

The Initial Reports on U.S. Access to Banking Records

The New York Times

http://www.nytimes.com/2006/06/22/washington/22cnd-intel.html?_r=1&ei=5094&en=3653468f88851bcd&hp=&ex=1151035200&partner=homepage&pagewanted=all&oref=slogin

Bank Data Secretly Reviewed by U.S. to Fight Terror

WASHINGTON, June 22 - Under a secret Bush administration program initiated weeks after the Sept. 11 attacks, counterterrorism officials have gained access to financial records from a vast international database and examined banking transactions involving thousands of Americans and others in the United States, according to government and industry officials.

The program is limited, government officials say, to tracing transactions of people suspected of ties to Al Qaeda by reviewing records from the nerve center of the global banking industry, a Belgian cooperative that routes about \$6 trillion daily between banks, brokerages, stock exchanges and other institutions. The records mostly involve wire transfers and other methods of moving money overseas or into and out of the United States. Most routine financial transactions confined to this country are not in the database.

Viewed by the Bush administration as a vital tool, the program has played a hidden role in domestic and foreign terrorism investigations since 2001 and helped in the capture of the most wanted Qaeda figure in Southeast Asia, the officials said. The program, run out of the Central Intelligence Agency and overseen by the Treasury Department, "has provided us with a unique and powerful window into the operations of terrorist networks and is, without doubt, a legal and proper use of our authorities," Stuart Levey, an undersecretary at the Treasury Department, said in an interview Thursday. The program is grounded in part on the president's emergency economic powers, Mr. Levey said, and multiple safeguards have been imposed to protect against any unwarranted searches of Americans' records.

The program, however, is a significant departure from typical practice in how the government acquires Americans' financial records. Treasury officials did not seek individual court-approved warrants or subpoenas to examine specific transactions, instead relying on broad administrative subpoenas for millions of records from the cooperative, known as Swift.

That access to large amounts of sensitive data was highly unusual, several officials said, and stirred concerns inside the administration about legal and privacy issues. "The capability here is awesome or, depending on where you're sitting, troubling," said one former senior counterterrorism official who considers the program valuable. While tight controls are in place, the official added, "The potential for abuse is enormous."

The program is separate from the National Security Agency's efforts to eavesdrop without warrants and collect domestic phone records, operations that have provoked fierce public debate and spurred lawsuits against the government and telecommunications companies. But all the programs grew out of the Bush administration's desire to exploit technological tools to prevent another terrorist strike, and all reflect attempts to break down longstanding legal or institutional barriers to the government's access to private information about Americans and others inside the United States.

Officials described the Swift program as the biggest and most far-reaching of several secret efforts to trace terrorist financing. Much more limited agreements with other companies have provided access to A.T.M. transactions, credit card purchases and Western Union wire payments, the officials said.

Nearly 20 current and former government officials and industry executives discussed aspects of the Swift operation with The New York Times on condition of anonymity because the program remains classified. Some of those officials expressed reservations about the program, saying that what they viewed as an urgent, temporary measure had become permanent nearly five years later without specific Congressional approval or formal authorization.

Data from the Brussels-based banking consortium, formally known as the Society for Worldwide Interbank Financial Telecommunication, has allowed officials from the C.I.A., the Federal Bureau of Investigation and other agencies to examine "tens of thousands" of financial transactions, Mr. Levey said.

While many of those transactions have occurred entirely on foreign soil, officials have also been keenly interested in international transfers of money by individuals, businesses, charities and other organizations under suspicion inside the United States, officials said. A small fraction of Swift's records involve transactions entirely within this country, but Treasury officials said they were uncertain whether any had been examined.

Swift executives have been uneasy at times about their secret role, the government and industry officials said. By 2003, the executives told American officials they were considering pulling out of the arrangement, which began as an emergency response to the Sept. 11 attacks, the officials said. Worried about potential legal liability, the Swift executives agreed to continue providing the data only after top officials, including Alan Greenspan, then chairman of the Federal Reserve, intervened. At the same time, new controls were introduced.

Among the program's safeguards, government officials said, is an outside auditing firm that verifies that the data searches are based on a link to terrorism intelligence. Swift and Treasury officials said they were aware of no abuses. But Mr. Levey, the Treasury official, said one person had been removed from the operation for conducting a search considered inappropriate.

"We are not on a fishing expedition," Mr. Levey said. "We're not just turning on a vacuum cleaner and sucking in all the information that we can."

Treasury officials said Swift was exempt from American laws restricting government access to private financial records because the cooperative was considered a messaging service, not a bank or financial institution.

But at the outset of the operation, Treasury and Justice Department lawyers debated whether the program had to comply with such laws before concluding that it did not, people with knowledge of the debate said. Several outside banking experts, however, say that financial privacy laws are murky and sometimes contradictory and that the program raises difficult legal and public policy questions.

