Testimony of Stewart Baker[1]

Before the National Commission on Terrorist Attacks Upon the United States

December 8, 2003

Two and a half weeks before the attacks of September 11, 2001, the United States government knew the names of two of the hijackers. The government knew that these men were Al-Qa'ida killers and that they had entered the country. It started looking for them in late August.

In fact, Khalid al-Mihdhar and Nawaf al-Hazmi were living openly in the United States. They had used their true names to sign rental agreements, engage in financial transactions, attend flight school, earn frequent flier miles, and get a California DMV identity card. On September 11, they would fly American Airlines 77 into the Pentagon.

If we had found them, there is a real possibility that we could have thwarted most or all of the hijackings. That's because al-Mihdhar and al-Hazmi were linked to many of the other hijackers. They had shared addresses, for example, with Mohamed Atta, who flew American Airlines 11 into the North Tower of the World Trade Center, and Marwan Al-Shehhi, who flew United 175 into the South Tower. By searching other data in private hands, we could have linked them to most of the other hijackers as well.[2] In short, August 2001 offered our last, best chance to foil the attacks.

We failed. Let me say that again, because if there's a scandal that deserves investigating in these events, I'll wager that it isn't in the President's daily brief or some imaginary communication to the President from the Saudi government. It's what happened – and what didn't happen – in August of 2001. In two and a half weeks, despite all the resources of our intelligence and law enforcement agencies, we could not find two known terrorists living openly in San Diego under their own names. Not in a day. Not in a week. Not in two.

How can that possibly be? How can we have failed so badly in such a simple, desperate task?

---

[1] Stewart A. Baker is a partner and head of the Technology Department of Steptoe & Johnson in Washington, DC. He was General Counsel of the National Security Agency in 1992-94. He has served on numerous government boards and commissions concerned with technology and national security. He is currently a member of the Markle Foundation Task Force on National Security in the Information Age. *See* Attachment A.

[2] The details are laid out in the October 2002 report of the Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, p. 22.

In my view, there were two problems – a problem with the tools our agencies were able to use and a problem with the rules they were required to follow. What's worse, two years later, neither problem has been fixed. Which means that there is a very real risk we will fail again, and that more Americans will die at the hands of terrorists as a result of our failure.

1. Tools

When the FBI learned in late August that al-Mihdhar was in the country, an FBI agent began trying to locate him. The agent contacted the State Department to get al-Mihdhar visa information. There was evidently no computer link that would allow him to do the search. It took two days for him to get the information that al-Mihdhar had listed a New York Marriott hotel as his address on arrival. The agent also lacked access to the hotel's reservation system; it took him a week to find out that al-Mihdhar was not there. The agent did check the computerized records to which he had easy access – national and New York criminal records and motor vehicle records. They showed nothing, and the agent did not have easy access to the many other records that al-Mihdhar and al-Hazmi had generated with private companies and state governments. Getting such data required shoe leather and local contacts. When the agent finally did ask for help from the FBI's Los Angeles Field office, it was too late. The request for assistance was sent on September 11.[3]

The government's failure to find the hijackers was caused in the first instance by a lack of information technology tools. The FBI certainly had legal authority to obtain records from airlines, hotels, banks, and other government agencies. What it lacked was a quick, straightforward way to conduct searches of data that the FBI was entitled to obtain. The lack of computer tools made the agent's job much harder and much slower. And in this case, the delay was deadly for thousands of Americans.

a. The tools we need. Modern information technology can provide faster, more efficient access to records that will enable us to find the next group of terrorists planning attacks inside the country. Of course, future terrorists will not be as accommodating as al-Mihdhar and al-Hazmi. They may not use their own names while here, so we need to be able to conduct searches of private databases to locate terror suspects not just by name but also by address, phone number, credit and bank card number, and other potentially identifying information. We've made some progress in that area, but not much. Certainly not enough.

That is the capability we need just to defend against the last attack. It may not be enough to defeat the next. There are many other information technology tools that are

[3] House and Senate Intelligence Committee Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001, p. 154.

already available in the private sector and that should be adapted to respond to entirely plausible, even likely, future attacks.

What capabilities do we need? The Markle Foundation Task Force of which I am a member has just issued a second report, *Creating a Trusted Information Network for Homeland Security*, that deals precisely with the problem of how to improve the government's information tools to fight terrorism. In Appendix F to that report, Jeff Jonas and I set forth twelve information technology challenges – twelve terrorism-related capabilities that the government needs and should be able to achieve in the short term using commercially available technology. These challenges are specific, achievable, and tied to realistic scenarios. They include the following recommendations:

- "Counterterrorism officers should be able to identify known associates of the terrorist suspect within 30 seconds, using shared addresses, records of phone calls to and from the suspect's phone, emails to and from the suspect's accounts, financial transactions, travel history and reservations, and common memberships in organizations, including (with appropriate safeguards) religious and expressive organizations."

- "The government should be able to search, in real time, records showing the status and locations of foreign students, including prospective and former students, research assistants, and teachers in programs that raise terrorism concerns."

- "Police checking driver's licenses or license plates should, in most cases, be automatically alerted when they run the documentation of a terrorist suspect. However, the watch list database should not be easily reconstructed by local police agencies, and the alert should be tailored to the circumstances of the suspect and the stop."

- "The government should have a consolidated list of terrorism suspects that includes the different lists that have been assembled by different agencies for different purposes."

- "Watch lists should be updated in an accountable fashion on a real-time basis."

- "Both the government and the private sector should be able to identify false identities in real time when vetting employees or preparing to engage in a material transaction – opening a bank account, making a cruise-ship reservation, providing a pilot's license, etc."

- "When the government develops a credible new concern about a possible terrorist methodology – the intent to use a hazmat tanker in suicide attacks, for example, or scuba attacks against a specific port – it should be able to selectively request and receive data sets of specific interest associated with the threat. For example, it should be able to compare a list of persons with hazmat or scuba licenses against watch lists or other data sets that may give rise to concerns, such as travel, origin, or communications with foreign countries that are sources of terrorism, association with other terrorism suspects, and the like."

- "The government should be able to respond to reports of a particular mode of attack (for example, a plan to use chlorine tanker trucks to attack office buildings in several cities) by gaining access within four hours to private sector data relating to the status of that mode (for example, to obtain available information from industry sources about the location, status, drivers, and contact information for chlorine tankers)."

- "The U.S. should be able to determine the past history – cargo and itinerary – of containers bound for its ports, and should be able to identify suspicious patterns before those containers reach American waters."

- "Financial institutions conducting anti-money-laundering reviews should be able to identify account holders whose finances reflect such indicia of concern as irregular deposits from overseas. It should also be possible to review the background of such account holders on a rapid basis for other indicia of concern."

- "The government should have the ability to locate critical infrastructure nodes in the vicinity of an attack within five minutes – pipelines, power-generation plants and transmission lines, communications facilities, transportation, and the like."

All of these challenges could be met within 18 months if the government were prepared to make the commitment to do so. So far, Congress and the Executive Branch have not made that commitment. Indeed, for reasons I will get into shortly, we seem to be moving further from this goal, not closer.

b. Preventing abuses. One of the concerns, of course, is privacy and civil liberties. If these tools are provided to government investigators, how can we reduce the risk that they will be misused?

In fact, information technology also provides tool that can make abuse less likely. I will highlight three technologies worth considering for this purpose.

Anonymization. The development of public key cryptography and one-way hashing over the past quarter-century has enabled people to share data while still controlling the conditions of access. To take a simple example, one-way hashing permits two owners of lists to encrypt their lists, compare them, and identify all of the items that are on both lists – without either one learning anything else about the contents of the other's list.

It is easy to see how this technology could serve both privacy and security in the fight against terrorism. A list of terrorism suspects is highly sensitive. It should not be posted on every police station bulletin board in the country. Nor is there a need for every traffic stop in the country to be entered in real time into a central database in Washington. Yet it would be immensely valuable for local police to be able to check their traffic stops against a list of known terrorism suspects and to receive guidance if they have stopped someone of terrorism concern. Anonymization would address this problem. The federal list could be distributed without fear that it will be browsed by local police for improper purposes. And traffic stop data could be encrypted and compared to the list without being shared with Washington.

A similar approach could be taken to airline passenger data. The government does not need access to the travel records of millions of Americans or even foreign visitors, so long as it can gain access to the data to look for suspicious persons or patterns. Again, if airlines and the federal government use one-way hashing to produce lists that can be compared for overlapping entries, privacy is preserved until a match is found.[4]

Two points are worth making about this technology. First, it serves the goal not just of privacy but of counterterrorism as well. Of course, it provides protection against a local or federal official who simply wants to snoop on some private citizen's affairs. But it also protects against the possibility that an Al-Qa'ida sympathizer working part-time for a local sheriff might pull down the list to see which Al-Qa'ida operatives are on it and which are safe from scrutiny. In this case, good privacy policy is good operational security.

Second, this is new technology. It should not be overdeployed without careful testing. For example, one-way hashing only reveals matches when the data on the two lists are identical, right down to the punctuation and capitalization. This means that typos

[4] Attached to this testimony is a paper I recently prepared on anonymization, concluding that such a system would meet also the stringent data protection requirements of the European Union. *See* Attachment B.

and misspellings – things that would be easily ignored if the plaintext were read by humans – can defeat the matching process. So the technology only works when the data on both sides of the process are subject to careful quality control and a standard set of data-entry rules (e.g., always "MN," not "Minnesota"). This and other possible surprises mean that we should not make deployment of data-searching tools dependent on the simultaneous deployment of privacy tools. Instead, we should cautiously and incrementally launch the capabilities as they become field-ready and field-tested.

