The Money-Laundering Conundrum: Mugging Privacy in the Assault on Crime?[1]

Lawrence B. Lindsey

The nature of the money-laundering conundrum is inherently one of finding a balance, a balance of reason. The crux of the lesson I learned at the Federal Reserve was that we need to restore some reason and balance to the discussion of privacy. As a country, we have a strong commitment to privacy. We have discovered in our Constitution that we actually have a right to privacy—although the Founding Fathers never wrote that down—and yet we see constantly an assault on our privacy, an erosion of our privacy, both by the state and also by the private sector.

There is no question the threats posed by international terrorists and drug cartels are a serious threat to our national security and to our individual liberty. But it is also true that threats to our individual liberty by a potentially-abusive government exist as well. As citizens, we must use what was recommended to us—eternal vigilance over our government, not a one-time, fix-it solution—to make sure that the right balance is being struck.

Why is it an issue of balance? Consider the issue of money laundering. Using the term "crime" loosely, in the sense of something that is socially harmful, the use of money is not the crime. The reason we are interested in it is because it's the flip-side of a criminal transaction that is socially harmful. The government has a temptation because it is very hard to enforce the laws it has on the books against the real criminal activity. It finds it much easier to track the money trail and use it as a proxy for the criminal activity. Whenever you are going to use a proxy, a non-socially-harmful proxy, you had better raise the issue of balance and reason.

In his speeches, Richard Rahn raises the issue of Japanese internment during World War II. Although in some ways an unfortunate example because of its emotional force, it is also an appropriate one. The Supreme Court wrestled with taking an innocent characteristic, believing it to be correlated with a real or potential threat, and using that characteristic to enforce the law. That's exactly what is happening with money-laundering laws: The government is using the otherwise innocent characteristic of spending money, which it believes may be correlated with criminal activity, in order to enforce the law. In the case of Japanese internment, history suggests that where balance and reason were struck then differs from what we would find today. The justices of the Court at the time found the balance they struck appropriate. This underscores the point of why we are going to need eternal vigilance: Circumstances are going to change.

Another important point to understand about money laundering is that, because we are dealing with an innocent characteristic, the law can be overly-broad. The Financial Crimes Enforcement Network (FinCEN) argues that standards of conviction under the money-laundering statutes are in fact quite narrow. FinCEN maintains that one must know when using currency that it was obtained through the fruits of illicit activity. This is one reason why we are not seeing a lot of convictions for money laundering.

But it also raises a real problem, because of the issue of fungibility. For example, suppose a cabinet nominee who wasn't confirmed due to failure to pay nanny taxes—a potentially criminal activity—spent money. Was the precise unit of currency spent the same dollar saved by not paying the nanny taxes? No, of course not. That is not what is meant by the law. In fact, money is fungible. So, because of the fungibility of money, any time you use currency, assuming you have ever committed any criminal activity in the past, you theoretically could have engaged in money laundering. Again, what is necessary is to find the place of balance and reason.

Prosecutorial discretion and juries are what we now rely upon to decide where that balance and reason exist. But even under the supposedly-narrow definition of the law that FinCEN uses,

we have a literally unlimited application of that law to anyone engaging in any transaction who has ever committed a crime, or knows that they have committed a crime. And given that we are not a society of saints, but rather one of minor sinners, that unfortunately is probably most of us.

It is important to look at the issue of costs. We no longer require a reasonable basis to try to track the money flows. The government has implicitly decided that it needs to trace all money flows and be able at its leisure to look at that great collection of data and see if it can detect any suspicious information. Take, for example, what happens with currency-transaction reports, the main way in which the government gathers information. The government requires us to file a form any time we use currency to what it considers an excessive amount, typically any deposit over $10,000.[2]

Between 1987 and 1995, the government collected 77 million currency-transaction reports, something on the order of 62 tons of paper. Out of that, it was able to prosecute 3,000 money-laundering cases. That is roughly one case for every 25,000 forms filed. In other words, entire forests had to be felled in order to prosecute one case. But it gets worse: Of the 3,000 money-laundering cases prosecuted, the government managed to produce only 580 guilty verdicts.[3] In other words, in excess of 100,000 reports were filed by innocent citizens in order to get one conviction. That ratio of 99,999 to one is something we normally would not tolerate as a reasonable balance between privacy and the collection of guilty verdicts.

