



WASHINGTON NATIONAL OFFICE

Laura W. Murphy  
*Director*

1333 H Street, NW, 10TH Floor, Washington, DC 20005

Tel (202) 544-1681 Fax (202) 546-0738

**STATEMENT OF  
BARRY STEINHARDT  
DIRECTOR  
TECHNOLOGY AND LIBERTY PROGRAM  
AMERICAN CIVIL LIBERTIES UNION**

**ON  
GOVERNMENT DATA MINING**

**BEFORE THE  
TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS AND THE CENSUS  
SUBCOMMITTEE  
OF THE HOUSE OF REPRESENTATIVES  
COMMITTEE ON GOVERNMENT REFORM**

**MAY 20, 2003**

**BARRY STEINHARDT  
DIRECTOR  
TECHNOLOGY AND LIBERTY PROGRAM  
AMERICAN CIVIL LIBERTIES UNION**

**ON  
GOVERNMENT DATA MINING**

**BEFORE THE  
TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE  
CENSUS SUBCOMMITTEE  
OF THE HOUSE OF REPRESENTATIVES  
COMMITTEE ON GOVERNMENT REFORM**

**MAY 20, 2003**

---

My name is Barry Steinhardt and I am the director of the Technology and Liberty Program at the American Civil Liberties Union (ACLU). The ACLU is a nationwide, non-partisan organization with nearly 400,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and laws of the United States. I appreciate the opportunity to testify about government data mining on behalf of the ACLU before the Technology, Information Policy, Intergovernmental Relations And The Census Subcommittee of the House of Representatives Committee on Government Reform.

**Drift toward a surveillance society**

Government data mining is a vital topic because it is representative of a larger trend that has been underway in the United States: the seemingly inexorable drift toward a surveillance society – a trend well documented in a recent cover story in the *New York Times Magazine* and another in MIT's *Technology Review*.<sup>1</sup>

The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding what can be described as a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech method for invading privacy, from face recognition to implantable microchips, data-mining to DNA chips, and RFID identity chips in our clothing. The fact is, there are no longer any *technical* barriers to the creation of the surveillance society.

While the technological bars are falling away, we should be strengthening the laws and institutions that protect against abuse.

Unfortunately, even as this surveillance monster grows in power, we are weakening the legal chains that keep it from trampling our privacy. We should be responding to intrusive new technologies by building stronger restraints to protect our privacy; instead, we are doing the opposite – loosening regulations on government surveillance, watching passively as private

---

<sup>1</sup> Matthew Brzezinski, "Fortress America," *New York Times Magazine*, Feb. 23 2003; Dan Farmer and Charles C. Mann, "Surveillance Nation," *Technology Review*, April 2003 and May 2003.

surveillance grows unchecked, and contemplating the introduction of tremendously powerful new surveillance infrastructures that will tie all this information together. (The ACLU has written a report on this subject, entitled *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, which is available on our Web site at [www.aclu.org/privacy](http://www.aclu.org/privacy).)

### **Combating illusions of security**

Given this larger context in which data-mining proposals are being proposed, Congress must proceed carefully before authorizing their use and certainly none should be built or implemented without your explicit authorization.

In exercising your responsibilities, we believe you and all policymakers should apply a two-step test to proposals for potentially intrusive new programs and technologies:

- 1) Does the program actually makes us safer?
- 2) Is the actual improvement in safety provided by a technology enough to counterbalance its cost to our privacy and other fundamental freedoms?

If a new program is not actually effective, the matter should end there. There is no need to engage in detailed balancing tests or evaluations of a program's effect on privacy if it is not going to increase security.

We are not opposed to effective security. Far from it – as a New Yorker whose office is less than a dozen blocks away from the World Trade Center site, I take security especially seriously. And the ACLU has been calling for improvements in airport security since at least 1996, when we proposed measures like improved training and screening of airline personnel, tighter control of access to secure areas in airports, measures to enforce security standards at foreign airports, and luggage matching (recognized around the globe as a basic component of airline security, which the US has still failed to impose).<sup>2</sup> We have also proposed affirmative steps to increase the effectiveness of U.S. intelligence agencies at combating terrorism, including more reliance on human sources, better utilization of existing information technology to “connect the dots,” provision of sufficient incentives to recruit a diverse and skilled workforce of intelligence analysts (especially those skilled in foreign languages), in-depth training of all national security personnel, and a thorough review of excessive secrecy (it is secrecy, not civil liberties, which almost certainly represents the greatest barrier to effective information sharing in the government today).<sup>3</sup>

What we do oppose are measures that offer nothing but the illusion of security – programs that make us no safer but carry a substantial price in lost freedom.