The Bush administration has made no secret of its campaign to disrupt terrorist financing, and President Bush, Treasury officials and others have spoken publicly about those efforts. Administration officials, however, asked The New York Times not to publish this article, saying that disclosure of the Swift program could jeopardize its effectiveness. They also enlisted several current and former officials, both Democrat and Republican, to vouch for its value.

Bill Keller, the newspaper's executive editor, said: "We have listened closely to the administration's arguments for withholding this information, and given them the most serious and respectful consideration. We remain convinced that the administration's extraordinary access to this vast repository of international financial data, however carefully targeted use of it may be, is a matter of public interest."

Swift declined to discuss details of the program but defended its role in written responses to questions. "Swift has fully complied with all applicable laws," the consortium said. The organization said it insisted that the data be used only for terrorism investigations and had narrowed the scope of the information provided to American officials over time.

Swift's database provides a rich hunting ground for government investigators. Swift is a crucial gatekeeper, providing electronic instructions on how to transfer money between 7,800 financial institutions worldwide. The cooperative is owned by more than 2,200 organizations, and virtually every major commercial bank, as well as brokerage houses, fund managers and stock exchanges, uses its services. Swift routes more than 11 million transactions each day, most of them across borders.

The cooperative's message traffic allows investigators, for example, to track money from the Saudi bank account of a suspected terrorist to a mosque in New York. Using intelligence tips about specific targets, agents search the database in what one official described as a "24-7" operation. Customers' names, bank account numbers and other identifying information, can be retrieved, the officials said.

The data does not allow the government to track routine financial activity, like A.T.M. withdrawals, confined to this country, or to see bank balances, Treasury officials said.

And the information is not provided in real time - Swift generally turns it over several weeks later. Because of privacy concerns and the potential for abuse, the government sought the data only for terrorism investigations and prohibited its use for tax fraud, drug trafficking or other inquiries, the officials said.

The Treasury Department was charged by President Bush, in a September 2001 executive order, with taking the lead role in efforts to disrupt terrorist financing. Mr. Bush has been briefed on the program and Vice President Dick Cheney has attended C.I.A. demonstrations, the officials said. The National Security Agency has provided some technical assistance.

While the banking program is a closely held secret, administration officials have conducted classified briefings to some members of Congress and the Sept. 11 Commission, the officials said. More lawmakers were briefed in recent weeks, after the administration learned The Times was making inquiries for this article. Swift's 25-member board of directors, made up of representatives from financial institutions around the world, was previously told of the program, but it is not clear if other participants know that American intelligence officials can examine their message traffic.

Because Swift is based overseas and has offices in the United States, it is governed both by European and American laws. Several international regulations and policies impose privacy restrictions on companies that are generally regarded as more stringent than those in this country. United States law establishes some protections for the privacy of Americans' financial data, but they are not ironclad. A 1978 measure, the Right to Financial Privacy Act, has a limited scope and a number of exceptions, and its role in national security cases remains largely untested.

Several people familiar with the Swift program said they believed they were exploiting a "gray area" in the law and that a case could be made for restricting the government's access to the records on Fourth Amendment and statutory grounds. They also worried about the impact on Swift if the program were disclosed.

"There was always concern about this program," a former official said.

One person involved in the Swift program estimated that analysts have reviewed international transfers involving "many thousands" of people or groups in the United States. Two other officials also placed the figure in the thousands. Mr. Levey said he could not estimate the number.

The Swift data has provided clues to terror money trails and ties between possible terrorists and organizations financing them, the officials said. In some instances, they said, the program has pointed them to new suspects, while in others it has buttressed cases already under investigation.

Among the successes was the capture of a Qaeda operative, Riduan Isamuddin, better known as Hambali, believed to be the mastermind of the 2002 bombing of a Bali resort, several officials said. The Swift data identified a previously unknown figure in Southeast

Asia who had financial dealings with a person suspected of being a member of Al Qaeda; that link helped locate Hambali in Thailand in 2003, they said.

In the United States, the program has provided financial data in investigations into possible domestic terrorist cells as well as inquiries of Islamic charities with suspected of having links to extremists, the officials said.

The data also helped identify a Brooklyn man who was convicted on terrorism-related charges last year, the officials said. The man, Uzair Paracha, who worked at a New York import business, aided a Qaeda operative in Pakistan by agreeing to launder \$200,000 through a Karachi bank, prosecutors said.

In terrorism prosecutions, intelligence officials have been careful to "sanitize," or hide the origins of evidence collected through the program to keep it secret, officials said. The Bush administration has pursued steps that may provide some enhanced legal standing for the Swift program. In late 2004, Congress authorized the Treasury Department to develop regulations requiring American banks to turn over records of international wire transfers. Officials say a preliminary version of those rules may be ready soon. One official described the regulations as an attempt to "formalize" access to the kind of information secretly provided by Swift, though other officials said the initiative was unrelated to the program.

