGP states that only a very low fine would be appropriate under any circumstances: "An appropriate sanction for a single first-time violation, absent aggravating or mitigating factors, would be the low end of the corresponding range defined in the Table."[19] On the other hand, a sanction amount at the higher end of a range is appropriate only where there are aggravating factors. Moreover, individuals should be treated more leniently than a regulated entity. The penalty range for an individual who violates 49 CFR 1540.105(a)(1) is $2,500-$6,000. The penalty range for an individual who violates 49 CFR 1540.105(a)(2) is $1,000-$3,000. The penalty range for an individual who violates 49 CFR 1540.103 is $2,500-$6,000 plus a criminal referral. Of course, Soghoian was already investigated and cleared by the FBI. There are no circumstances justifying any penalty, never mind one higher than $2,500, the low end of the highest range.

Mr. Soghoian also meets the requirements of at least two Mitigating Factors cited in the Sanction Guidelines. The Guidelines specify that both "Disclosure by a Violator" and "Other Penalties assessed by federal, state, or local law enforcement" are mitigating factors in the assessment of fines. Mr. Soghoian voluntarily discussed his website with the FBI, the press, and the general public before the TSA's November 28th letter. He was also investigated and absolved by the FBI for his actions. He sustained significant damage to his home and equipment in complying with the FBI's procedures and requests. Another agency's consideration and favorable disposition of the matter mitigate any proposed fine.

---

[18] http://www.tsa.gov/assets/doc/FINALSanctionGuidancev1.12.07.doc (last visited January 18th, 2006). (Exhibit K)

[19] Id., p. 1.

V. Requests for Clarification

In addition to our substantive arguments, we raise several procedural questions and challenges.

What authority is there to impose these regulations on Mr. Soghoian, a civilian not-employed by the airline industry?

The three sections of Federal Regulations cite of a number of statutes as authority. All of those statutes regulate TSA and the aviation industry.[20] None of the statutes regulate individuals or passengers. Section 49 C.F.R. 1540.1 states that "This subchapter and this part apply to persons engaged in aviation-related activities." It does not state that its regulations apply to unaffiliated individuals. Meanwhile, Congress passed statutes specifically prohibiting passenger misconduct, including 18 U.S.C. 1036 (entry by false pretenses to any secure area of the airport) and 49 U.S.C. 46314 (Entering aircraft or airport area in violation of security requirements). The FBI investigation cleared Mr. Soghoian of these allegations. What statutes give TSA the authority to go beyond Congressional enactments in penalizing passengers?

What authority is there to impose civil damages as a result of violating these CFR sections?

Section 49 U.S.C. 46301 applies to violations of sections 49 U.S.C. 44901-44907, and those sections are cited as authority for the promulgation of the C.F.R. sections at issue here. However, sections 44901-44907 only govern the conduct of the Department of Transportation, the aviation industry, and airports. We have seen no legal authority for the proposition that the TSA can create civil liability for individuals where Congress chose not to do so in sections 18

[20] 49 U.S.C. 114, (generally creating the TSA); 49 U.S.C.5103 (reporting requirements, hazardous transport requirements, TSA consultation with the Department of Homeland Security, Secretary of Transportation's annual report, and "General Regulatory Authority"); 49 U.S.C. 40113 (All-cargo air transportation certificates of air carriers); 49 U.S.C. 44901 (requirements upon the TSA for screening passengers and property and accompanying procedures); 49 U.S.C. 44902 (requiring airlines refusal to transport passengers and property); 49 U.S.C. 44903 (requirements upon the Department of Transportation for aviation regulation ensuring passenger safety; publishing sanctions); 49 U.S.C. 44904 (requirements upon the Under Secretary of Transportation for assessing domestic air transportation system security); 49 U.S.C. 44905 (requirements on airports for disclosing information about threats to civil aviation); 49 U.S.C. 44906 (requirements for foreign air carrier security programs); 49 U.S.C. 44907 (Security standards for foreign airports); 49 U.S.C. 44913 (requiring airports' purchase of explosion detection equipment); 49 U.S.C. 44914 (Airport construction guidelines); 49 U.S.C. 44916 (exemptions for Alaskan airports); 49 U.S.C. 44917 (requiring periodic air carrier assessments by airports); 49 U.S.C. 44918 (security crew training requirements); 49 U.S.C. 44935 (employment standards and training for aviation and security personnel); 49 U.S.C. 44936 (requirements on aviation industry for employment investigations and restrictions); 49 U.S.C. 44942 (allowing the Secretary of Transportation to set performance goals and objectives); 49 U.S.C. 46105 (outlining how Secretary of Transportation should handle and institute regulations).

U.S.C. 1036 and 49 U.S.C. 46314. What statutes give TSA authority to penalize those not covered by the statutory authority under which they have been passed?

Other requests for clarification:

1. What procedural guidelines would the TSA follow in investigating and/or charging Christopher Soghoian?
2. Who would preside over any hearings, consider any motions or pleas, or adjudicate any dispute between Christopher Soghoian and the TSA.
3. What opportunities for appeal and presentation of his case would Christopher Soghoian have in the context of this investigation and any subsequent charges?
4. Why has TSA disregarded the FBI's conclusion that Christopher Soghoian did not break the law?
5. Has TSA submitted any complaint or similar form to any Administrator or Administrative Law Judge?
6. Has any official, particularly any Chief Counsel, been designated for or assigned to this case?

We look forward to hearing from you on these issues, and to the termination of this investigation on terms favorable to Mr. Soghoian. We will be in contact within two weeks to follow up on this matter.

Sincerely,

JENNIFER S. GRANICK
Stanford Law School
Executive Director, Center for Internet and Society
Director, Cyberlaw Clinic