Electronic audit. Widespread hacker, worm, and virus attacks on computer networks have had one good effect on the technology world. Venture capitalists have recognized the need for security tools and have funded a host of new technologies designed to monitor network activity and identify users whose patterns of use change suddenly or violate existing policies. In addition, aggressive steps are being taken by PC hardware and software makers to assure network administrators that they can track and control activity on networks with far greater precision than was possible a few years ago.

These tools can be used to ensure accountability on the part of antiterrorism investigators. Every time an investigator conducts a search of a database made available to the authorities, that search can be logged, timestamped, and preserved. If the data is later misused, everyone who accessed the data can be identified, and if they passed it on to others, that transaction can also be tracked. For once, there is an answer to the classic question, "Who will guard the guards themselves?" The logs will. And any auditor authorized to use the logs will be able to identify and discipline those who misuse their access to the data.

In contrast to the last technology discussed, I see fewer reasons to be cautious about rapid deployment of electronic audit technology. It operates in the background and does not prevent access to data. What's more, it also serves multiple purposes. It allows auditors to follow up on privacy invasions by investigators, but it also allows them to look for other misdeeds, such as Al-Qa'ida sympathizers or foreign agents seeking information about the state of our terrorism knowledge. If the FBI had had good electronic audit capabilities in the 1990s, Robert Hanssen's spying on behalf of Russia and the Soviet Union could have been identified far earlier.

Rules-based access control. Finally, again thanks to the wave of network security research over the past several years, it is also possible to establish and enforce a variety of rules determining which network users have access to what data. Every user can be uniquely identified, and his network privileges can be restricted on the basis of his attributes. Again, such technology can be used to improve both security and privacy. Local officials without security clearances can be given access to unclassified data while FBI field agents with Secret clearances get access to additional data, and analysts with Top Secret clearances get access to even more. Similarly, investigators could be given access to a large body of data only under privacy protective limits – they could, for example, be given access to records about funds transferred from terrorist havens to the

United States but not to the names and associated account numbers without some special showing of suspicious behavior.

This technology has promise. The most effective way to maintain investigators' concern about data privacy is to give them individualized reminders that the privacy implications of their activities are being scrutinized. But the technology also carries risks. It is dangerous, as I will discuss shortly, to write rules that prevent investigators from seeing potentially critical data simply to prevent theoretical abuses. Consequently, I would deploy these rules-based technologies, not to deny access but to require further information from the investigators. Rather than restrict access to the names of accountholders in the example above, the system could instead display a pop-up window requiring a one-sentence explanation of why the investigator needs the data. That explanation could be logged and audited as well, but the more important effect may be the reminder to the investigator that the system is tracking any activity with privacy implications.

2. Rules

I said that it is dangerous to write rules restricting access to data based on theoretical fears of abuse. Let me be more plain. The reason we could not find al-Mihdhar and al-Hazmi in August of 2001 was not just that we didn't have enough tools. It was that we had imposed far too many rules on antiterrorism investigators – rules designed to protect against privacy abuses were mainly theoretical.

In fact, we missed our best chance to save the lives of three thousand Americans in August because we were spending more effort and imagination guarding against those theoretical privacy abuses than we spent guarding against terrorism. I feel some responsibility for sending the government down that road. Having gone down it once, though, we know where it leads – to death on our shores in numbers we can hardly fathom. And yet I fear that we are already starting down that road again.

a. How the rules failed us. Let me go back to the two and a half weeks that began in August 2001. It is true that the agents looking for al-Mihdhar and al-Hazmi didn't have the computer access they needed to do the job alone. But if this was a job for shoe leather and contacts, why not ask for help from the Bureau's criminal investigators – who had plenty of shoe leather and contacts and who outnumbered the counterintelligence agents three to one? Or from state and local police officers, who number more than a million? If those resources had been tapped, it's likely that al-Mihdhar and al-Hazmi would have been located quickly even without sophisticated new tools, and we would have had a fighting chance to roll up the rest of the plot as well.

Why didn't the New York agent use those resources? It was not for lack of trying. He fought for the help, and he was turned down flat. Acting on legal advice, FBI headquarters refused to involve any criminal agents: "If al-Midhar is located, the

interview must be conducted by an intel[ligence] agent. A criminal agent CAN NOT be present at the interview. This case, in its entirety, is based on intel[ligence]. If at such time as information is developed indicating the existence of a substantial federal crime, that information will be passed over the wall according to the proper procedures and turned over for follow-up criminal investigation."[5]

It breaks my heart to read this exchange. The agent in New York protested the ban on using law enforcement resources in eerily prescient terms. "[S]ome day someone will die – and wall or not – the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the [lawyers who gave the advice] will stand behind their decisions then, especially since the biggest threat to us now, UBL [Usama Bin Laden], is getting the most 'protection.'"[6]

The "wall" between intelligence and law enforcement was put in place to protect against a theoretical risk to civil liberties that could arise if domestic law enforcement and foreign intelligence missions were allowed to mix. In fact, in 1994, after I left my job as General Counsel to the National Security Agency, I regret to say that I defended the wall for just that reason, arguing that it should be left in place because foreign "[i]ntelligence-gathering tolerates a degree of intrusiveness, harshness, and deceit that Americans do not want applied against themselves."[7] I recognized then that the privacy risks were still just theoretical, but proclaimed the conventional wisdom of the time: "However theoretical the risks to civil liberties may be, they cannot be ignored."[8] I foresaw many practical problems as well if the wall came down, and I argued for an approach that "preserves, perhaps even raises, the wall between the two communities."[9]

I was wrong, but I was not alone in assigning a high importance to theoretical privacy risks. In fact, over the 1990s, the wall grew higher and higher, well beyond anything I could have imagined. Indeed, in 2000 and 2001, as Al-Qa'ida was slowly bringing its September 11 plans to fruition, the FBI office that handled Al-Qa'ida wiretaps in the U.S. was thrown into turmoil because of the new heights to which the wall had been raised. The special court that oversees national security wiretaps, known as the Foreign Intelligence Surveillance Act, or FISA, Court, had ordered strict procedures to ensure that its intelligence wiretaps were not contaminated by a law enforcement purpose. When those procedures were not followed strictly enough, the court barred an

---

[5] Joint Intelligence Inquiry Report at 153.

[6] *Id*.

[7] *Should Spies Be Cops?* 97 Foreign Policy 36, 40 (Winter 1994-95). *See* Attachment C.

[8] *Id*.

[9] *Id*. at 47.

FBI agent from the court because his affidavits did not fully list all contacts with law enforcement. In the spring and summer of 2001, with Al-Qa'ida's preparations growing even more intense, the turmoil apparently grew so bad that numerous national security wiretaps were allowed to lapse.[10]

Let me say that again. It is a shocking statement. In the months before the worst foreign attack on our nation in history, one of our best sources of information was allowed to lapse – something that had never happened before in the history of the program. It isn't clear what intelligence we missed as a result of that lapse. But it does seem clear that the loss of those wiretaps was treated as less troubling than the privacy scandal that now hung over the antiterrorism effort.

Knowing how such matters are usually handled, I'll wager that the agent who provoked the FISA Court's wrath was being measured for disciplinary action and perhaps even a perjury indictment. And the Joint Intelligence Committee Inquiry has concluded that the lesson was not lost on the rest of the office: "FBI personnel involved in FISA matters feared the fate of the agent who had been barred and began to avoid even the most pedestrian contact with personnel in criminal components of the Bureau or DOJ because it could result in intensive scrutiny by OIPR [the Justice Department office that reviewed national security wiretaps] and the FISA Court."[11]

Against this background, it's easy to understand why FBI headquarters and its lawyers refused so vehemently to use law enforcement resources in the effort to find al-Mihdhar and al-Hazmi. To do so would be to risk a further privacy scandal and put their careers in jeopardy. Viewed in this light, the New York agent's fight to get law enforcement involved looks like an act of courage that borders on foolishness.

We can all be thankful for his zeal. But in the end, one agent's zeal was not enough to overcome the complex web of privacy rules and the machinery of scandal that we built to enforce those rules.

He lost. And on the 11th, so did we all.

b. Lessons from the failure. What lessons can we learn from this tragic unfolding of events? I would offer two.

First, we must admit that the source of this tragedy was not wicked or uncaring officials. The wall was built by smart, even wise, professionals who thought they were acting in the country's and their agency's best interest. They were focused on the

[10] Joint Intelligence Inquiry Report at 153.

[11] *Id*.

theoretical privacy risks that would come if foreign intelligence and domestic law enforcement were allowed to mix, and by a fear that in the end the courts and Congress would not understand if we put aside those theoretical concerns to combat a threat that was both foreign and domestic. They feared, and with good reason, that years of successful collaboration would end in disaster if the results of a single collaboration could be painted in the press and public as a privacy scandal. To protect against that possibility, they drafted ever more demanding rules – created an ever-higher wall – to govern operations at the border between domestic law enforcement and foreign intelligence.

As drafted, the rules still allowed antiterrorism investigators to do their jobs – at least in theory. The drafters counted on the fierce determination of law enforcement and intelligence agents to accomplish their mission. They weren't wrong. The New York agent's determination is palpable. But even if he could in theory have found a route through the maze of rules, it was the FISA court scandal that finally choked off any practical hope of getting that job done. No one at headquarters wanted to thread that needle. No one wanted to find a way to say "yes" to the New York request, because they knew that that kind of creativity was likely to end in disgrace.

