After her parents retired, Duong followed in their footsteps and opened her own restaurant, The Lemongrass Café;, bringing a taste of her native land to her new home. I ask my colleagues in the Senate to recognize and pay tribute to this remarkable woman.

Mr. President, I ask unanimous consent that the article, ''Restaurant a testament to Vietnamese family's drive'' from The Courier-Journal, be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

[From the Louisville Courier-Journal, Feb. 22, 2004]

RESTAURANT A TESTAMENT TO VIETNAMESE FAMILY'S DRIVE

(By Byron Crawford)

The Lemongrass Cafe in Louisville's Highlands neighborhood is more than a quaint oasis for Thai, Vietnamese and Chinese cuisine. It is a monument to one Vietnamese family's appetite for freedom and opportunity.

The cafe's proprietor, Hanh Thai Duong, 34, was 10 years old in 1979 when the Vietnamese government told her parents that because of her father's Chinese ancestry the family would be allowed to leave Vietnam—if they gave up all their possessions and paid the government a sum in gold.

''You really leave empty-handed, but my mom and dad were thinking for a better future for their children,'' Duong said. ''My parents always said that the United States was the land of opportunity. We left on a fishing boat for Hong Kong.''

Such voyages were treacherous. The boats were small and often unsafe.

The trips sometimes took weeks. Twenty to 30 passengers jammed into tight quarters and often went days without food. Pirates roamed the South China Sea, sometimes boarding the fishing vessels, killing, raping and taking women and children captives.

''We were lucky. It only took us four or five days to reach Hong Kong, but my aunt and her twins did not get to Hong Kong . . . for like a month or so, and one of the twins died of hunger and they ended up burying her out at sea,'' Duong said. ''As soon as my aunt stepped on the ground in Hong Kong, she passed away, too.''

Duong's baby sister was badly burned in an accident soon after the fishing boat reached Hong Kong Harbor and was taken to the mainland for treatment. The family lost track of the child for months but finally found her in a refugee camp. Duong's mother, not having seen the baby for months, did not immediately recognize her.

Another of Duong's aunts, who then lived in Louisville, sponsored the family to immigrate in 1980, and they were flown to America by Catholic Charities, which they later repaid. Duong's father, Trung Thai, had owned a successful grocery-supply business in Vietnam, and her mother, Nga, was a good cook. They opened a small restaurant from which they have since retired.

Duong married at an early age but was determined to get an education, and she worked her way through the University of Louisville to earn a degree in finance and international business. She and her husband, Edward Duong—who had twice been captured while trying to leave Vietnam in violation of government orders—later lived in New York City. But they soon decided that they preferred Louisville, where Edward Duong now works at Ford's Kentucky Truck Plant.

Hanh Duong's older brother and younger sister both earned degrees from UofL and are working in business. Another sister owns a nail salon and her youngest sister is working her way through college.

''You think about your parents' sacrifice for you and you don't want to fail,'' she said. ''You don't take things for granted and you don't give up easily.''

Duong has forgotten much of her early life in Vietnam, but a few vivid memories remain: one of her parents running with her for shelter as bombs exploded nearby, and her mother being wounded by a stray bullet near their home in Saigon (now known as Ho Chi Minh City).

Today, Duong works hard in the Lemongrass Cafe, on Bardstown Road to make happier memories for her children—a daughter, Cheryl, 17, a senior at Male High School and a Governor's Scholar who will enter the University of Kentucky next fall, and a son, Nick, 9, a student at Greathouse/Shryock Traditional Elementary School. Many of their grandmother's favorite recipes are helping to lure customers to their mother's cafe.

''Other than the delicious food, I guess it was just the simplicity of Lemongrass and the personality of Hanh that I like about the place,'' said Jeannie Treitz, a frequent customer.

A few years ago, Hanh said, she took her children to Vietnam to show them the country their parents and grandparents had fled.

''They were raised here and they don't know how people have to struggle in Vietnam,'' she said. ''I took them back so they could understand that they have bundles of opportunities here, and that they should work hard and never give up on anything.''

RFIDS AND THE DAWNING MICRO MONITORING REVOLUTION

Mr. LEAHY. Mr. President, today I outlined some of the privacy challenges we will soon face as new micro monitoring technologies begin to proliferate in our society. I spoke in particular about breakthroughs in Radio Frequency Identification, also known as RFID.

My remarks were offered at Georgetown University Law Center, during a conference on the legal and technological challenges of video surveillance. Micro monitoring is a subject that deserves the attention of the Senate and of the American people, and I ask unanimous consent the text of my address be printed in the RECORD in the interest of advancing this discussion.

There being no objection, the material was ordered to be printed in the RECORD as follows:

THE DAWN OF MICRO MONITORING: IT'S PROMISE, AND ITS CHALLENGES TO PRIVACY AND SECURITY

In our post-9/11 world, technology often has been our crucial but silent partner in helping us to ramp up our law enforcement and national security capabilities. We in this city are profoundly aware of the new risks we face. But we also need to do it right. The public does not want false assurances, nor do they want to be unduly alarmed. What the American people want is to actually be safer. And we still have a way to go in accomplishing that.