---

<sup>2</sup> See for example, Statement Of Gregory T. Nojeim Before White House Commission On Aviation Safety And Security, September 5, 1996, online at <http://archive.aclu.org/congress/airtest.html>; or Statement Of Gregory T. Nojeim Before International Conference On Aviation Safety And Security In The 21st Century, January 14, 1997, online at <http://archive.aclu.org/congress/t011497a.html>.

<sup>3</sup> Timothy Edgar, Testimony at a Hearing on “Securing the Freedom of the Nation: Collecting Intelligence Under the Law” Before the House Permanent Select Committee on Intelligence, April 9, 2003, online at <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12313&c=206>.

## **Total Information Awareness**

The Pentagon's "Total Information Awareness" (TIA) program is a good example of a fundamentally flawed system that will not be effective at increasing our security.

DARPA has offered repeated assurances that it is only the developer of this system, and will not itself be involved in its deployment, and we take them at their word. TIA officials, however, appear to be understating what they have in mind. When their recent statements explaining the program are compared to statements made before TIA exploded as a controversy in the media, the story appears to have changed. For example, a chart that was posted on the TIA Web site (but replaced after the story broke) contained an extensive list of the categories of information planned for inclusion in the system: Financial, Education, Travel, Medical, Veterinary, Country Entry, Place / Event Entry, Transportation, Housing, Critical Resources, Government, Communications. The chart clearly indicated that such data would be fed into "automated virtual data repositories." (See Appendix 1) This chart has now been replaced by a new, more soothing presentation of what the program would look like. (See Appendix 2) Accompanying the new chart is a new and far less foreboding logo.

The fact is, TIA would be the infrastructure for a massive government surveillance program. In theory, it will be capable of searching countless public and private databases and combining the information found there to create an intimate look into the lives of 300 million Americans. We believe that members of Congress did precisely the right thing when you prohibited DARPA from training TIA on Americans, and required that it report on the key privacy and security issues involving TIA. That report will apparently be sent today. In preparation for that report, the ACLU has prepared its own report detailing the key questions that DARPA must answer to satisfy the Congressional requirement. (See Appendix 3)

## **Mission Creep**

Perhaps the most fundamental problem with a surveillance system like TIA is "mission creep." Information systems inevitably grow – not only in the data they collect, but in the uses to which they are put. My parents, for example, were promised when they received their Social Security numbers that they would not be used as a national identifier. Congress wrote into law a prohibition on their use for any purpose other than administering the retirement program. Fast forward a few decades, and when my children received their Social Security numbers – at birth – they were immediately put to use for a host of identification purposes.

Once TIA is in place, we will see a similar dynamic. Its operators will grow frustrated at the gaps in its coverage, and seek to have more and more transaction records available to them. TIA will be expanded from terrorists to murderers to thieves, and so on down the scale of wrongdoing until everyone is put on guard against the slightest infraction of every law, rule, regulation, and social code in America. At some point the Congress will want to draw the line, but it may well be too late once we start down that track. Despite the promises we are now hearing about protecting privacy – and they are only promises without any real proposals to back them up – TIA is very unlikely to remain restricted to hunting terrorists for very long.

### **Needed: proof it will work**

Where is the proof that TIA's operators will be able to pick out a handful of terrorists among 300 million Americans – that it will actually work?

As the non-partisan Association for Computing Machinery said in a January 23, 2003 letter to the Senate Armed Services Committee:

Research into areas such as new data mining and fusion methods and privacy-enhancement technologies is needed and welcomed. However, the overall surveillance goals of TIA suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. Technological research alone cannot make a system such as TIA viable.

As computer scientists and engineers we have significant doubts that the computer-based TIA Program will achieve its stated goal of "countering terrorism through prevention."