The Scramble for New Tools

Like other counterterrorism measures carried out by the Bush administration, the Swift program began in the hectic days after the Sept. 11 attacks, as officials scrambled to identify new tools to head off further strikes.

One priority was to cut off the flow of money to Al Qaeda. The Sept. 11 hijackers had helped finance their plot by moving money through banks. Nine of the hijackers, for instance, funneled money from Europe and the Middle East to SunTrust bank accounts in Florida. Some of the \$130,000 they received was wired by people overseas with known links to Al Qaeda.

Financial company executives, many of whom had lost friends at the World Trade Center, were eager to help federal officials trace terrorist money. "They saw 9/11 not just as an attack on the United States, but on the financial industry as a whole," said one former government official.

Quietly, counterterrorism officials sought to expand the information they were getting from financial institutions. Treasury officials, for instance, spoke with credit card companies about devising an alert if someone tried to buy fertilizer and timing devices that could be used for a bomb, but they were told the idea was not logistically possible, a lawyer in the discussions said.

The F.B.I. began acquiring financial records from Western Union and its parent company, First Data Corporation. The programs were alluded to in Congressional testimony by the F.B.I. in 2003 and described in more detail in a book released this week,

"The One Percent Doctrine," by Ron Suskind. Using what officials described as individual, narrowly framed subpoenas and warrants, the F.B.I. has obtained records from First Data, which processes credit and debit card transactions, to track financial activity and try to locate suspects.

Similar subpoenas for the Western Union data allowed the F.B.I. to trace wire transfers, mainly outside the United States, and to help Israel trace the financing of about a half-dozen possible terrorist plots there, an official said.

The idea for the Swift program, several officials recalled, grew out of a suggestion by a Wall Street executive, who told a senior Bush administration official about Swift's database. Few government officials knew much about the consortium, which is led by a Brooklyn native, Leonard H. Schrank, but they quickly discovered it offered unparalleled access to international transactions.

Swift, a former government official said, was "the mother lode, the Rosetta stone" for financial data.

Intelligence officials were so eager to exploit the Swift data that they discussed having the C.I.A. covertly gain access to the system, several officials involved in the talks said. But Treasury officials resisted, the officials said, and favored going to Swift directly. At the same time, lawyers in the Treasury Department and the Justice Department were considering possible legal obstacles to the arrangement, the officials said.

In 1976, the Supreme Court ruled that Americans had no constitutional right to privacy for their records held by banks or other financial institutions. In response, Congress passed the Right to Financial Privacy Act two years later, restricting government access to Americans' banking records. In considering the Swift program, some government lawyers were particularly concerned about whether the law prohibited officials from gaining access to records without a warrant or subpoena based on some level of suspicion about each target.

For many years, law enforcement officials have relied on grand-jury subpoenas or court-approved warrants for such financial data. Since the Sept. 11 attacks, the F.B.I. has turned more frequently to an administrative subpoena, known as a national security letter, to demand such records.

After an initial debate, Treasury Department lawyers, consulting with the Justice Department, concluded that the privacy laws applied to banks, not to a banking cooperative like Swift. They also said the law protected individual customers and small companies, not the major institutions that route money through Swift on behalf of their customers.

Other state, federal and international regulations place different and sometimes conflicting restrictions on the government's access to financial records. Some put greater burdens on the company disclosing the information than on the government officials demanding it.

Among their considerations, American officials saw Swift as a willing partner in the operation. But Swift said its participation was never voluntary. "Swift has made clear that it could provide data only in response to a valid subpoena," according to its written statement.

Indeed, the cooperative's executives voiced early concerns about legal and corporate liability, officials said, and the Treasury Department's Office of Foreign Asset Control began issuing broad subpoenas for the cooperative's records related to terrorism. One official said the subpoenas were intended to give Swift some legal protection.

Underlying the government's legal analysis was the International Emergency Economic Powers Act, which Mr. Bush invoked after the Sept. 11 attacks. The law gives the president what legal experts say is broad authority to "investigate, regulate or prohibit" foreign transactions in responding to "an unusual and extraordinary threat."

But L. Richard Fischer, a Washington lawyer who wrote a book on banking privacy and is regarded as a leading expert in the field, said he was troubled that the Treasury Department would use broad subpoenas to demand large volumes of financial records for analysis. Such a program, he said, appears to do an end run around bank-privacy laws that generally require the government to show that the records of a particular person or group are relevant to an investigation.

"There has to be some due process," Mr. Fischer said. "At an absolute minimum, it strikes me as inappropriate."

Several former officials said they had lingering concerns about the legal underpinnings of the Swift operation. The program "arguably complies with the letter of the law, if not the spirit," one official said.