And so the first lesson is that, with the best will in the world, we cannot write rules that will both protect us from every theoretical risk to privacy and still allow the government to protect us from terrorists. We cannot fine-tune the system to perfection, because systems that ought to work can fail, as this one did so catastrophically in August of 2001. That is why I am so profoundly skeptical of efforts to write new privacy rules to go on top of all the rules we had in August 2001, and why I would rely instead on auditing for actual abuses. Now we know that the cost of protecting against theoretical risks to privacy can be thousands of American dead. That cost was too high. We should not again put American lives at risk for the sake of some theoretical risk to our civil liberties.

And now to the second lesson. Perhaps it isn't fair to blame all the people who helped to create the wall for the failures that occurred in August of 2001. No one knew then what the cost of building that wall would be.

But now we do know. Or at least we should. We should know that we can't prevent every imaginable privacy abuse without hampering the fight against terror. We should know that an appetite for privacy scandals hampers the fight against terror. And we should know that, sooner or later, the consequence of these actions will be more attacks and more dead Americans, perhaps in numbers we can hardly fathom.

We should know that. But somehow we don't. The country and its political leaders have had more than two years to consider the failures that occurred in August 2001 and what should be done to correct them. These were failures bad enough for people to lose their jobs over. But only one man has been forced out in those two years.

Adm. John Poindexter. He tried to build information technology tools (including privacy tools) to address the failings of August 2001. But he was enmeshed in a "scandal" over privacy abuses that were entirely theoretical – when they weren't simply false. And so he and his program went the way of the TIPS program, also killed because of theoretical privacy worries. Next up for the same treatment are Section 215 of the USA PATRIOT Act, attacked for allowing library searches that, it turns out, have never occurred, and CAPPS II, designed to use information that will improve airline security while reducing the humiliating searches that now occur at airports around the nation but attacked because it poses a theoretical risk of abuse by airport security officials.

Libertarian Republicans have joined with civil-liberties Democrats to teach the law enforcement and intelligence communities the same lesson that FBI headquarters taught its New York agent in August 2001. You won't lose your job for failing to protect Americans, but if you run afoul of the privacy lobby, you're gone.

And so, the effort to build information technology tools to find terrorists has stalled. No one wants to be the next John Poindexter. Worse, the wall is back. Intelligence experts in the Terrorist Threat Integration Center (TTIC) have been barred from examining law enforcement reports due to an overly cautious (and scandal-haunted) reading of the executive order that creates a charter for the intelligence community.[12]

In short, bit by bit, we are again creating the political and legal climate of August 2001.

And sooner or later, I fear, August will again lead to September.

[12] See Executive Order 12,333 (1981).

ATTACHMENT A

Stewart A. Baker
Tel 202.429.6413
Direct Fax 202.261.9825
sbaker@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
Tel 202.429.3000
Fax 202.429.3902
steptoe.com

Stewart A. Baker was described by *The Washington Post* (November 20, 1995) as "one of the most techno-literate lawyers around." His practice includes issues relating to privacy, data protection, computer security, electronic surveillance, national security, encryption, digital commerce, and export controls. He has advised hardware and software companies on US export controls and on foreign import controls on encryption. In October 2000, he was named to the Washington "Power 100" by Regardie's magazine for his work in this field. He also represents major telecommunications equipment manufacturers and carriers in connection with the Communications Assistance for Law Enforcement Act ("CALEA") and law enforcement intercept requirements. In the area of authentication and digital signatures, his clients include major banks, mortgage companies, and credit card associations, as well as technology companies.

Mr. Baker is the former General Counsel of the National Security Agency (1992-1994) and author of the book, *The Limits of Trust: Cryptography, Governments, and Electronic Commerce* (1998), as well as various other publications and articles on electronic commerce and international trade. Earlier in his career, Mr. Baker served as Law Clerk to John Paul Stevens, US Supreme Court (1977-78), Frank M. Coffin, US Court of Appeals, First Circuit (1976-77), and Shirley M. Hufstedler, US Court of Appeals, Ninth Circuit (1975).

Mr. Baker has been named to numerous US government and international bodies dealing with electronic commerce and related topics, including: President's Export Council Subcommittee on Export Administration (2003); Markle Foundation's Task Force on National Security in the Information Age (2002-present); Defense Science Board's Task Force on Information Warfare (1995-1996; and 1999-2001); Federal Trade Commission's Advisory Committee on Online Access and Security (2000); President's Export Council Subcommittee on Encryption (1998-2001); Free Trade of the Americas Experts Committee on Electronic Commerce (1998-present); UNCITRAL Group of Experts on Digital Signatures (1997-2001); OECD Group of Experts on Cryptography Policy (1995-1997); International Telecommunication Union Experts Group on Authentication (1999); American Bar Association Standing Committee on Law and National Security (1998-present); American Bar Association Task Force on International Notarial Issues (1996-1998); International Chamber of Commerce Working Party on Digital Authentication (1996-1998); International Chamber of Commerce Group of Experts on Electronic Commerce (1996-present). In addition to his private clients, Mr. Baker has also been retained as a consultant on computer security issues by a variety of international bodies, including the ITU, the OECD, and the Government of Japan.

ATTACHMENT B

STEPTOE & JOHNSON LLP
ATTORNEYS AT LAW

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
Tel 202.429.3000
Fax 202.429.3902
steptoe.com

ANONYMIZATION, DATA-MATCHING AND PRIVACY: A CASE STUDY

Stewart Baker
Kees Kuilwijk
Winnie Chang
Daniel Mah

December 2003

One of the challenges posed by terrorism is how to catch or foil terrorists without sacrificing the democratic values that the terrorists are attacking. One promising tool is the use of modern data processing to correlate the large amounts of information generated or collected by private industry. Properly marshalled and processed, such data holds the promise of identifying suspicious actors and activities before they coalesce into an attack. At the same time, the use of such capabilities raises concerns about privacy and the possible misuse of the capabilities for purposes other than foiling terrorism. The thesis of this paper is that cryptography and related technologies will allow democratic nations to make effective use of data-processing capabilities while dramatically reducing the risk of misuse. In particular, advanced techniques for "anonymizing" personal data will help to preserve privacy while obtaining the many benefits of data processing technology.

This is not simply a philosophical question. Protection of privacy and personal data are enshrined in law by most democracies. For that reason, any effort to use private data in the fight against terrorism must pass legal muster. This paper examines the extent to which sophisticated anonymization techniques can resolve some of the most difficult conflicts between privacy and security.

We sought to test our thesis by examining a particularly intransigent problem under particularly strict data protection rules and chose the CAPPS II dispute between the United States and the European Union over the sharing of passenger information possessed by airlines. CAPPS II provides a good case study for demonstrating the uses of anonymous data matching technology because it implicates the EU Directive on data protection, arguably the most rigorous and broadly applicable standard for the protection of personal data anywhere in the world today.

I. Introduction and Summary

The United States and European Union are engaged in difficult negotiations concerning the transfer of Passenger Name Record ("PNR") data from EU airlines to the U.S. government for the purposes of detecting and preventing possible terrorist and other criminal activity. The underlying problem is that the United States would like to be able to search a large volume of PNR data for terrorism and other criminal suspects whom it has identified from a variety of intelligence and law enforcement sources. While there is little doubt that specific information about individual suspects could be transferred to the U.S. pursuant to an exception to the EU data protection laws, the U.S. cannot send such a sensitive list to a large number of companies. Instead, it needs to be able to search for the names by comparing its list to a list of all passengers. This would give the U.S. government access to the PNR data of numerous ordinary passengers in whom the U.S. has no law enforcement or national security interest. This creates a conflict between the legitimate needs of the U.S. government and EU data protection laws designed to preserve the privacy of EU citizens.

This paper considers whether the CAPPS II issues can be resolved through the use of anonymization and anonymous data matching technology. Under our proposal, the airlines would provide anonymized PNR data to a trusted third party intermediary who would then match that data against a similarly anonymized list of suspects provided by the U.S. government. Only if this "blind" process yielded a match would information about particular passengers be revealed to the U.S. government. We conclude that the anonymous matching process outlined above (or some variant thereof) meets the stringent requirements of the data protection laws of the EU, including the data protection laws of four of its Member States – Germany, Spain, France, and the United Kingdom.

In summary, under the EU Directive and the data protection laws of these four Member States:

- PNR data that have been anonymized so that the person who possesses the data cannot easily identify the individuals involved is no longer "personal data" that is subject to the EU data protection laws.

- As a result, the transfer of such anonymized PNR data to the United States is not subject to the restrictions on cross-border data transfers under those laws, provided that the recipient in the United States cannot easily de-anonymize the data upon receipt.

- Even if the transferred data could be easily de-anonymized by the Unites States, the transfer would be permissible if it was "necessary or legally required" to transfer that information "on important public interest grounds." This would likely be the case for information about suspected terrorists (and possibly other serious criminal offenders).

- Finally, the process of anonymization might itself be "data processing" that is subject to the EU data protection laws, but no additional notice or consent is required before PNR data may be anonymized.

This analysis suggests that a properly designed and implemented system of anonymization and anonymized data processing has real promise in the effort to use modern technology to provide protection against terrorism without sacrificing privacy. In particular, anonymization could solve the

current deadlock over CAPPS II and the sharing of PNR data. The system would have to ensure that anonymized PNR data is not received in the United States by anyone who could easily rediscover the identities of the individual passengers, and limit the transfers of identifiable information or data that could be de-anonymized to only that which is necessary "on important public interest grounds."