Study after study has concluded that the failure to prevent the 9/11 attacks was a result not of insufficient information, but of the government's inability to process, analyze and distribute the bountiful data it already had.<sup>4</sup> TIA solves the wrong problem: it seeks to prevent terrorism by sucking in vast new troves of information. You don't look for a needle in a haystack by adding more hay to the pile. Especially when much of that hay is rotten – when so much data is wrong, TIA will inevitably be sent on endless wild goose chases, in the process subjecting countless Americans to harassment or worse.

TIA's defenders are fond of noting that it would have to comply with all current laws. But that argument completely misses the point. There are no overarching or specific privacy laws that would fundamentally interfere with the creation or operation of massive data exploitation programs like TIA. Current laws are simply not sufficient to protect our privacy in the face of a program like TIA, which makes use of new technological capabilities that have far outstripped our outdated laws. If not for the Wyden Amendment that restricts the uses of TIA against Americans, it is not clear that anything would have prevented DARPA from building it.

### **CAPPS II**

CAPPS II (for "Computer Assisted Passenger Pre-Screening System") is an attempt to update a more rudimentary airline profiling system already in existence, known as CAPS I. The details of that system, which has been in place for several years, have been kept secret. Transportation Security Agency (TSA) chief Admiral James Loy, however, has said that it is "too broken to be repaired."<sup>5</sup>

---

<sup>4</sup> For example, see *Final Report of the Congressional Joint Inquiry Into September 11: Findings and Conclusions*, online at [http://www.fas.org/irp/congress/2002\\_rpt/findings.html](http://www.fas.org/irp/congress/2002_rpt/findings.html).

<sup>5</sup> Admiral James M. Loy, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the House Committee on Government Reform, May 6, 2003. Loy's prepared statement is online at <http://us.gallerywatch.com/testimony/108/pdf/PDFTest2689.pdf>. The quotation used here was made during the question-and-answer period.

Another disastrous attempt at airline security has been the government's "no-fly" list of terrorist suspects, ensnaring what appear to be tens of thousands of innocent Americans who find themselves facing intense security scrutiny every time they fly, with no way of finding out how they got on a list or how to get off.

### **Innocent Americans singled out**

Jan Adams and Rebecca Gordon of California, for example, were detained at San Francisco International Airport, and told that their names appeared on the secret "no-fly" list. The two women – peace activists who publish a newspaper called *War Times* – were told nothing about why they were on such a list, or how they could get off. The ACLU has filed suit against the Federal Government on their behalf to find out how the "no fly" lists were created, how they are being maintained or corrected and, most importantly, how people who are mistakenly included on the list can have their names taken off. One question we believe needs answering is whether our clients are on the "no fly" list because of their First Amendment protected political views.<sup>6</sup>

While the Federal Government has thus far refused to provide us with any information, according to documents released to the ACLU by the City of San Francisco, our clients were part of much bigger mess. According to City documents more than 340 persons were investigated by the San Francisco police after being flagged by the "No-Fly List." All of them were eventually found to be innocent of any wrongdoing.

Federal documents obtained by the Electronic Privacy Information Center further confirm that Adams and Gordon are only on the tip of the iceberg.<sup>7</sup> Those documents, which include letters forwarded to the Executive Branch by member of Congress, represent hundreds of complaints by passengers from all walks of life:

- A New Jersey man wrote to his member of Congress because he is routinely denied access to curbside check-in and interrogated at the check-in counter, because his common Middle Eastern name appears on the no-fly list. A former member of the U.S. Navy, the man has never traveled to the Middle East and cannot speak Arabic. "This problem also applies to my son and grandson," he wrote. "Likewise American born, loyal citizens of the United States of America."
- A Washington state man wrote that his co-workers now go out of their way not to be placed on the same reservation as him when traveling. "I have now become known to staff as the person not to travel with," he wrote. Apparently there is nothing he can do to reverse this quasi-pariah status; he was told by Alaska Airlines and Southwest Airlines to contact the government, but has not received responses from any federal agency.
- One woman wrote to the TSA in October 2002 to complain that she, her sister and her 76-year old mother were stopped every time they fly, because their last name

---

<sup>6</sup> An ACLU press release on the case is online at <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12439&c=206>

<sup>7</sup> EPIC has posted the documents online at [http://www.epic.org/privacy/airtravel/foia/watchlist\\_foia\\_analysis.html](http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html).

appeared on the no-fly list. “We are from Texas and Oklahoma,” she wrote. “Our last name is not foreign. We are not foreign. So why do we get flagged every time?”