Another official said: "This was creative stuff. Nothing was clear cut, because we had never gone after information this way before."

Treasury officials would not say whether a formal legal opinion was prepared in authorizing the program, but they said they considered the government's authority to subpoena the Swift records to be clear. "People do not have a privacy interest in their international wire transactions," Mr. Levey, the Treasury under secretary, said.

Tighter Controls Sought

Within weeks of the Sept. 11 attacks, Swift began turning over records that allowed American analysts to look for evidence of terrorist financing. Initially, there appear to have been few formal limits on the searches.

"At first, they got everything - the entire Swift database," one person close to the operation said.

Intelligence officials paid particular attention to transfers to or from Saudi Arabia and the United Arab Emirates because most of the Sept. 11 hijackers were from those countries. The volume of data, particularly at the outset, was often overwhelming, officials said. "We were turning on every spigot we could find and seeing what water would come out," one former administration official said. "Sometimes there were hits, but a lot of times there weren't."

Officials realized the potential for abuse, and soon narrowed the program's targets and put in more safeguards. Among them were the auditing firm, an electronic record of every search and a form documenting the intelligence that justified each data search. Mr. Levey said the program was used only to search the records of individuals or entities, not for broader data searches.

Despite the controls, Swift executives became increasingly worried about their secret involvement with the American government, the officials said. By 2003, the cooperative's officials were discussing pulling out because of their concerns about legal and financial risks if the program were revealed, one government official said.

"How long can this go on?" a Swift executive asked, according to the official. Even some American officials began to question the open-ended arrangement. "I thought there was a limited shelf life and that this was going to go away," the former senior official said.

In 2003, administration officials asked Swift executives and some board members to come to Washington. They met with Mr. Greenspan, Robert S. Mueller III, the F.B.I. director, and Treasury officials, among others, in what one official described as "a full-court press."

The executives agreed to continue supplying records after the Americans pledged to impose tighter controls. Swift representatives would be stationed alongside intelligence officials and could block any searches considered inappropriate, several officials said. The procedural change provoked some opposition at the C.I.A. because "the agency was chomping at the bit to have unfettered access to the information," a senior counterterrorism official said. But the Treasury Department saw it as a necessary compromise, the official said, to "save the program."

The Los Angeles Times

<http://www.latimes.com/news/nationworld/nation/la-na-swift23jun23,0,6482687.story?coll=la-home-headlines>

Secret U.S. Program Tracks Global Bank Transfers

The Treasury Dept. program, begun after the Sept. 11 attacks, attempts to monitor terrorist financing but raises privacy concerns.

By Josh Meyer and Greg Miller
Times Staff Writers
June 23, 2006

WASHINGTON — The U.S. government, without the knowledge of many banks and their customers, has engaged for years in a secret effort to track terrorist financing by accessing a vast database of confidential information on transfers of money between banks worldwide.

The program, run by the Treasury Department, is considered a potent weapon in the war on terrorism because of its ability to clandestinely monitor financial transactions and map terrorist webs.

It is part of an arsenal of aggressive measures the government has adopted since the Sept. 11 terrorist attacks that yield new intelligence, but also circumvent traditional safeguards against abuse and raise concerns about intrusions on privacy.

White House spokesman Tony Snow insisted today that the program offers "abstract harms" but "concrete benefits."

"It works," he said.

He added that it has contributed to indictments of would-be terrorists and to investigations of acts of terrorism.

"This is government at its best," said Treasury Secretary John W. Snow. "It's responsible government. It's government that works. This is a program that makes Americans and the world safer."

John Snow called it "regrettable" that the program had been made public. "That can only help the terrorists," said Snow, whose department runs the program.

Under this effort, Treasury routinely acquires information about bank transfers from the world's largest financial communication network, which is run by a consortium of financial institutions called the Society for Worldwide Interbank Financial Telecommunication, or SWIFT.

The SWIFT network carries up to 12.7 million messages a day containing instructions on many of the international transfers of money between banks. The messages typically include the names and account numbers of bank customers — from U.S. citizens to major corporations — who are sending or receiving funds.

Through the program, Treasury has built an enormous — and ever-growing — repository of financial records drawn from what is essentially the central nervous system of international banking.

In a major departure from traditional methods of obtaining financial records, the Treasury Department uses a little-known power — administrative subpoenas — to collect data from the SWIFT network, which has operations in the U.S., including a main computer hub in Manassas, Va. The subpoenas are secret and not reviewed by judges or grand juries, as are most criminal subpoenas.

"It's hard to overstate the value of this information," Treasury Secretary John W. Snow said Thursday in a statement he issued after The Times and other media outlets reported the existence of the Terrorist Finance Tracking Program.