II. Background and Context

A. U.S.-EU Debate Over Passenger Data Transfers – CAPPS II

The U.S. Aviation and Transportation Security Act of 2001 introduced the requirement that airlines operating passenger flights to, from or through the United States, provide the U.S. Customs and Border Protection Bureau ("CBP"), upon request, with electronic access to PNR data contained in their reservation and departure control systems.

From a European legal standpoint, EU airlines may not transfer personal data from the EU to a non-EU country that does not provide an "adequate level of protection" for such data. The European Commission has raised the data protection concerns in bilateral contacts with the United States. On February 18, 2003, the European Commission and CBP issued a Joint Statement reflecting an interim agreement under which it became possible for airlines to transfer personal data of passengers to the United States. Since early March 2003, the United States government has been collecting PNR data from U.S.-bound flight passengers from the EU.

The two sides agreed to work together towards a final bilateral arrangement to reconcile U.S. requirements with the requirements of data protection law in the EU. Several rounds of talks have taken place, but the interim agreement has come under attack from the European Parliament and the data protection agencies of the Member States.

Any final agreement with the U.S. will have to address the new U.S. passenger filtering system. This Computer Assisted Passenger Pre-Screening ("CAPPS II") system is due to be launched in 2004. CAPPS II will be used to cross-check a set of data so as to "weigh" the risk of each airline passenger. The European Parliament has particularly raised concerns about providing data for the CAPPS II system, fearing that data would be circulated on an even wider scale than is currently the case.

B. Current Major Open Issues in the Debate

At the time of writing, press reports indicate that disagreement remains on several issues in particular. The Commission reportedly is concerned about the purposes for which the data may be used. The U.S. wants to use the data not only for combating terrorism but also for combating "other serious criminal offenses," such as narcotics offenses and money laundering, which sometimes have been linked to terrorism. The EU considers the phrase "other serious criminal offences" to be too vague to be a limitation on the kinds of investigations that could be conducted with PNR data. Also, some disagreement remains on whether and to what extent "sensitive" information (*e.g.,* religious or health information) needs to be transferred.

In addition, discussions have focused on the length of time that the data will be available to the U.S. authorities. Currently, the U.S. seeks access for seven years, while the Commission is seeking to limit archiving to a period of three years.[1]

Finally, the U.S. has not fully resolved concerns about remedies for passengers in cases where errors may have been made. Any passenger who wants to review his personal data will be able to do so, and a chief privacy officer has been appointed in the department that handles these issues. However, the EU is seeking further assurances. Since no formal procedures have been established with regard to access to data, the EU believes the rights of data subjects are not sufficiently protected.

C. Anonymization and Anonymous Data-Matching as a Possible Solution

"Anonymization" is a recognized method for dealing with personal data in the U.S. and EU alike. It has spawned technical approaches that can be quite sophisticated. For example, some anonymization technology uses cryptographic methods to transform identifying information using a "one-way hash function," which converts a record to a character string that serves as a unique identifier (like a fingerprint). Correctly implemented, anonymization would make it extremely difficult to extract the person's identity from the anonymized information. Such a system can be particularly useful in determining whether the same name appears on two lists owned by different parties that do not wish to share the lists themselves. Thus, by using such technology, it would be possible for EU airlines to provide a list of passengers and to have that checked against a list of U.S. government terrorism suspects without the airlines seeing the U.S. list or the U.S. government seeing the airlines' list. To ensure that the data matching is truly "blind," the anonymized data could be provided by each party to a trusted intermediary with no access to the original data. Only if there was a match would any personal data of any kind be provided to the U.S. government.

Use of anonymization and anonymous data-matching technology could help eliminate many of the issues in the current U.S.-EU dispute. A properly designed and implemented system would (i) allow the data-matching to be conducted without disclosing the identities of the vast majority of passengers in the data set, and (ii) limit disclosures of personal data to the U.S. to information about passengers who appear or are closely associated with individuals on the U.S. list of suspects. Transfers of personal information about passengers on the suspect list to the U.S. would ordinarily be justified under the recognized "public interest" exception to the EU restriction on personal data transfers.

III. EU Data Protection

The European Union's Data Protection Directive[2] lays down rules regarding the protection of the "personal data" of EU citizens. The two aspects of the EU Directive that are of concern here are the

---

[1] This is most likely because three years is the term granted by the Computer Reservation System ("CRS") Regulation. Regulation (EEC) No. 2299/89 on computerized reservations systems, as amended by Regulation (EC) No. 323/1999. Under Article 6(1)(a), personal data have to be taken off-line within 72 hours of the completion of the booking (*i.e.*, flight arrival), can be archived for a maximum of three years, and access to the data is allowed only for billing-dispute reasons.

rules on transfers of personal data outside of the EU and principles for the "processing" of personal data.[3]

A. Restrictions on Transfers of Personal Data Outside of the EU

Articles 25 and 26 of the EU Directive prescribe restrictions on the transfer to countries outside the EU of "personal data" that are subject to processing or which are intended to be processed in other countries outside the EU after being transferred. Data transfers to non-EU countries that do not offer an "adequate level of protection"[4] are only permitted in certain defined situations, for example:

- when the data subject has given his or her unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or is at the request of the data subject;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interest of the data subject; or
- when a binding contract protecting the exported data, or a similar binding arrangement, such as the EU-U.S. Safe Harbor[5] arrangement, is in place.

---

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EU Member States were required to bring their existing domestic laws, regulations and administrative provisions relating to data protection in compliance with the Directive at the latest by October 24, 1998. Not all Member States succeeded in doing so before this deadline, but currently only France has not yet fully implemented the Directive.

[3] The European Commission has competence to address any external relations questions arising under the Directive, such as cross-border data transfers to non-EU countries. Specifically in the area of airline passenger data transfers, the Commission also has responsibilities under the CRS Regulation. The Regulation provides a code of conduct for computerized booking systems, and contains data protection provisions in Article 6. Article 11(1) of the Regulation provides that: "Acting on receipt of a complaint or on its own initiative, the Commission shall initiate procedures to terminate infringement of the provisions of this Regulation."

[4] The Council and the European Parliament have given the Commission the power to determine, on the basis of Article 25(6) of Directive 95/46/EC whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. The Commission has so far recognized Switzerland, Hungary, the U.S. Department of Commerce's Safe Harbor Privacy Principles, Canada, and Argentina as providing adequate protection.

[5] The Safe Harbor is an arrangement between the EU and the U.S. which provides a way for U.S. companies that are not subject to Directive 95/46/EC to nonetheless provide "adequate" privacy protection, as defined by this Directive. This means that personal data can be transferred from the EU to U.S. companies that have signed up to Safe Harbor even though the U.S. as such is not recognized as providing adequate protection. To benefit from Safe Harbor companies must comply with seven specific privacy principles. *See*

The data protection laws of the Member States considered in this paper treat transfers of personal data to non-EU countries in similar ways.

B. Restrictions on Processing of Personal Data Without Consent (or Other Appropriate Basis) and Notification Requirements

The Directive also stipulates that any processing of personal data must be lawful and fair to the individuals concerned (the "data subjects"). The data kept by "data controllers" (*e.g.*, airlines) must be adequate, relevant and not excessive in relation to the purposes for which they are processed.[6] In order to be lawful, any processing of personal data must be carried out with the "unambiguous consent" of the data subject or, alternatively, must be "necessary" on certain specific grounds – for example:

- necessary to perform a contract binding on the data subject, or to take steps at the request of the data subject prior to entering into a contract; or
- necessary for compliance with a legal obligation to which the controller is subject; or
- necessary in order to protect the vital interests of the data subject; or
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (except where such interests are overridden by the data subject's privacy rights).[7]

The data protection laws of all Member States considered in this paper (Germany, United Kingdom, Spain, and France) include similar provisions.

More stringent rules apply to the processing of "sensitive data" which are defined by the Directive as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership," and data "concerning health or sex life." In principle, such data can only be processed with the data subject's "explicit" consent or in very specific circumstances, such as where the processing of data is mandated by employment law, or where it may be necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable

---

http://www.export.gov/safeharbor for information on the Safe Harbor arrangement and the companies that have joined it.

[6] Art. 6 of the Directive.

[7] Art. 7 of the Directive.

of giving his consent.[8] The data protection laws of the Member States considered in this White Paper define and treat "sensitive data" in essentially the same way.

In addition, the EU Directive requires the data controller to notify the data subject of certain information when collecting personal data, including the identity of the data controller, the purposes of the processing for which the data are intended, and recipients or categories of recipients of the data, unless the data subject already has this information.[9]

IV. Analysis

A. Anonymized PNR Data is not "Personal Data"

Once PNR data has been anonymized, it is no longer "personal data" and thus no longer subject to the restrictions on processing or transfers of personal data in the EU Directive and data protection laws. The issue that may be disputed, however, is whether the data has been sufficiently "anonymized" so that the individuals involved cannot be identified.

"Personal Data" and Identifiability. The Directive and national laws show remarkable consistency in defining personal data. The Directive defines "personal data" as: "any information relating to an identified or identifiable natural person ("data subject")." An identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[10] Recital 26 of the Data Protection Directive states that: "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." The data protection laws of the Member States considered in this paper define "personal data" in essentially the same way.[11]

---

[8] Art. 8 of the Directive.

[9] Art. 10 of the Directive.