Now we are told CAPPS II will fix those problems, but it has all the makings of an even bigger, more frightening system.

### **CAPPS II: How it would work**

As we understand CAPPS II, it is a two-stage program. In the first stage, passengers making a reservation will be asked to provide four pieces of data:

1. name
2. home address
3. home phone number
4. date of birth

This data will be checked against the headers on credit histories and a score will be assigned expressing the likelihood that the person is who she says she is.

In stage 2, secret intelligence and law enforcement databases and potentially commercial databases as well (TSA refuses to rule this out) will be checked, and then, based on a constantly changing algorithm, a security rating will be assigned: green for normal security, yellow for enhanced searches, and red for no-fly.

This proposed system would seem, on its face, to be an improvement over CAPPS I, but both the security and privacy devils are in the details.

First, the identifying information for stage 1 is easily obtained by hook or crook. I bought my own data online for only \$29. It is not hard or expensive to assume someone else’s identity in the US. Indeed, when I bought my own data, I discovered that there was a second Barry Steinhardt, who apparently lives in California and whose data I could easily obtain for the same \$29.

Second, the secret databases, whether governmental or commercial, are likely to be replete with errors that will expose the innocent to humiliation or worse, and waste scarce security resources that could be used far more effectively.

Approximately 100 million Americans fly every year. Since many fly more than once, there are approximately one billion records. If even a tiny fraction of the searches were wrong – let us say 1/10 of 1 percent, or an accuracy rate of 99.9 %, the result would be as many as 1 million erroneous alarms affecting approximately 100,000 separate individuals. That would be unacceptable from a civil liberties point of view – and from a security perspective as well.

And, of course, the underlying records will contain so many inaccuracies that a 99.9% accuracy rate is likely to be unrealistically high. Indeed, while many good people are likely to get caught up in this drag net search, the bad guys will quickly learn how to avoid the system and enhanced security.

### **The problem with profiling**

Although we are not being told how Americans' security ratings will be generated in the secret government databases to which CAPPs II will connect, there is good reason to be suspicious of the whole concept of trying to stop terrorism through profiles.

From a security perspective, profiles are notoriously under inclusive. Those who do not "fit the profile" are given only cursory attention, or no attention at all. Yigal Amir, the man who assassinated Israeli Prime Minister Yitzhak Rabin, did not fit the "profile" of a "terrorist" and was therefore allowed unwarranted access to the Prime Minister. Indeed, the TSA explicitly told us that their CAPPs II profiling would not include a domestic terrorist like Timothy McVeigh, who was convicted of murdering 168 men, women and children in Oklahoma City.

The first recorded bombing of a commercial plane occurred in 1949, when a woman hired assassins to kill her husband, who was on the aircraft. What profile would prevent that from recurring? The first bombing of a U.S. commercial carrier occurred in 1955, when a passenger's son arranged to have a bomb explode in a passenger's luggage so that the son could collect on an insurance policy. Did that passenger fit the profile of a "terrorist?" The problem is that profiles are always one step behind the attackers. Brian Roehrkasse, a spokesperson for DHS Secretary Tom Ridge, could not have put it more clearly when he told *USA Today*, "One thing that we know about terrorists is there is no way to predict what will happen."<sup>8</sup>

Profiles offend not only the goal of safety, but also the U.S. Constitution. The Fourth Amendment requires that a person should not be subjected to invasive investigative techniques without probable cause that is particularized to that person. Profiling violates that principle: it treats people as potential criminals in the absence of facts specific to them suggesting they are likely to engage in wrongdoing. The use of such stereotypes may temporarily make people feel safer, but they will not actually increase safety and may instead decrease safety. These profiling systems will fail. When they do, the proponents of profiling will not admit that profiling does not work. They will insist that it needs to be "improved" by adding ever more personal data about passengers to the mix. A perfect example of this is CAPPs II itself: Despite the fact that CAPS I is "too broken to be repaired," proponents, rather than giving up on the concept, seek to "improve" it by accessing even more personal information.<sup>9</sup>

### **The danger of racial profiling**

Another danger is that protected characteristics such as race could become the basis for security profiles – and CAPPs II's potential to lead to racial or religious profiling is something that bears just as much advance scrutiny as the issues of privacy and due process.