SWIFT acknowledged Thursday in response to questions from The Times that it has provided data under subpoena since shortly after Sept. 11, 2001, a striking leap in cooperation from international bankers, who long resisted such law enforcement intrusions into the confidentiality of their communications.

But SWIFT said in a statement that it has worked with U.S. officials to restrict the use of the data to terrorism investigations.

The program is part of the Bush administration's dramatic expansion of intelligence-gathering capabilities, which includes warrantless eavesdropping on the international phone calls of some U.S. residents. Critics complain that these efforts are not subject to independent governmental reviews designed to prevent abuse, and charge that they collide with privacy and consumer protection laws in the United States.

Steven Aftergood, director of the Project on Government Secrecy at the Federation of American Scientists, said the SWIFT program raises similar issues. "It boils down to a question of oversight, both internal and external. And in the current circumstances, it is hard to have confidence in the efficacy of their oversight," he said. "Their policy is, 'Trust us,' and that may not be good enough anymore."

A former senior Treasury official expressed concern that the SWIFT program allows access to vast quantities of sensitive data that could be abused without safeguards. The official, who said he did not have independent knowledge of the program, questioned what becomes of the data, some of it presumably related to innocent banking customers.

"How do you separate the wheat from the chaff?" the former official said. "And what do you do with the chaff?"

At the White House, Tony Snow said "a whole series of safeguards" were in place to prevent violations of ordinary Americans' privacy. "If you're not a member of Al Qaeda you're safe," he said.

The perception of potential privacy violations "seems to be limited to the press corps," Snow said.

The program's legitimacy was established by a presidential executive order signed 10 days after the terrorist attacks of Sept. 11, 2001, he added.

Snow said the House and Senate intelligence committees were fully apprised of the program. The American people, he said, understand that such efforts lose their effectiveness if they are widely known.

Treasury analysts must provide a link to suspected terrorism before getting access to any data, said Treasury Undersecretary Stuart Levey. "We are not permitted to browse through this data," he said.

More than a dozen current and former U.S. officials discussed the program with The Times on condition of anonymity, citing its sensitive nature.

The effort runs counter to the expectations of privacy and security that are sacrosanct in the worldwide banking community. SWIFT promotes its services largely by touting the network's security, and most of its customers are unaware that the U.S. government has such extensive access to their private financial information.

U.S. officials, some of whom expressed surprise the program had not previously been revealed by critics, acknowledged it would be controversial in the financial community. "It is certainly not going to sit well in the world marketplace," said a former counterterrorism official. "It could very likely undermine the integrity of SWIFT."

Bush administration officials asked The Times not to publish information about the program, contending that disclosure could damage its effectiveness and that sufficient safeguards are in place to protect the public.

Dean Baquet, editor of The Times, said: "We weighed the government's arguments carefully, but in the end we determined that it was in the public interest to publish information about the extraordinary reach of this program. It is part of the continuing national debate over the aggressive measures employed by the government."

Under the program, Treasury issues a new subpoena once a month, and SWIFT turns over huge amounts of electronic financial data, according to Stuart Levey, the department's undersecretary for terrorism and financial intelligence. The administrative subpoenas are issued under authority granted in the 1977 International Emergency Economic Powers Act.

The SWIFT information is added to a massive database that officials have been constructing since shortly after Sept. 11. Levey noted that SWIFT did not have the ability to search its own records. "We can, because we built the capability to do that," he said.

Treasury shares the data with the CIA, the FBI and analysts from other agencies, who can run queries on specific individuals and accounts believed to have terrorist connections, Levey said Thursday in an interview with The Times.

Levey said that "tens of thousands" of searches of the database have been done over the last five years.

The program was initially a closely guarded secret, but it has recently become known to a wider circle of government officials, former officials, banking executives and outside experts.

Current and former U.S. officials said the effort has been only marginally successful against Al Qaeda, which long ago began transferring money through other means, including the highly informal banking system common in Islamic countries.

The value of the program, Levey and others said, has been in tracking lower- and mid-level terrorist operatives and financiers who believe they have not been detected, and militant groups, such as Hezbollah, Hamas and Palestinian Islamic Jihad, that also operate political and social welfare organizations.

It's no secret that the Treasury Department tries to track terrorist financing, or that those efforts ramped up significantly after the Sept. 11 terrorist attacks. But the SWIFT program goes far beyond what has been publicly disclosed about that effort in terms of the amount of financial data that U.S. intelligence agencies can access.

The program also represents a major tactical shift. U.S. investigators long have been able to subpoena records on specific accounts or transactions when they could show cause — a painstaking process designed mainly for gathering evidence. But access to SWIFT enables them to follow suspicious financial trails around the globe, identifying new suspects without having to seek assistance from foreign banks.