TENSION BETWEEN LIBERTY AND SECURITY

In our constitutional system there is always tension between liberty and security and never more so than since September 11th. One of the difficult challenges we face is to strike the right midpoint. Our constitutional checks and balances are intended to help us do that.

The video technologies you are discussing today offer tools that are better, faster and smarter, on scales of magnitude that are unprecedented. As an advocate of emerging technologies who also has a keen interest in them, I watch these breakthroughs with great interest.

I have sought to find ways to encourage the commercial sector to create new products and opportunities, and I have promoted use of new technologies by law enforcement agencies, while also protecting consumer privacy and constitutional freedoms. That was the balance I sought to strike in my work on CALEA and in other legislation that blends law enforcement's needs, the needs of our robust technology sector, and the privacy interests of the American people. The hands-off approach to the Internet that I have favored is another example, and right now I am working with others to extend the Internet tax moratorium, to keep the Internet free from discriminatory and multiple state and local taxes.

ON THE CUSP OF A MICRO-MONITORING REVOLUTION

The marriage of information-gathering technology with information storing technology, manipulated in increasingly sophisticated databases, is beginning to produce the defining privacy challenge of the information age. Modern databases, networks and the Internet allow us to easily collect, store, distribute and combine video, audio and other digital trails of our daily transactions. We are on the verge of a revolution in micro-monitoring the capability for the highly detailed, largely automatic, widespread surveillance of our daily lives.

RFIDS

And one of the most dramatic and dazzling new challenges we all will be facing soon is the emergence of a relatively new, surveillance-related technology called radio frequency identification—R–F–I–D for short.

RFID tags are tiny computer chips that can be attached to physical items in order to provide identification and tracking by radio. Their potential invasiveness is obvious from their size, which already is surprisingly small. And they will only get smaller.

In their basic function, RFID chips are like barcodes, which by now are ubiquitous in our stores and offices and crime labs and manufacturing plants.

BARCODES ON STEROIDS

But RFID chips are like supercharged barcodes—barcodes on steroids, if you will. They are so small they can be tagged onto almost any object. They do not have to be in open view; RFID receivers just have to be within the vicinity—at a security checkpoint, in a doorway, inside a mailbox, atop a traffic light. And RFID chips can carry a lot more information than barcodes. Some versions are recordable so that they can carry along the object's entire history.

RFID chips are more powerful than today's video surveillance technology. RFIDs are more reliable, they are 100 percent automatic, and they are likely to become more pervasive because they are significantly less expensive, and there are many business advantages to using them. RFIDs seem poised to become the catalyst that will launch the age of micro-monitoring.

I have followed RFID technology for some time and have welcomed its potential for many constructive uses. I have supported the use of RFIDs in a Vermont pilot program for tracking cattle to curtail outbreaks, like mad cow disease, and our Vermont program

is now being emulated for a national tracking system. RFID technology may also help thwart prescription drug counterfeiting, a use the FDA encouraged in a recent report. Leading retailers like Wal-Mart and Target—as well as the Department of Defense—are requiring its use by suppliers for inventory control. Fifty million pets around the world have embedded RFID chips. Of course, many of us already have experience with simpler versions of the technology in ''smart tags'' at toll booths and ''speed passes'' at gas stations.

But this is just the beginning. RFID technology is on the brink of widespread applications in manufacturing, distribution, retail, healthcare, safety, security, law enforcement, intellectual property protection and many other areas, including mundane applications like keeping track of personal possessions. Some visionaries imagine, quote, ''an internet of objects''—a world in which billions of objects will report their location, identity, and history over wireless connections. Those days of long hunts around the house for lost keys and remote controls might be a frustration of the past.

These all raise exciting possibilities, but they also raise potentially troubling tangents. While it may be a good idea for a retailer to use RFID chips to manage its inventory, we would not want a retailer to put those tags on goods for sale without consumers' knowledge, without knowing how to deactivate them, and without knowing what information will be collected and how it will be used. While we might want the Pentagon to be able to manage its supplies with RFID tags, we would not want an al Qaeda operative to find out about our resources by simply using a hidden RFID scanner in a war situation.

DRAWING LINES

Of course these are just some of the foreseeable possibilities, and a lot depends on enhancements in the technology, reductions in costs, and developments in voluntary standard-setting, systems and infrastructure to manage RFID-collected information. But the RFID train is beginning to leave the station, and now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy rights.

The need to draw some lines is already becoming clear. Recent reports revealed clandestine tests at a Wal-Mart store where RFID tags were inserted in packages of Max Factor lipsticks, with RFID scanners hidden on nearby shelves. The radio signals triggered nearby surveillance cameras to allow researchers 750 miles away to watch those consumers in action. A similar test occurred with Gillette razors at another Wal-Mart store.

These excesses suggest that Congress may need to step in at some point. When privacy intrusions reach the point of behavior that is absurdly out of bounds, we find ourselves having to deal with such issues as the ''Video Voyeurism Prevention Act,'' a bill now before Congress that would ban the use of camera to spy in bathrooms and up women's skirts, a practice that by now has even been given a name, ''upskirting,'' which I'm sure is as new to you as it is to most of us in Congress.