---

<sup>8</sup> Laura Parker, "Terrorists' most likely weapon here? Bombs," *USA Today*, May 15, 2003.

<sup>9</sup> This was predicted by the ACLU in 1997 and now coming true in 2003. See Statement Of Gregory T. Nojeim Before International Conference On Aviation Safety And Security In The 21st Century, January 14, 1997, online at <http://archive.aclu.org/congress/t011497a.html>.

As TSA itself has acknowledged, discriminatory profiling is both poor law enforcement technique and offensive to the Constitution. But even profiles that do not explicitly include race or other protected categories as an element can have a discriminatory effect on minority communities. A 1997 Justice Department review of the CAPS I system found that CAPS I did not use race, religion, national origin, or ethnicity as a screening factor, but did find that the system might have a disparate impact on passengers in those groups.<sup>10</sup> The DOJ report included numerous recommendations for oversight and reporting requirements that would ensure that the profiling system remained constitutionally sound. As far as we know, none of these recommendations have been followed to date. For years the ACLU urged the Department of Transportation to establish an independent entity that would monitor abuse in aviation security such as discriminatory searches. The Civil Liberties Advisory Panel to the White House Commission made a similar recommendation.<sup>11</sup> No such panel has been established to date.

Given the secrecy around the CAPPs II risk assessment criteria, it is difficult to assess any likely disparate impact that such a program would have on particular racial, ethnic, or religious groups. But the fact that CAPPs II would rely on credit information suggests individuals without a credit history will immediately be suspect – and that includes the very young, the very old, and especially people of color.

At a minimum, there should be independent assessments of CAPPs II for discriminatory impact before a decision is made to go forward. It is incumbent on the government to ensure that the Constitution's promise of equal protection is not being overrun by ineffective and discriminatory security measures.

### **Expansion plans already laid**

We urge you to heed the advice of Mark Forman, associate director of the Office of Management and Budget, who expressed doubt about CAPPs II in testimony before this very subcommittee in March. "If we can't prove it lowers risk, it's not a good investment for government," he declared, adding that OMB will not let the program go forward until questions about its effectiveness are answered.<sup>12</sup>

But even assuming that CAPPs II could meet the first part of our test (effectiveness), it certainly cannot meet the second. Balanced against any marginal improvement in catching terrorists that the program manages to provide would have to be the fact that it would lead to an enormously dangerous expansion of the government's role. It would none-too-slowly be transformed into a general data mining or profiling system.

Unlike the TIA program, the path has already been explicitly laid out for how CAPPs II will be expanded. As Admiral Loy told this subcommittee on May 6, the TSA envisions CAPPs

---

<sup>10</sup> Department of Justice Civil Rights Division, October 1, 1997

<sup>11</sup> White House Commission on Aviation Security and Safety, Final Report to President Clinton submitted by Vice President Al Gore, Chairman, February 12, 1997.

<sup>12</sup> Leslie Miller, Associated Press, "U.S. Passenger-Screening Plan Questioned," March 25, 2003.

II being expanded to boats and trains and other modes of transportation, and tied into the massive TSA identity card program known as TWIC (Transportation Workers Identification Credential). Once in place, CAPPS II and TWIC would become the foundation of a “trusted traveler” program, in which the government would begin conducting in-depth background checks on fliers – checks that would be “limited” and “voluntary” at first, but would inevitably spread from there.<sup>13</sup> There are approximately 60 million “frequent flyers” in the US, so this would be no small system.

While we appreciate that Admiral Loy and his staff took the time to meet with us to explain the program and answer some, although not all, of our questions, a system of this size, scope and complexity will inevitably be expanded. As with TIA, mission creep as to both scope and purpose will be unavoidable.