There is another angle: Since banks are used as enforcement agents, the Treasury Department engages in sting operations to monitor compliance. FinCEN officials go to a bank and tempt it to commit a crime. Between 1990 and 1995, 290 defendants were charged as a result of sting operations, with 29 convictions.[4] That's one in 10. And that's out of thousands of sting operations. By any standard of cost-benefit analysis, we are asking for a lot of compliance to catch a few people. Merely analyzing the situation from the viewpoint of the use of scarce government prosecutorial resources, this practice does not make the grade.

But there should be more in the calculus besides scarce government resources. There is the invasion of our privacy, which doesn't seem to enter into the calculation.

It is worth remembering that the people being caught are on the money side. It is impossible to imagine the counterfactual here, but we also are forced to live with the existing level of global terrorism, the existing level of drug lords. How much hypothetical reduction we get is supposedly the benefit. But if you actually look at the people we've managed to prosecute, it looks kind of small compared to the burden of paperwork and the number of people who have to engage in required activity to comply with the law.

This compliance burden is only getting greater. For example, in my last year at the Federal Reserve we approved a rule that if you wish to transfer or "wire" more than a certain amount of money domestically, a report needs to be filed. This covers all sorts of situations, often seen in TV ads—"Hey Dad, I need $200 to pay the rent, can you wire it to me?" Any time that figure exceeds $750, the people who provide you with this service are required to keep records on you. They have to know who you are; they have to keep information on you in their files, all for having allowed you to wire $750. That's just the starting point.

The number of tangible pieces of paper that have to be filed may be shrinking, largely because records can be kept on magnetic tape. But whether we're talking about pieces of paper, computer bytes, or reels of tape, lots of reports are being filed. For example, consider the Suspicious Activity Report. According to FinCEN, suspicious activity is defined as any suspicious transaction involving possible violations of law—a definition no doubt helpful if you are trying to enforce the law. Regulations issued under the Bank Secrecy Act require banks to report their customers as "suspects" whenever the banker has "reason to suspect" that a large transaction is unusual for the customer and the "bank knows of no reasonable explanation for the transaction."

In 1993, of the roughly 10 million currency-transaction reports filed, 63,000 were marked suspicious[5]—a number that should give an idea of the level of overcompliance. The 0.6 per-

cent share resulted in a 1 percent rate of criminal charges. But the banks had produced an important degree of filtering for the law-enforcement professionals. It was therefore the regulators' hope that a more sophisticated screening of the data would produce an even more efficacious ratio of "suspicious" to "probable cause" than 100 to one. The requirement that banks monitor all their customers' transactions could conceivably be advanced as making government more efficient, not nosier. Hence the "Know Your Customer" rules proposed—and withdrawn under intense pressure—in early 1999.

The number of reports labeled suspicious has roughly doubled, because banks are becoming much more concerned about getting it wrong. If a financial institution does get it wrong, it is subject to penalties. That is the nature of what could be termed overly-broad enforcement. We don't know where to draw the line—we don't know if it is $750 for a domestic transfer or $3,000—but it is important, given our obligation for eternal vigilance, to keep these numbers in mind.

Another concern too seldom considered is the disproportionate impact of these rules on the least-fortunate people in society. I never appreciated this issue until I was on a community tour in Denver in the Five Corners neighborhood of the city. I was visiting the first bank to open in Five Corners since World War II. It is a low- and moderate-income area, now predominantly African-American. A lady came up to me and said, "You folks in Washington think we are all drug dealers, don't you?" I asked what she meant by that and she replied:

> I had saved money for a down payment on a house and, of course, there being no banks, I saved it at home. I brought in the cash to the bank for the closing and they didn't believe me. They wouldn't accept it. They wouldn't accept US currency for the down payment on this house that I'd saved all my life for.

This is the chilling effect that these laws have on a society in which roughly 15 percent of our citizens are unbanked.[6] And

that percentage climbs to nearly 25 among lower-income families. They do not have access to the traditional mechanisms that much of the rest of society uses to engage in financial transactions. They are the ones who must use cash; they are the ones who must use those wire services to transfer money so the daughter can pay the rent. Just watch or listen to the commercials; individuals who are unbanked are exactly those being targeted. With our rules, the government is actually creating an impediment to commerce for those who need access the most.

But when FinCEN considers making exceptions, it makes exceptions like, "You don't have to file a report if you are a company traded on the New York Stock Exchange." This does nothing for the people who really bear the burden of this law, who are those in the low- and moderate-income populations of America.