[10] Art. 2(a) of the Directive.

[11] The German Data Protection Act defines "personal data" as "any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)." *See* German Data Protection Act, Sec. 3(1). The United Kingdom defines personal data as "data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual." *See* UK Data Protection Act, Sec. 1(1). In Spain, personal data means "any information concerning identified or identifiable natural persons." *See* Spanish Data Protection Act, Art. 3(a). In the draft French law, personal data included "all information with regard to an identified natural person or one that can be identified, directly or indirectly, by reference to an identification number or by one or several elements that are his. To determine whether a person is identifiable one needs to consider all means that can be reasonably employed either by the data controller or by a third person." *See* French Draft Data Protection Act, Art. 2(2).

In other words, data that cannot be used to identify a particular individual is not "personal data." Accordingly, if personal data have been stripped of all personal identifiers such that the data can no longer be used to identify the data subject, then the data will cease to be personal data, and non-personal data are not subject to the EU Directive and data protection laws.

Anonymization. This reasoning is confirmed by Recital 26 of the Data Protection Directive which states that: "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable." Similarly, the data protection laws of the Member States considered in this paper all address the issue of anonymization.

Most of the EU members considered here take the view that anonymized data are not personal data and that their data protection laws do not restrict the processing of such data. The Spanish Data Protection Act refers to anonymization (literal translation: "depersonalization"), which it defines as: "any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person."[12] Article 11, the basic provision on data processing, stipulates that "personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject," or for a limited number of other legitimate reasons.[13] But Article 11(6) explicitly provides that "if the communication is preceded by a depersonalization procedure, the provisions of the preceding paragraphs shall not apply." In other words, anonymized data can be freely processed.

Similarly, under the French (draft) Data Protection Act, most forms of data processing are excluded from the application of the Act where the processing is preceded by an "anonymization procedure" that has been approved by the French Data Protection Agency (the "CNIL").[14] While the CNIL has not yet established official standards for approved anonymization procedures, it has previously expressed a view (in a related context) that techniques such as hashing ("hachage") or encryption are recognized methods for handling medical data.[15]

The United Kingdom and Germany take a less categorical approach but come to the same conclusion. The guidance issued by the UK data protection authority provides that "whether or not data which have been stripped of all personal identifiers are personal data in the hands of a person to whom they are disclosed, will depend upon that person being in possession of, or likely to come into possession of, other information, which would enable that person to identify a living individual."[16]

---

[12] Spanish Data Protection Act, Art. 3(f).

[13] Spanish Data Protection Act, Art. 11(a)-(f).

[14] Art. 8:IIbis and Art. 32:IIbis of the French (draft) Data Protection Act.

[15] Recommendation n° 97-0008 (Feb. 4, 1997)

[16] U.K. OFFICE OF THE INFORMATION COMMISSIONER, DATA PROTECTION ACT 1998 LEGAL GUIDANCE 14, *available at* http://www.informationcommissioner.gov.uk (last visited Nov. 26, 2003) ("U.K. LEGAL GUIDANCE").

What matters to the UK authority, in other words, is the data controller's ability to identify the data subject, not its intent to do so.[17]

The German Data Protection Act also defines anonymization (literal translation: "depersonalization") as: "the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual."[18] The Act does not require elaborate technological guarantees against matching data with names. Nor does it take the strict UK view adopted that what matters is a controller's ability to recombine the anonymized data. It provides that data may be processed without data protection obligations where "the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual" are "stored separately."[19]

When is data anonymized? This raises the question of when personal data is anonymized. Unfortunately, as the discussion above suggests, there is no clear standard. Some countries, like Germany and the UK, put an emphasis on the separate storage of information capable together of identifying individuals. Other countries make reference to how easily a person in possession of the anonymized data can use "reasonable efforts" to identify a person. In the words of the Directive, "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."

The strictest view, taken by the UK Guidance Notes, suggests that if a person possesses both the anonymized data and the original data set, all of the data (even the anonymized data) remains personal data. Where this strict view prevails, it might be further argued that the transfer even of anonymized data by an entity that also holds the original data set is still subject to the cross-border data transfer restrictions in the EU Directive. However, this is an unduly strict reading of the data transfer restrictions. In ordinarily usage, the "transfer" of personal data connotes the combined acts of sending *and* receiving data. So, even if anonymized data remains "personal data" in the hands of the person that sends the data, there is no "transfer" of that data if no personal data are received by the entity at the other end of the line.

In short, even in jurisdictions that treat anonymized data as personal data while in the possession of entities that have the ability to "de-anonymize" the data, it is unlikely that those entities are "transferring" personal data when they convey the data to a party that cannot de-anonymize the data. Finally, even if this were viewed as a transfer of personal data, the anonymization process could easily be tailored to eliminate any doubt, simply by using a trusted intermediate party. That is, the airlines

---

[17] "The fact that the data controller is in possession of the original data set which, if linked to the data that have been stripped of all personal identifiers, will enable a living individual to be identified, means that all the data (including the data stripped of personal identifiers), remain personal data in the hands of the data controller and cannot be said to have been anonymised. The fact that the data controller may have no intention of linking these two data sets is immaterial." *Id.* at 13.

[18] German Data Protection Act, Sec. 3(7).

[19] German Data Protection Act, Sec. 30(1).

could retain the original data set while giving anonymized data to an intermediary in the EU. Provided that the intermediary cannot access the original data set, it would not be a data controller in possession of personal data. The export of the anonymized data by the intermediary would not then be subject to the cross-border data transfer restrictions in the EU Directive and data protection laws.[20]

B. Transfers of Anonymized PNR Data Outside of the EU Are Not Transfers of Personal Data, Provided the Recipient Cannot Easily De-anonymize the Data

Because anonymized data, at least in the hands of an intermediary, are not "personal data," anonymized data are no longer subject to the EU restrictions on transfers of such data to non-EU countries that do not provide an "adequate level of protection" for personal data. There is a second reason for the use of an intermediary in the CAPPS II context. Remember that the use of hashing to anonymize the data is designed to allow the U.S. government to identify a "match" between data tied to terrorism suspects (names, phone numbers, credit cards, and the like) and similar data on passenger lists – all without gaining access to the identities of any other passenger. This means that, for a very limited group of passengers – terrorism suspects – the government may learn that a particular passenger has an important characteristic in common with someone on its terrorism suspect list. Whether this constitutes de-anonymization is open to question, but taking a strict view of the question, one might conclude that the personal data of persons associated with terrorism suspects (and only terrorism suspects) has been transferred to the U.S. government, at least if the transfer occurs directly.

Does this matter? We are inclined to doubt that it does. Even extreme advocates of data protection would not argue that a nation could not be alerted by the airlines when a terrorism suspect gets on a plane bound for that nation. In such a case, personal data would ordinarily be transferable under the EU Directive pursuant to the "necessary . . . on important public interest grounds" exception to the restriction on transfers. And in any event, because only the U.S. government has the ability to identify the terrorism suspects whose data has been matched, transfers to intermediaries do not transfer the personal data even of the terrorism suspects. In consequence, such transfers would seem to comply fully with EU law.

C. Anonymization is Data "Processing," But No Additional Notice or Consent Procedures are Required

As noted above, the last issue is whether the process of anonymization is itself data "processing" under the EU Directive and data protection laws. If so, then anonymization is only permissible with the data subject's "unambiguous consent" or if anonymization is "necessary" in the ways described in Section III.B. Anonymization might fall within the broad definition of "processing of personal data," but additional notice and consent of the passenger is not required.

---

[20] This is a variant on a proposal by the Austrian data protection agency for PNR data to be filtered through a short-term storage intermediary, whereby controlled access would then be permitted to foreign governments. The difference here is that the data intermediary would be a private entity located within the EU that would only hold the anonymized PNR data. The original personal data remains with the airline that collected it.

"Processing of Personal Data." The Directive defines "processing of personal data" as: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[21] The data protection laws of the Member States considered in this paper define "processing of personal data" in essentially the same way.

This broad definition suggests that anonymization, because it involves "alteration" or "erasure or destruction" of personal data may be data "processing" under the EU Directive. The guidance notes issued by the UK data protection authority state that "[i]n anonymizing personal data [a] data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the [Data Protection] Act."[22] This is implicit in the Spanish Data Protection Act as well, which refers to anonymization as "any *processing of personal data* carried out in such a way that the information obtained cannot be associated with an identified or identifiable person."

On the other hand, anonymization is a measure designed to improve the privacy of personal data and it seems strange to impose the notice and consent requirements of the Directive and data protection laws on a measure designed to increase the protection offered to personal data. Even in the UK, the Court of Appeal in *Regina v. Department of Health, ex parte Source Informatics Ltd.*[23] has expressed a view that the Directive should be construed purposively so that "anonymization" is not considered "processing" under the Data Protection Act.

Notice and consent requirements? If anonymization is not "processing of personal data," then the notice and consent requirements in the EU Directive and data protection laws will not apply. But even if anonymization constituted "processing of personal data," it is our view that no additional notice or consent is required before such processing can take place.

For non-sensitive data, additional notice and consent of the passenger is not required. First, anonymization actually improves the privacy of the passenger's personal data. Because anonymization will actually increase the protection of the data subject's personal data, it would be inappropriate to require data controllers to obtain prior consent before doing so. Second, the anonymization is necessary to comply with existing legal requirements, including the data security requirement as well as the obligation not to transfer personal data outside of the EU to countries without adequate safeguards. (Some would argue that compliance with U.S. law ought also to be considered under this heading, but data protection authorities have resisted this conclusion.) And finally, anonymization is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed," except where the passenger's privacy interests override.[24] Here, the legitimate

---

[21] Art. 2(b) of the Directive.