### **Due process**

One of the most troubling aspects of CAPPS II is the absence of any real due process. There will be mistakes and lots of them, but adding a few customer advocates is hardly going to solve the problem, when the individuals still won’t be able to get a reason they are on the list, see the information being used against them, or correct errors in their record. Under the TSA’s own descriptions of the program, CAPPS II decisions will be based on information contained in government databases that are utterly secret – mysterious black boxes the contents of which we will not know and cannot be revealed to ordinary Americans. For those who are falsely accused, there will be no good way out of the CAPPS II “prison.”

In the end, the proponents of CAPPS II have not demonstrated that it will work. Its effectiveness is uncertain, but there is no doubt that it will lay the groundwork for a massive governmental surveillance program.

### **Questions that Congress should ask about programs like TIA and CAPPS II**

In summary, there are six questions that Congress needs to have answered before it should even consider giving a go-ahead to programs like CAPPS II and Total Information Awareness:<sup>14</sup>

#### **1. Where is the evidence that the program will actually work?**

Before such dangerous programs are implemented, policymakers need hard evidence – not speculation – that they will work.

---

<sup>13</sup> Loy, testimony, op. cit. The point cited here was made during the question-and-answer period.

<sup>14</sup> The Senate Commerce Committee is also asking questions about CAPPS II. On May 8 the Senate unanimously passed a provision requiring TSA to deliver a report on the program. See Audrey Hudson, “Hill assumes oversight role on airline screening,” *Washington Times*, May 10, 2003.

**2. What will the error rate be?**

Congress needs to know the likely false negative (incorrectly allowing a terrorist to pass) and false positive (incorrectly flagging an innocent person) rates for these systems, and what the estimates are based upon. Because the number of terrorists is so small in comparison to the overall population, false positives are especially likely to be a problem.

**3. How much will the program cost to build and operate?**

The Congress was recently asked to provide \$35 million to build CAPPS II.<sup>15</sup> (In a presentation given to us by TSA at Wye River, we were told it would cost just over \$35 million to both build and operate the system). Given the enormous scope of this system – processing a billion records for 100 million separate passengers, correcting errors, fielding complaints, connecting computer systems to every airline counter in the nation – that figure strains credulity. What is the real cost, and what other security measures (for example, aircraft anti-missile systems) might we be giving up to pay for these programs?

**4. Is there a credible method for the falsely accused to get off the list?**

The right to travel is a core human liberty. If some people are going to be deprived of that liberty – in effect, punished – they must have genuine due process. That must include real access to the records on which such decisions are made, and access to some kind of neutral magistrate who can evaluate the fairness of the deprivation of liberty. How will such due process be provided in a system based on secret government databases? Or will unfairly profiled passengers have to rely on the very same government agency that made the mistake in the first instance?

**5. What laws are in place that will protect us?**

What current laws would protect against unauthorized abuses of our private information – and more importantly, the authorized misuse of our private data?

**6. What will be the cost to our privacy and freedoms of building these systems?**

In light of the historical fact that government agencies and surveillance systems alike tend to expand and not contract, can we really restrict these kinds of programs to their original purpose?

**Chaining the surveillance monster**

TIA and CAPPS II are the ultimate expressions of a growing surveillance monster. If we do not take steps to control and regulate surveillance to bring it into conformity with our values, we will find ourselves being tracked, analyzed, profiled, and flagged in our daily lives to a degree we can scarcely imagine today. We will be forced into an impossible struggle to conform to the letter of every rule, law, and guideline, lest we create ammunition for enemies in the government or elsewhere. Our transgressions – whether real or imagined – will become permanent Scarlet Letters that follow us throughout our lives, visible to all.

---

<sup>15</sup> Loy, testimony before the Senate Appropriations Subcommittee on Homeland Security, May 13, 2003. Online at <http://appropriations.senate.gov/releases/LoyMay13.pdf>.

Some commentators have already pronounced privacy dead. The truth is that a surveillance society does loom over us, and privacy, while not yet dead, is on life support. It is not too late to put chains on the surveillance monster. The Congress acted properly by curtailing both the utility-worker informant program TIPS and TIA, and by requiring a review of CAPPs II. But you need to remain vigilant, and continue to resist programs that will make us neither safe nor free.