SWIFT is a consortium founded in 1973 to replace telex messages. It has almost 7,900 participating institutions in more than 200 countries — including Bank of America, JP Morgan Chase Bank, Citibank and Credit Suisse. The network handled 2.5 billion financial messages in 2005, including many originating in countries such as Saudi Arabia, Pakistan and the United Arab Emirates that the United States scrutinizes closely for terrorist activity.

The system does not execute the actual transfer of funds between banks; that is carried out by the Federal Reserve and its international counterparts. Rather, banks use the network to transmit instructions about such transfers. For that reason, SWIFT's data is extremely valuable to intelligence services seeking to uncover terrorist webs.

CIA operatives trying to track Osama bin Laden's money in the late 1990s figured out clandestine ways to access the SWIFT network. But a former CIA official said Treasury officials blocked the effort because they did not want to anger the banking community.

Historically, "there was always a line of contention" inside the government, said Paul Pillar, former deputy director of the CIA's counterterrorism center. "The Treasury

position was placing a high priority on the integrity of the banking system. There was considerable concern from that side about anything that could be seen as compromising the integrity of international banking."

Before Sept. 11, a former senior SWIFT executive said, providing access to its sensitive data would have been anathema to the Belgium-based consortium. But the attacks on the World Trade Center and the Pentagon led to a new mind-set in many industries, including telecommunications.

SWIFT said the Treasury Department's Office of Foreign Assets Control sent the first subpoena shortly after Sept. 11, seeking "limited sets of data" to learn about how Al Qaeda financed the attacks.

Unlike telephone lines and e-mail communications, the SWIFT network cannot be easily tapped. It uses secure log-ins and state-of-the-art encryption technology to prevent intercepted messages from being deciphered. "It is arguably the most secure network on the planet," said the former SWIFT executive who spoke on condition of anonymity. "This thing is locked down like Fort Knox."

SWIFT said it was responding to compulsory subpoenas and negotiated with U.S. officials to narrow them and to establish protections for the privacy of its customers. SWIFT also said it has never given U.S. authorities direct access to its network.

"Our fundamental principle has been to preserve the confidentiality of our users' data while complying with the lawful obligations in countries where we operate," SWIFT said in its statement.

Current and former U.S. officials familiar with the SWIFT program described it as one of the most valuable weapons in the financial war on terrorism, but declined to provide even anecdotal evidence of its successes.

A former high-ranking CIA officer said it has been a success, and another official said it has allowed U.S. counterterrorism officials to follow a tremendous number of leads. CIA officials pursue leads overseas, and the FBI and other agencies pursue leads in the United States, where the CIA is prohibited from operating.

Officials said the program is relied upon especially heavily when intelligence chatter from phone and e-mail intercepts suggested an imminent attack, conveying real-time intelligence for counterterrorism operations.

The former SWIFT executive said much can be learned from network messages, which require an actual name and address of both the sender and recipient, unlike phone calls and e-mails, in which terrorist operatives can easily disguise their identities.

"There is a good deal of detail in there," he said.

As the global war on terrorism has succeeded in taking out some senior terrorists and their financiers, particularly within Al Qaeda, the organization and its many affiliates have sought to move to hidden locations and to transfer their money through proxies such as charities, aid organizations and corporate fronts.

The officials said the SWIFT information can be used in "link analysis." That technique allows analysts to identify any person with whom a suspected terrorist had financial dealings — even those with no connection to terrorism. That information is then mapped and analyzed to detect patterns, shifts in strategy, specific "hotspot" accounts, and locations that have become new havens for terrorist activity.

The SWIFT program is just one of the Bush administration's post-Sept. 11 initiatives to collect intelligence that could include information on U.S. residents.

The National Security Agency, which can intercept communications around the world, is eavesdropping on the telephone calls and e-mails of some U.S. residents without obtaining warrants. And it has been accused of asking telecommunications companies to help create a database of the phone-call records of almost all Americans.

The Justice Department also has asked Internet companies to keep records of the websites customers visit and the people they e-mail for two years, rather than days or weeks, which would greatly expand the government's ability to track online activity.

Numerous lawsuits have been filed against the government and phone companies, challenging the NSA efforts. The government has asked courts to throw them out, invoking the "state secrets" privilege and arguing that trials would compromise national security. The NSA's interception of telephone calls also has been criticized for lacking an independent review process to ensure that the information is not abused.

The SWIFT program raises similar concerns, some critics say.

Privacy advocates have questioned "link analysis" because it can drag in innocent people who have routine financial dealings with terrorist suspects.

And no outside governmental oversight body, such as the Foreign Intelligence Surveillance Court or a grand jury, monitors the subpoenas served on SWIFT.

Levey said the program is subject to "robust" checks and balances designed to prevent misuse of the data. He noted that requests to access the data are reviewed by Treasury's assistant secretary for intelligence; that analysts can only access the data for terrorism-related searches; and that records are kept of each search and are reviewed by an outside auditor for compliance.