[22] U.K. LEGAL GUIDANCE, *supra* note 16, at 13.

[23] [2001] Q.B. 424.

[24] *See* Art. 7 of the Directive.

interests are the security of the data as well as the security and law enforcement interests of the U.S. and EU governments, the airlines, and the passengers themselves.

A different analysis is required for "sensitive data" (*i.e.*, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and information concerning health or sex life). In many cases, sensitive data may simply be excluded from the database. Such information is not routinely gathered in PNR data, although it might be argued that sensitive data could be inferred from a passenger's dietary preferences or wheelchair requests. But such information is, of course, provided initially with the consent of the passenger – it is the passenger's request after all – and for flights to the United States. Thus, the information almost by definition must be exported to that country, and in today's world it certainly must be subjected to electronic data processing. It is reasonable to conclude that the very act of requesting a particular type of meal or a wheelchair includes an explicit consent to the use of that information on an electronic network. It cannot be necessary to obtain a separate consent for each step in the electronic process – *e.g.*, transmitting to a server, populating a database, encrypting for security, transferring to a client from the server, etc. This is particularly true in the case of measures, such as encryption or anonymization, designed to protect the passenger's personal data. Indeed, the passenger has a right to expect the airline to keep his or her sensitive information secure, and anonymization is simply one means by which the airline can do so.

Finally, as to the notification requirement, the airline is required to inform the passenger of "the purposes of the processing for which the data are intended" unless the passenger already has this information. As with sensitive data, the passenger plainly knows that the airline will process the personal data that is collected and has a right to expect that it will be stored securely. Since anonymization is one means of ensuring the security of personal data, the passenger is already aware of the relevant purpose for which his or her personal data will be processed.

V. CONCLUSION

Terrorism poses one of the most difficult challenges facing democratic nations today – how to combat terrorism while protecting the privacy of ordinary citizens. On the one hand, modern data processing technology is a promising tool for combating terrorism. On the other hand, such technology raises privacy concerns and the possibility of misuse. These competing concerns are particularly evident in the current U.S.-EU deadlock over the sharing of airline passenger data. The analysis in this paper presents a possible solution to this deadlock in the form of a properly designed and implemented system of anonymization and anonymous data processing. By securely anonymizing personal data before it is processed by an intermediary, relevant data about suspected terrorists can be shared while fully complying with the strict privacy protections of the EU Directive on data protection. Thus, this technique of anonymizing personal data before the data is processed represents an important means in a wide variety of contexts by which benefits of data processing technology can be realized without sacrificing privacy.

ATTACHMENT C

FOREIGN POLICY

NUMBER 97 WINTER 1994–95 $7.95

97

SHOULD SPIES BE COPS?

by Stewart A. Baker

Like generals ready to fight the last war, bureaucrats excel at avoiding last year's scandal. Usually that does no harm. But every once in a while avoiding last year's scandal means sowing the seeds for next year's.

That is what is happening today in a strenuous but largely hidden struggle among the federal agencies that operate at the intersection of law enforcement and intelligence gathering. The struggle has come to a head as a result of the BNL affair. Also known as Iraqgate, the BNL affair centered on charges that the Justice Department and the CIA had covered up the Bush administration's channeling of prewar military assistance to Iraq through the Atlanta branch of Banca Nazionale del Lavoro, or BNL.

Though driven by recent headlines, the struggle has its roots in the late 1940s, when the American peacetime intelligence "community" was created to help fight the Cold War. American intelligence agencies were shaped by individuals who understood the mechanics of totalitarianism and wanted none of it here. They knew that the Gestapo and the Soviet KGB had in common a sweeping authority to conduct internal and external security and intelligence gathering. Determined not to become what they were fighting, the drafters of the 1947 National Security Act declared that the newly created CIA "shall have no police, subpena [sic], or law enforcement powers or internal security functions." The CIA's role was to deal with America's foreign enemies, not its domestic wrongdoers.

The drafters of that language were only being prudent. Combining domestic and foreign intelligence functions creates the possibility that domestic law enforcement will be infected by the secrecy, deception, and ruthlessness that international espionage requires. Dividing the responsibilities among different agencies reduces that risk. It also creates a tension between agencies that is itself a safeguard against abuse. It is surely no accident that the Russian democrats who helped break up the Soviet Union also stripped the KGB of its internal security duties—adopting, in essence, an American system of divided responsibility.

The irony, of course, is that the end of the Cold War has pushed U.S. policymakers in the opposite direction. A strict separation of intelligence from law enforcement proved workable enough while the Cold War continued. Apart from counterespionage work, there was little overlap between the two. The intelligence agencies had a desperate job to do abroad, but they faced a threat that was almost exclusively foreign. Law enforcement, by contrast, had few international dimensions and almost no way to address international criminal activity.

By the 1990s, much had changed. Because the Soviet Union was no longer a threat, some of the resources devoted to extracting its secrets could be turned to other tasks, to other foreign targets. But some of those foreign targets had a domestic tinge. As topics like international narcotics trafficking, terrorism, alien smuggling, and Russian organized crime rose in priority for the intelligence community, it became harder to distinguish between targets of law enforcement and those of national security.

Intelligence agencies were not alone in expanding their traditional beat. The Justice Department had gradually extended its reach into foreign affairs. If foreign heads of state could be indicted in the United States for acts committed while in office (as Manuel Noriega and Ferdinand Marcos were in the 1980s), almost any foreign policy problem could wind up as a criminal matter.

These were the practical responses of law enforcement and intelligence officials to changing times. As the 1980s wore on, the same practical officials began to see the admonition of the 1947 act as more a technicality than a guiding principle. Surely, the pragmatists ar-

STEWART A. BAKER, *a partner in the Washington, D.C., law firm of Steptoe & Johnson, was general counsel of the National Security Agency from mid-1992 to mid-1994. The author researched this article while a visiting scholar at the Council on Foreign Relations.*

gued, the two communities should coordinate their efforts to understand common problems, should pool resources to avoid unnecessary duplication, should share what they know. What was wrong with that? As intelligence "centers" focusing on joint concerns like terrorism and narcotics trade proliferated, the Justice Department became a major consumer (or at least recipient) of intelligence reports.

All that was done like border trading between vast, self-sufficient empires—at the margin, and when it suited both communities. Neither community intended to change its fundamental way of doing business. Few foresaw any danger in nibbling a bit at the principle that intelligence and law enforcement must remain separate undertakings.

The BNL Affair

Then came the BNL affair, with its charges of a massive coverup at Justice and the CIA. Two years later, such claims seem overwrought. At least three separate investigations have turned up no support for them, and no intelligence or law enforcement official has been indicted—or apparently even disciplined—as a result of BNL. Even the Clinton administration, which had no reason to soft-pedal its probe, seems now to have quietly concluded that no wrongdoing occurred in either community.[1]

At the time, however, press coverage of the affair had a strident breathlessness that brought to mind coverage of Watergate and Iran-*contra*. When it turned out that both the CIA and the Justice Department had failed to identify all of the intelligence reports on BNL in their files, respected career professionals in both agencies found themselves attacked as co-conspirators in a coverup.

Thus did these agencies learn the hidden cost of their practical accommodations in years past. Their critics were simply carrying the concept of "coordination" to its logical conclusion. If intelligence gathering has been harnessed to the cause of catching and prosecuting criminals, the outsiders said, then intelligence agencies should live by the rules that govern criminal investigators. The critics assumed that the intelligence community was obliged to search its files for any information that might help the defendant's case. So when the CIA produced arguably exculpatory documents that the Justice Department had never shown the defendant or the judge, it looked like dereliction of duty or worse.

Later, a postmortem would show that some of the intelligence reports had been sent to Justice, where they were lost or forgotten; that others were simply overlooked when the CIA first searched its own records; and that some were informal reports that had never been formalized for fear of exposing sensitive intelligence sources and methods in a criminal investigation. Gallingly, even the agencies' defenders found themselves arguing that the agencies were not corrupt, just incompetent.

That, it turned out, was also the conclusion reached in the investigations that followed. The staff of the Senate Select Intelligence Committee wrote a detailed report criticizing the government's failure to use intelligence assets to get to the bottom of the BNL affair, calling for more and better coordination between the communities and for more and better access to intelligence files. The attorney general's independent counsel, Judge Frederick Lacey, found no criminal wrongdoing at Justice or the CIA but criticized the CIA's procedures for disseminating information as well as the lack of systematic intelligence record keeping and processing at Justice.

In the wake of the investigations, a task force dominated by career officials was formed to recommend ways to improve the relationship between Justice and the intelligence community. The career officials, perhaps predictably, proposed to do more of what they had been doing—only better this time. The career officials' report has not yet been adopted by the administration, but its thrust is clear: The law enforcement and intelligence communities will continue to converge; and there are no problems in their converging relationship that cannot be solved with more staff, more computers, and more high-level coordination. It is an eminently practical conclusion.

[1] *See Kenneth I. Juster, "The Myth of Iraqgate," in FOREIGN POLICY 94 (Spring 1994).*

But on this issue the forces of practicality are simply wrong. Putting intelligence resources increasingly at the disposal of prosecutors poses much the same threat today as it did in 1947. Intelligence-gathering tolerates a degree of intrusiveness, harshness, and deceit that Americans do not want applied against themselves.