Indeed, the enforcement mechanism here is rather troubling. Consider, just as a random example, a Treasury Department release from May, 1997, announcing the results of a Geographic Targeting Order. Under the Bank Secrecy Act, FinCEN can tell any group of people that any set of transactions is subject to particularly-close monitoring. And the particularly-close monitoring in this situation was any wire order going to Colombia. The people who were covered by it, which included 3,500 different sources of wire transaction, were largely located in the Colombian neighborhoods of New York City. If any bank in the US had pursued such a policy, it would immediately have been hit with civil-rights complaints, probably justified. But that was not a problem for FinCEN because that was, in fact, the target population.

Suppose, though, that you are a bank caught in this net. You have a problem, because the activity reports are confidential. If you deny performing a wire transfer for someone based on the activity report, you might be sued. But you are not allowed to use the Suspicious Activity Report in your defense, even though the report is the reason the government told you that you couldn't perform the service. So you are subject to a violation of civil-rights law, and you cannot use something in your defense which the government ordered you to use in the first place.

How did this work out in this instance? The banks were caught in the middle. The government trumpeted as a success the fact that there was a 30 percent drop-off in money being transmitted to Colombia. They particularly noted that business to Colombia dropped off even at money remitters not subject to the Geographic Targeting Order, suggesting that much of the money remitted to Colombia was controlled centrally by high-level cartel money brokers. But that doesn't necessarily follow. If I hear that the government is looking at all money going to Colombia, and I am planning to remit my $800 to my family after working all month to earn it, I might get nervous fearing I might go to jail. Not to mention the fact that the banks executing the transmission might decide to say no.

This is the unspoken other cost. I am not for money laundering; I am not for drug trafficking; I am not for gun running. The question is, how do we most effectively enforce the law? The answer, returning to our central premise, is eternal vigilance. Balance and reason will decide. And we have overstepped the bounds of balance and reason today.

The difficulty of striking a balance between stopping criminals and safeguarding privacy is not a new one. America's founding fathers faced a similar dilemma. It is interesting to recall how they saw the balance when they wrote the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

The presumption was that a search warrant would be issued, and it would specify who was targeted for search and what information was to be seized. It would seem to be clear that current money-laundering-enforcement practices are the kind of blanket search that the writers of the Constitution sought to prohibit.

Somehow "probable cause" does not seem to mesh with the one in 25,000 odds that the currency-transaction reports provide.

The reason all of this has passed constitutional muster may say more about the circumscription of our privacy than we care to admit. The government has argued with a straight face that it is not carrying out the search—the banks are. In examples such as the currency-transaction reports, the government claims that all it is doing is requiring an informational document from entities (that is, banks) which it has the power to regulate.

So the government has gone too far. But I don't think that we can politically separate invasions of privacy by the government from invasions of privacy by the private sector. Many of us may think that the erosion of privacy by the state and by the private sector are separate issues. In fact, they probably are not. They certainly are not separate in the minds of the public. A fine, theoretical case why that should be so can be made. After all, when I give information to my bank, it is a contract and we can negotiate the contract and the market can dictate the solution, and I can be there if you want me to be there. But that's not a very useful political argument, despite its useful rhetorical value. The real political problem is when the bank uses that information to call me at 6 o'clock at night, just when my family is sitting down to dinner, to market some additional service to me. I find that a much more intrusive invasion of my privacy than I do if the government is theoretically collecting currency-transaction reports, and so I resent it more.

The financial-services industry obviously wants to be able to use information for marketing purposes much more, particularly as it is developing into a more-comprehensive industry from a balkanized one. But it should be very careful to resist the temptation to invade people's privacy. It is joining not the side of the angels, but the side of the state. Obviously, there is an incentive for the financial-services industry instead to line up on the side of the individual citizen, to affirmatively resist invasions of privacy, both by the state and by the private sector.

The key point is that the financial-services industry today should be very careful who it makes a deal with. It has every

interest to be on the side of privacy. When it makes deals in the interest of marketing, which result in erosions of privacy, it is in the end undercutting its own base.

Notes

[1] This article is a compilation of Dr. Lindsey's views principally derived from remarks he gave at CEI's conference on financial privacy, held on November 30, 1999.

[2] Bank Secrecy Act, Public Law 91-508.

[3] "Clean Getaway for Money Launderers," *The Journal of Commerce*, December 10, 1996.

[4] Ibid.

[5] "Money Laundering: Needed Improvements for Reporting Suspicious Transactions Are Planned," GAO report GGD-95-156.

[6] "Banking Relationships of Lower-Income Families and the Government Trend Toward Electronic Payment," *Federal Reserve Bulletin* (July 1999). The actual number is 12.6 percent.