Levey said there had been one instance of abuse in which an analyst had conducted a search that did not meet the terrorist-related criteria. The analyst was subsequently denied access to the database, he said.

During the last five years, SWIFT officials have raised concerns about the scope of the program, particularly at the outset, when it was handing over virtually its entire database. The amount of data handed over each month has been winnowed down.

"The safeguards were not all there in September 2001," Levey acknowledged. "We started narrowing it from the beginning."

New safeguards have been added, he said, noting that SWIFT officials are now allowed to be present when analysts search the data and to raise objections with top officials.

Officials from other government agencies have raised the issue of accessing the records for other investigative purposes, but Levey said such proposals have been rejected — largely out of concern that doing so might erode support for the program.

Asked what would prevent the data from being used for other purposes in the future, Levey said doing so would likely trigger objections from SWIFT and the outside auditor.

A SWIFT representative said that Booz Allen Hamilton, an international consulting firm, is the auditor, but provided no further details on how the oversight process works.

Although the searches focus on suspected terrorist activity overseas, U.S. officials acknowledged that they do delve into the financial activities of Americans, noting that privacy laws don't protect individuals believed to be acting as a "foreign terrorist agent."

Officials said the administration has briefed congressional intelligence committees on the SWIFT program. In contrast, information on the NSA wiretapping was shared only with key lawmakers. One senior congressional aide said the committees have "a good handle on what the executive branch is doing to track terrorist financing" and are generally supportive of those efforts.

But the operation seems to have been kept secret from key segments of the banking industry, including senior executives in the United States and overseas.

John McKessy, chairman of the SWIFT user group in the United States, said he was unaware of any such program. McKessy represents companies and institutions that are not members of the SWIFT cooperative, but use its messaging system.

SWIFT noted that its published policies clearly indicate that it cooperates with law enforcement authorities and that the subpoenas were "discussed carefully within the board," made up of members from 25 major banks. SWIFT said it has also kept informed an oversight committee drawn from the central banks of the major industrial countries.

The SWIFT program plugs a gap in global efforts to track terrorism financing.

In the United States, law enforcement authorities can access bank records if they get

permission through the legal process. The FBI also has various legal ways to get almost instantaneous access to financial records. And U.S. banking laws require financial institutions to file Suspicious Activity Reports, but authorities believe Al Qaeda and other terrorist groups know how to evade the activities that trigger such red flags.

U.S. officials, however, long have complained that they cannot get access to financial records overseas and that some requests for cooperation from foreign governments and financial institutions took months, while others were rebuffed.

"The sort of 18th century notions on this stuff drive me nuts," said one senior U.S. counterterrorism official. "Somebody can move money with the click of a mouse, but it takes me six months to find it. If that is the world in which we live, you have to understand the costs involved with that."

The Sept. 11 commission urged the government in its July 2004 report on the U.S. intelligence failures leading up to the terrorist attacks to put more emphasis on tracking the flow of funds, rather than seeking to disrupt them, to learn how terrorist networks are organized.

Lee Hamilton, a former congressman and co-chairman of the commission who said he has been briefed on the SWIFT program, said U.S. intelligence agencies have made significant progress in recent years, but are still falling short. "I still cannot point to specific successes of our efforts here on terrorist financing," he said.

The Washington Post

<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300167.html>

Bank Records Secretly Tapped

Administration Began Using Global Database Shortly After 2001 Attacks

By Barton Gellman, Paul Blustein and Dafna Linzer
Washington Post Staff Writers
June 23, 2006

The Bush administration, relying on a presidential declaration of emergency, has secretly been tapping into a vast global database of confidential financial transactions for nearly five years, according to U.S. government and industry officials.

Initiated shortly after Sept. 11, 2001, the surveillance program has used a broad new interpretation of the Treasury Department's administrative powers to bypass traditional banking privacy protections. It has swept in large volumes of international money transfers, including many made by U.S. citizens and residents, in an effort to track the locations, identities and activities of suspected terrorists.

Current and former counterterrorism officials said the program works in parallel with the previously reported surveillance of international telephone calls, faxes and e-mails by the National Security Agency, which has eavesdropped without warrants on more than 5,000 Americans suspected of terrorist links. Together with a hundredfold expansion of the FBI's use of "national security letters" to obtain communications and banking records, the secret NSA and Treasury programs have built unprecedented government databases of private transactions, most of them involving people who prove irrelevant to terrorism investigators.

Stuart Levey, undersecretary of the Treasury for terrorism and financial intelligence, said in an interview last night that the newly disclosed program -- the existence of which the government sought to conceal -- has used the agency's powers of administrative subpoena to compel an international banking consortium to open its records. The Brussels-based cooperative, known as the Society for Worldwide Interbank Financial Telecommunication, or SWIFT, links about 7,800 banks and brokerages and handles billions of transactions a year.