Today the risk to civil liberties is largely theoretical. Among the more surprising discoveries I made when I joined the National Security Agency was the depth of the agency's commitment to obeying the legal limits on gathering intelligence relating to American citizens. The intelligence scandals and institutional reforms of the 1970s remain living lessons in the secret world.

However theoretical the risks to civil liberties may be, they cannot be ignored. The intelligence community serves a constituency of several hundred officials. If top military and civilian policymakers are pleased with what the community produces, it glows with success. When President Bill Clinton cancels his intelligence briefing four or five times in a week, as he did early in his term, the entire community trembles. No other part of the government has so narrow an audience—or responds so enthusiastically to guidance from above.

One of my office's jobs at the agency was to review requests for intelligence from drug enforcement agencies. In some cases, we suspected they were trying to shortcut constitutional or statutory limits, and their requests were denied. But I have no illusions that our objections would have prevailed if a different message had been coming from the leaders of the agency and the government.

As a counterweight to the risk of shortcuts, the reforms of the 1970s brought the rule of law explicitly to intelligence activities. For security reasons, that has meant attorney general review more often than judicial review. And for 20 years, it has worked well: The Justice Department has served as an effective check on the intelligence community. The department could credibly act as a surrogate judge in that period because it did not owe the intelligence agencies anything. But should it come to depend on the intelligence agencies to help it enforce the law, the department will be less credible, and perhaps less vigilant, as a guardian of civil liberties.

The difference between the legal regimes governing law enforcement and intelligence can perhaps best be seen by looking at the way each conducts wiretaps, or electronic surveillance. Police taps are governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which imposes elaborate controls. Police must have probable cause to believe that the target is engaged in a crime, the crime must be one identified by Congress as particularly serious, the police must have no way other than a tap to collect the evidence they seek, they must persuade a judge to issue a warrant for it, and they must report to the judge every few weeks to show that it is still yielding valuable information.

Taps performed for foreign intelligence purposes were not regulated until 1978, when Congress enacted the Foreign Intelligence Surveillance Act. That act governs national security wiretaps, providing protections against surveillance of Americans and requiring the government to obtain a warrant for national security wiretaps within the United States. But the warrants can last for up to a year, and the standards for granting a warrant depend not on behavior but on status. If the target is a foreign power or agent of a foreign power, surveillance will be authorized.

The standards for intelligence taps are—and must be—looser, for obvious reasons. For one, the stakes are higher. Foreign powers like the old Soviet Union certainly pose a greater threat to this country than any conceivable criminal organization. For another, the targets are more elusive. Intelligence agencies spend years intercepting anodyne conversations, waiting for the one moment when discipline breaks down and a crucial fact slips out. For a third, relations between the United States and foreign governments are governed not by the social contract underlying American democracy, but by the rules of international relations, in which espionage is hallowed by tradition.

But what happens when the distinction between law enforcement and foreign intelligence

wiretaps begins to fade? The most obvious consequence is that law enforcement officials hoping to conduct a wiretap are tempted to redefine their criminal investigations in foreign intelligence terms. That saves them much of the hassle of meeting Title III standards for the wiretap. The bigger the role assigned to law enforcement in defining the country's foreign intelligence requirements, the easier that becomes. It may all be done in good faith by pragmatic men and women. But it will gradually erode some of the protections that Title III was designed to confer.

The other threat is also real though less obvious. It is that the courts will respond to the growing convergence by forcing intelligence agencies to live by the rules that govern law enforcement. The Supreme Court was careful to separate national security from criminal investigative taps in 1967 when it first declared wiretaps to be "searches" subject to the Fourth Amendment, and both Congress and the lower courts have agreed that foreign intelligence taps are judged by a different standard under the U.S. Constitution.

But courts are quick to spot a risk of abuse. In 1972, for example, the Supreme Court struck down a Nixon administration claim that the calls of domestic dissidents could be intercepted without warrants under the rubric of national security. If the distinction between intelligence and law enforcement grows too artificial, the judiciary could cripple intelligence surveillance by demanding that it conform to the same standards as law enforcement.

In fact, the consequences would be worse than that. If the courts were to determine that just one intelligence wiretap has in fact crossed the line into law enforcement's territory (and that would be easy to do, given the vagueness of the line and the growing convergence of investigative targets), a series of statutory traps would be sprung. The target would be entitled to notice of the tap. Those who approved and carried it out would be subject to prosecution for committing a felony. The sources and methods used to conduct the tap would be at risk, if not fatally blown.

A similar problem arises in deciding how and when to share intelligence with law enforcement agencies. That field is less sexy than intelligence collection but no less crucial. From Pearl Harbor to BNL, the intelligence failures that hurt the worst have not been those of collection but rather those of dissemination.

Investigative Dissemination

Dissemination to law enforcement falls into two categories: investigative and exculpatory. Investigative dissemination in many respects resembles ordinary intelligence dissemination. If, say, the Drug Enforcement Administration (DEA) is concerned about Central Asian drugs smuggled by the Russian mob, it will want to know more about both Central Asian drugs and organized crime in Russia. In preparing analyses and transmitting intelligence on these topics, the intelligence agencies are acting in an entirely traditional fashion. Over the years, law enforcement agencies and the Justice Department have expressed interest in a wide range of such topics, with the result that a torrent of intelligence has been transmitted to that department on many issues. But, as was embarrassingly clear in the aftermath of the investigations into the BNL affair, much of the intelligence that Justice gets is desultorily skimmed and discarded—if it is read at all.

Why? General information on law enforcement topics has limited value for investigators and prosecutors. What they care about, for the most part, are individual investigations leading to individual convictions. Their narrow focus shapes their view of intelligence. Intelligence that is vital while an investigation is underway suddenly becomes irrelevant once the jury has spoken. Law enforcement respects secrecy and confidential sources—but only for a time. Intelligence that cannot ultimately be introduced as evidence at trial borders on the worthless.

So if intelligence is to be valuable to Justice Department prosecutors, it must be focused on what they care about—individual investigations. That is the inevitable direction in which closer coordination with Justice will push the intelligence agencies. Not only is that what prosecutors want, but that is what the intelligence community was criticized for not doing in BNL. Critics found it incredible that the CIA did not know what defense the accused was likely to

make in the BNL prosecution and that it had not sent reports relevant to that defense to the right lawyers.

Any dissemination system that seeks to move all intelligence relevant to all Justice prosecutions into the hands of prosecutors is doomed to fail. The self-preservation instincts of government officials would make coordination resemble a game of hearts: Everyone knows that, sooner or later, the game will end—that some arguably relevant piece of intelligence will not be delivered to a federal prosecutor in, say, the Southern District of Florida. When that happens, no one wants to be holding the queen of spades. Thus, the Justice Department will be increasingly inclined to issue sweeping demands for "all relevant intelligence" in any case with an international flavor. And the intelligence community will be increasingly inclined to send masses of intelligence indiscriminately to the Justice Department and let Justice figure out where it might be relevant. By implicitly offering tighter coordination as a way to avoid future BNLs, the task force is writing a check that no dissemination system can cash.

That is a recipe for failure—and a colossal waste of resources. But the cost of success would be equally high. If intelligence agencies succeed in providing the kind of case-oriented "tactical" intelligence that law enforcement values most, the distinction between intelligence and law enforcement will erode even more, with the consequences described above: a long-term risk to civil liberties or an invitation for the courts to impose law-enforcement procedures on intelligence agencies.

Exculpatory Dissemination

The other sort of dissemination to law enforcement is exculpatory. A good example of the kind of procedures that the courts could impose is found in *Brady v. Maryland* (1963). In that case, the U.S. Supreme Court held that prosecutors may not withhold from a criminal defendant information that is material and favorable to the defense. That and related rulings have left prosecutors with a clear obligation to review their files and those of investigating agencies for information that could help the defendant.

The more closely intelligence agencies work with investigators, the more often this obligation will fall on them. The long-term consequences will be worse than the pragmatists suppose. For law enforcement agencies, *Brady* searches are a pain in the neck. But for intelligence agencies, they are a nightmare.

Law enforcement agencies have learned to live with *Brady*. When the FBI opens a case, it knows that a successful investigation will only end in one place—in court. The entire investigative record-keeping system used by the FBI is designed with that end in mind. Records likely to be relevant to a later prosecution are identified and stored so as to make later criminal discovery searches easy. And reports are prepared with the trial in mind—every agent who writes a report on a case does so in the knowledge that what he writes will be read by a defense attorney at the end of the day.

Not so for intelligence agencies. The uses of their information are more diverse, the process more fluid. Intelligence agencies gather information for policymakers. An error that creeps into intelligence reporting may go uncorrected—may even be repeated—if having that fact exactly right is irrelevant to the policy issues of the day. And intelligence does not have a predetermined goal. The information does not have to be made public. So intelligence agency files are more likely than law enforcement files to contain casual speculation or fragments of data that could be construed as exculpatory. The prospect of releasing those files is thus more likely to come as a painful surprise.

That is what happened in BNL. And given the structural barriers to thorough *Brady* searches of intelligence files, we can be certain that that particular queen of spades will turn up again and again, though perhaps not in quite so charged an atmosphere.