Other powerful new technologies are on the horizon, like sensor technology and nanotechnology. All the more reason to think about these issues broadly and to establish guiding principles serving the twin goals of fostering useful technologies while keeping them from overtaking our civil liberties.

With RFID technology as with many other surveillance technologies, we need to consider how it will be used, and will it be effective. What information will it gather, and how long will that data be kept? Who will have access to those data banks, and under what checks-and-balances? Will the public have appropriate notice, opportunity to consent and due process in the case mistakes are made? How will the data be secured from theft, negligence and abuse, and how will accuracy be ensured? In what cases should law enforcement agencies be able to use this information, and what safeguards should apply? There should be a general presumption that Americans can know when their personal information is collected, and to see, check and correct any errors.

These are all questions we need to consider, and it is entirely possible that Congress may decide that enacting general parameters would be constructive. It is important that we let RFID technology reach its potential without unnecessary constraints. But it is equally important that we ensure protections against privacy invasions and other abuses. Technology may also help with the answers—for example, ''blockers'' that deactivate RFID tags, and software that thwarts spyware.

BEGINNING A NATIONAL DIALOGUE

There is no downside to a public dialogue about these issues, but there are many dangers in waiting too long to start. We need clear communication about the goals, plans and uses of the technology, so that we can think in advance about the best ways to encourage innovation, while conserving the public's right to privacy.

We have seen this time and time again where a potentially good approach is hampered because of lack of communication with Congress, the public and lack of adequate consideration for privacy and civil liberties.

Take for example the so-called CAPPS II program. No doubt in a post-9/11 world, we should have an effective airline screening system. But the Administration quietly put this program together, collected passengers' information without their knowledge and piloted this program without communicating with us and before privacy protections were in place. The result was a recent GAO analysis that showed pervasive problems in the screening program and admissions that we are now set back in our efforts to create an effective screening system.

As another example, the Administration recently funded the MATRIX program to provide law enforcement access to state government and commercial databases. This was potentially a useful crime-fighting tool. But there was insufficient information about the program and about potentially intrusive data mining capabilities, and there were unaddressed concerns about privacy protections. Now 11 out of 16 states participating in the program have pulled out—many, citing privacy concerns—thus hampering the effectiveness of the information sharing program. Again, had some of these issues been vetted in advance, we may have been able to enhance law enforcement intelligence.

Just recently, there were reports about the FBI's new Strategic Medical Intelligence program, in which doctors have been enlisted to report to the FBI ''any suspicious event,'' such as an unusual rash or a lost finger. The goal of preventing bio-terrorism is important. But there are many unanswered questions about the program's privacy protections and its ability to identify truly suspicious events and not unrelated personal medical situations. Hopefully, this program will not be hampered by lack of communication and oversight.

I have written oversight letters to the Justice Department and to the Department of Homeland Security on all of these issues and am waiting for their responses.

I want to make sure that mistakes like those are not repeated, especially with RFID technology, where there is so much potential value. That is why I asked to speak with you today, to begin the process of encouraging public dialogue in both the commercial and public sectors before the RFID genie is let fully out of its bottle.

This is a dialogue that should cut across the political spectrum, and it should include the possibility of constructive, bipartisan congressional hearings. The earlier we begin this discussion, the greater the prospects for success in reaching consensus on a set of guiding principles.

When several of us from both parties banded together years ago to found the Congressional Internet Caucus, we were united by our appreciation for what the Internet would do for our society. Years later, we remain united, we remain optimistic, and partisanship has never interfered in the Caucus's work.

That is the spirit in which I hope a discussion can now begin on micro-monitoring.

Thank you for your interest in these cutting-edge issues, and thanks for this opportunity to share some ideas with you.

BUDGET SCOREKEEPING REPORT

Mr. NICKLES. Mr. President, I hereby submit to the Senate the budget scorekeeping report prepared by the Congressional Budget Office under Section 308(b) and in aid of Section 311 of the Congressional Budget Act of 1974, as amended. This report meets the requirements for Senate scorekeeping of Section 5 of S. Con. Res. 32, the First Concurrent Resolution on the Budget for 1986.

This report shows the effects of congressional action on the 2004 budget through March 22, 2004. The estimates of budget authority, outlays, and revenues are consistent with the technical and economic assumptions of the 2004 Concurrent Resolution on the Budget, H. Con. Res. 95, as adjusted.

The estimates show that current level spending is above the budget resolution by $14.1 billion in budget authority and under the budget resolution by $222 million in outlays in 2004. Current level for revenues is $244 million below the budget resolution in 2004.

This is my first report for the second session of the 108th Congress.

I ask unanimous consent that the report be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 23, 2004.

Hon. DON NICKLES,
Chairman, Committee on the Budget,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The enclosed tables show the effects of Congressional action on the 2004 budget and are current through March 22, 2004 (the last day that the Senate was in session before the recent recess). This report is submitted under section 308(b) and in aid of section 311 of the Congressional Budget Act, as amended.