Terrorism investigators had sought access to SWIFT's database since the 1990s, but other government and industry authorities balked at the potential blow to confidence in the banking system. After the 2001 attacks, President Bush overrode those objections and invoked his powers under the International Emergency Economic Powers Act to "investigate, regulate or prohibit" any foreign financial transaction linked to "an unusual and extraordinary threat."

Levey and other officials emphasized that the government has confined its financial surveillance to legitimate terrorism investigations and tightly targeted searches.

After identifying a suspect, Levey said, "you can do a search, and you can determine whom he sent money to, and who sent money to him."

"The way the SWIFT data works, you would have all kinds of concrete information -- addresses, phone numbers, real names, account numbers, a lot of stuff we can really work with, the kind of actionable information that government officials can really follow up on," Levey said.

He spoke about the program after it became clear the New York Times was planning to publish an article about it. The Times and other news organizations posted articles online last night.

Levey maintained that the government has "put into place very robust controls to make sure we are only using this information for anti-terrorism purposes."

He added: "We can only search the data we receive in furtherance of a terrorism lead. In fact, the analysts who have access to the data can't even access the database unless they type in the search they want to do and articulate why it's connected to terrorism."

The program is "on rock-solid legal ground," Levey said, and is based on the IEEPA, which he said "specifically gives us the authority to conduct this type of investigation if there is an emergency declared by the president."

In addition, the administration informed major central banks, including the Federal Reserve and the European Central Bank, of the program. "They were all briefed so they could exercise appropriate oversight," Levey said. "We have kept it confidential but made sure the appropriate people knew about it," including members of Congress involved in intelligence matters, he said.

The White House complained last night that the disclosure could hurt anti-terrorism activities.

"We are disappointed that once again the New York Times has chosen to expose a classified program that is working to protect Americans," spokeswoman Dana Perino said. "We know that al-Qaeda watches for any clue as to how we are fighting the war on terrorism and then they adapt, which increases the challenge to our intelligence and law enforcement officials."

Levey said it was no secret that investigators tried to follow terrorist money flows, but had been "trying to keep confidential . . . precisely how we do that." Because SWIFT is not a well-known source of financial information, "we're very disappointed that this source has now been revealed, because it will make our job much more difficult."

Levey's boss, outgoing Treasury Secretary John W. Snow, underlined those arguments in a statement the department issued late yesterday. Treasury's Terrorist Finance Tracking Program, he said, is an essential tool in the war on terror that has helped government officials "locate operatives and their financiers, chart terrorist networks, help bring them to justice, and save lives."

"It is not 'data mining,' or trolling through the private financial records of Americans. It is not a 'fishing expedition,' but rather a sharp harpoon aimed at the heart of terrorist activity," he said.

Levey declined to discuss instances in which the data gleaned from SWIFT had aided the crackdown on terrorism. He said that information is classified but added he could confirm that the information has been used to "confirm the identity of a major Iraqi terrorist facilitator."

Asked whether any high-ranking administration officials had expressed reservations about the program, Levey said: "Not that I've ever heard. This is a program which, to my knowledge, has been universally embraced and praised."

Intelligence analysts from the CIA and the FBI, working with Levey's office, have been poring over the financial transactions for the past several years in search of more links to al-Qaeda operatives. Officials said investigators now seek financial data on individuals

and companies whose names first appear in documents, intercepted communications and other evidence gathered by intelligence agencies around the world.

"You can't type in a random name of someone" and search his data, said one intelligence official who spoke on the condition of anonymity. "The program only works for names already within the intelligence system that were collected elsewhere and are identified as being part of an open investigation."

That was not the case when the program began in the weeks after Sept. 11, 2001, when Bush signed Executive Order 13224 going after al-Qaeda's finances. Officials said far more information was collected early on, often on people who had nothing to do with al-Qaeda but whose Muslim names or businesses were similar to those used by suspected members of al-Qaeda. That method flooded the intelligence community with reams of material that was laborious to go through and repeatedly misled investigators.

"It has narrowed over time as our expertise has increased," one official said in describing a "higher bar" for searches that now depend on intelligence collected elsewhere.

Intelligence officials were eager to distance this program from the NSA's eavesdropping operation, saying repeatedly that the technology employed does not allow for the broad sweeps the NSA can conduct.

In a statement, SWIFT said it "responded to compulsory subpoenas for limited sets of data from the Office of Foreign Assets Control of the United States Department of the Treasury. Our fundamental principle has been to preserve the confidentiality of our users' data while complying with the lawful obligations in countries where we operate. Striking that balance has guided SWIFT through this process with the United States Department of the Treasury."