Nor are intelligence agencies' problems finished once they find and review all the relevant documents. The Justice Department will want its prosecutors to decide which reports are relevant to their case. The prosecutors will want to be briefed on the sources and methods that produced each report. And even if they conclude that a piece of intelligence is probably not exculpatory, they will want to discuss any

piece of intelligence that could conceivably assist the defendant with the judge in the case. So the judge will have to be briefed as well. Then, if any of the information is deemed materially exculpatory, it will have to be revealed in some form to the defendant and his lawyers. Under the Classified Information Procedures Act, to avoid a risk to intelligence sources and methods, the government is allowed to propose a sanitized substitute for classified data; but the substitute must be just as good as the original for the defendant's purposes. If it is not, the government must reveal its secrets or drop the prosecution.

If the distinction between intelligence and law enforcement grows too artificial, the judiciary could cripple intelligence surveillance by demanding that it conform to the same standards as law enforcement.

It is bad security to describe highly sensitive sources and methods to a steady stream of prosecutors—many of them young lawyers who will soon be making a career out of representing criminal defendants. Even worse, when a court says classified information is relevant to the defense, intelligence agencies will find themselves locked in battle with prosecutors who would rather reveal classified information than give up their prosecution. Of course, defense counsel will have every incentive to exploit the opportunity for graymail. They will strain to find ways of including classified information in their defenses, all in the hope of forcing the government to drop the case rather than reveal its secrets.

What does this add up to? In an effort to give law enforcement more information that it does not want very badly and does not use very well, government officials may be about to stretch the rules that preserve civil liberties, flirt with harsh new judicial limits on how intelligence is gathered, impose unworkable new search and record-keeping duties on intelligence agencies, spread the knowledge of intelligence sources and methods much more widely, routinize conflict between prosecutors seeking convictions and agents keeping secrets, and encourage defense lawyers to exploit each of those problems to the hilt in the hope of forcing the government to abandon the prosecution of their clients.

Why are we doing this? The practical men and women in law enforcement and intelligence tell us we have no choice. They say that all those problems will arise to some degree no matter what we do; that we cannot go back to the days when intelligence and law enforcement were sealed off from each other; and that proper coordination and good will on all sides can minimize the damage.

Maybe so, but given the stakes perhaps we should try an alternative approach first—one that preserves, perhaps even raises, the wall between the two communities. We should begin by shedding illusions. The first and most dangerous is the illusion that intelligence agencies or the Justice Department itself should be expected to identify and disseminate every piece of intelligence that might be relevant to every investigation conducted by federal law enforcement agencies. No one knows enough about the thousands of pending investigations to route intelligence reports efficiently to every interested prosecutor and investigator. To accept responsibility for doing so is like starting every game with the queen of spades in your hand. Instead of establishing mechanisms that purport to carry out that task, we should frankly declare that it cannot be done. Indeed, it should not be done; such all-encompassing distribution would align law enforcement and intelligence to a degree that should appall any student of twentieth-century history.

Instead, we should construct a dissemination system that makes sense. That means distinguishing between top Justice Department officials, who need intelligence to help them make wise policy choices, and other law enforcement officials, who want intelligence to help them make their cases.

Top law enforcement officials—the ones that allocate resources and set strategy—need the same kind of "strategic" intelligence that other policymakers do. If Chinese gangs are planning massive alien smuggling drives, or if the Rus-

sian mob has turned Central Asian collective farms into opium factories, the attorney general and the heads of the FBI and DEA need to know. But such information can and should be fairly tightly controlled. There is not much reason for it to go below the level of deputy assistant attorney general.

Individual Justice Department attorneys, and generalists like the U.S. attorneys around the country, are unlikely to need such strategic intelligence, at least in detail. To the extent that such intelligence requires analysis, the function could be centralized in a Justice Department (or investigating agency) intelligence unit. Under such a system, Justice would not get thousands of documents of doubtful relevance. And what it did get would be controlled and analyzed in a way that would make for greater accountability.

If intelligence agencies succeed in providing the kind of case-oriented "tactical" intelligence that law enforcement values most, the distinction between intelligence and law enforcement will erode even more.

It should go without saying that such information would be gathered only if it has foreign intelligence—and not simply international law enforcement—significance. Decisions about what intelligence to gather must remain the province of the director of central intelligence and the national security apparatus. But there is no reason to insist that the Justice Department be treated differently from, say, the Defense Department in the dissemination of such "strategic" intelligence.

That is not the case for "tactical" intelligence—information about particular shipments, particular schemes, particular individuals. Here the wall of separation between intelligence and law enforcement should largely be maintained. Intelligence agencies should not be asked routinely to use their intelligence-gathering authority to help law enforcement agencies bust criminals.

What about cases where both communities have a legitimate interest in gathering information about the same person or group? Surely there are both law enforcement and intelligence reasons to seek information about the man who shot several CIA employees outside CIA headquarters and then fled the country. Must the FBI and CIA work separately to track him down? No, but the investigations should be coordinated under strict controls. Most important, intelligence agencies should know in advance that they are entering into a coordinated investigation. Then they can keep records in a way that makes it easier to search for exculpatory information—and they can use sources and methods that could, in a pinch, be made public if that is the only way to bring to justice a particularly dangerous offender.

Similarly, a conscious decision to coordinate law enforcement and intelligence activities for an investigation could be preceded by an analysis of whether law enforcement is the predominant interest. If it is, intelligence should be gathered only under law enforcement authority, subject to law enforcement limits and supervision. In such cases, intelligence agencies will know from the start that they are working for—not with—law enforcement.

A system in which tactical intelligence is shared only rarely and only after careful thought will go a long way toward preserving the spirit of the 1947 act. It will protect the current legal distinction between how information may be gathered for law enforcement and national security purposes. And, with luck, it will help address the thorny question of criminal discovery.

The cases requiring that prosecutors turn over exculpatory evidence can be read as applying broadly or narrowly. Read narrowly, the obligation applies to information in the hands of the prosecutors themselves and to the investigators who developed the case. Read broadly, the obligation covers any information in any government file. In my view, the better reading of the cases is that the government ordinarily must search only those records available to the prosecutor and those aligned with the prosecutor. On that reading, intelligence records would be subject to discovery whenever the two com-

munities engaged in a coordinated investigation—although probably only the information gathered in that coordinated effort should be open to discovery.

If there is no coordinated investigation but the defendant believes that his other activities are likely to have been of interest to intelligence agencies, no searches should be ordered—at least in the absence of strong indications that particular intelligence records will produce exculpatory evidence. The burden and risks of searching intelligence files are simply too great. Such cases will be rare. Perhaps the best example is a defendant who claims to have been violating U.S. law because he was hired by the CIA to do so; in that event, checking the CIA's employment records might be an appropriate search, but checking every operational file in the agency would not.

Ironically, the loudest objections to restricting discovery in this way will come not from judges and defendants but from prosecutors who do not want to surrender their chance to review intelligence files. The reasons for the resistance are many. Turning over exculpatory evidence is seen as a prosecutor's ethical obligation. It is difficult to delegate that obligation to another, particularly someone who does not know the case as well as the prosecutor. And, some prosecutors say, the intelligence agencies have not proven reliable when they conduct *Brady* searches on their own. Some in the intelligence community, on the other hand, suspect that while prosecutors talk about having to search for exculpatory information, they never really abandon the hope that their search will turn up something inculpatory. Finally, prosecutors are heavily influenced by the expectations of district court judges, who tend to want broad discovery in order to forestall postconviction appeals. Prosecutors would much rather inconvenience intelligence agencies than annoy the local judges they deal with (and depend on) every day.

The only way out of that box is to elevate the issue beyond the reach of individual prosecutors' preferences and district courts' jawboning. That will only happen if the highest levels of the Justice Department decide that discovery of intelligence agency files should be resisted strongly. The department and the intelligence community need to agree on when a search is necessary and when it is not. At a minimum, that standard should be written into the prosecutors' manual; a statutory standard would be even better.

Either way, to maximize the chances of prevailing against the inevitable constitutional challenge, access limits should apply to prosecutors as well as defendants. As a practical matter, judges are more likely to order that documents be turned over if they come from files the prosecutor has already searched. And the briefing of sources and methods that accompanies prosecutorial searches is at least as great a strain on security as debating the relevance of a few arguably exculpatory documents before a federal judge.

When I was at the National Security Agency, we used to joke about the predictable stages traversed by prosecutors who sought intelligence reports in connection with big investigations. The first reaction was open-mouthed wonder at what the intelligence agencies were able to collect. That was followed by an enthusiastic assumption that vast quantities of useful data must lie in our files. Next came the grinding review of individual documents and the growing realization that the reports were prepared for other purposes and so were unlikely to contain much of relevance to the investigator's specific concerns. Last came ennui, and a gritted-teethed plod through the reports, mostly to avoid a later charge that the examination was incomplete.

The lesson of that progression is one that must be conveyed more widely. Intelligence agencies have great capabilities, but they only produce useful intelligence if they are asked the right questions. Reviewing intelligence collected for one purpose in the hopes that it will shed light on some related issue is almost always a fool's errand. Except for employment files and the like, the only intelligence files likely to contain information genuinely relevant to a criminal case are those assembled as part of a coordinated law enforcement/intelligence investigation. In short, prosecutors and defendants lose little or nothing if searches are restricted to such files.

Implementing that alternative approach will take courage and persistence. It may well seem impractical, at least in the short run. The advantages of coordination and convergence can be realized here and now: New roles are created for intelligence officials; new worlds are opened to law enforcement officials; the echoes of the BNL affair are stilled. The risks that come with more coordination and convergence—risks to sources and intelligence-gathering techniques—all lie in the future. But the advantages of convergence are so fleeting, and the risks so palpable, that we cannot afford to settle for practicality.