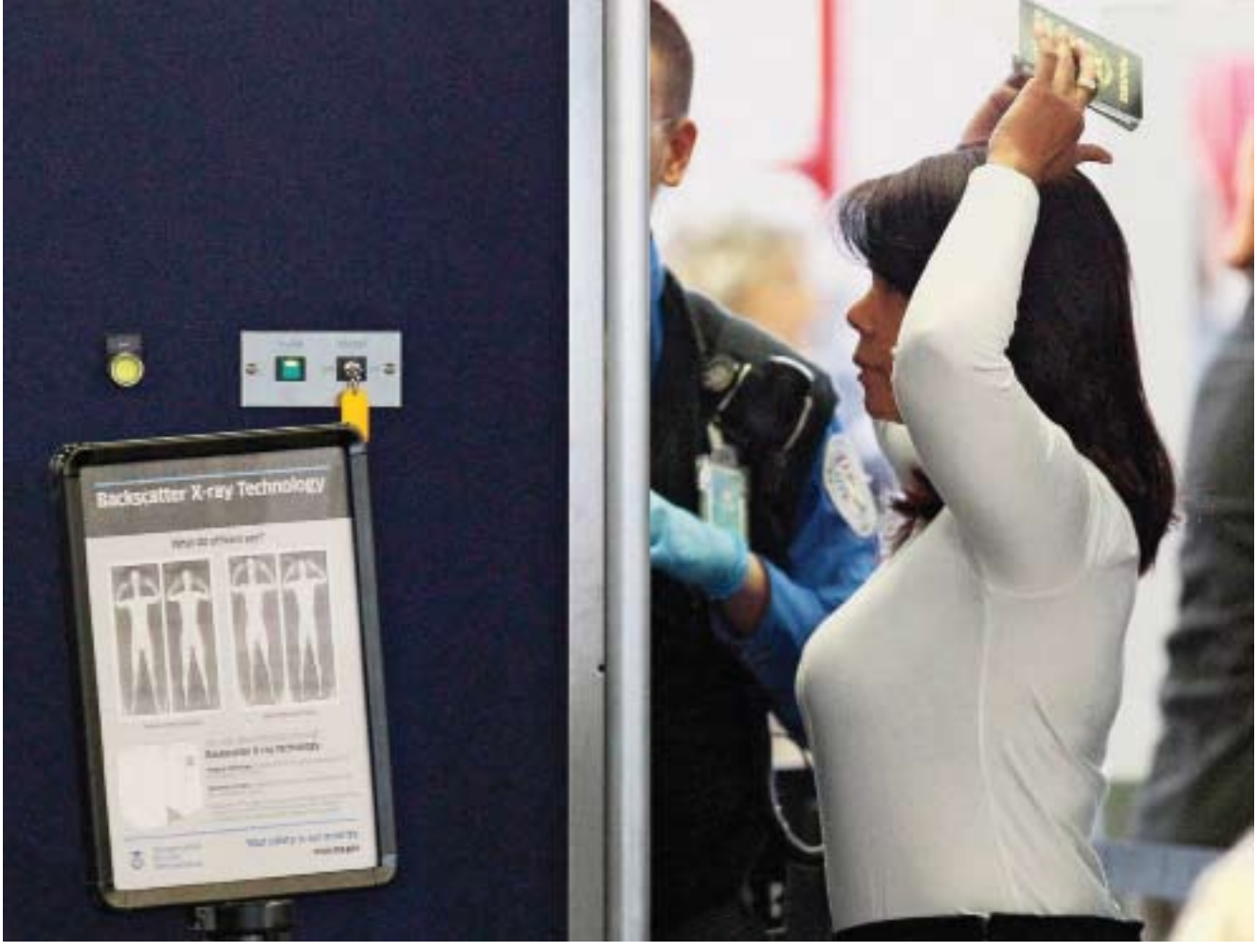

Hands up: *Some experts believe that tough new airport screening methods are inefficient at identifying ever-changing terrorist threats*

CHARLES REX ARBOGAST/AP

SECURITY

DON'T TOUCH MY JUNK

Are Canada and the U.S. sacrificing privacy in the name of security?

AS STEPPED-UP U.S. airport security has American Thanksgiving travellers boiling over pat-downs and naked-body scanners, Canada is getting ready to open up some more private records for Uncle Sam to look at. Starting next year, U.S. authorities will be able to collect personal information, which may include passport details and flight itineraries, for the roughly five million Canadians who cross U.S. airspace every year travelling to destinations such as Mexico, Latin America and the Caribbean, even if they never touch U.S. soil.

On both sides of the border a new round of government peeking in the name of security is refocusing minds on an old question: do we really need to do this? Increasingly, people north and south of the border are saying no. But the backlash is also raising debate about how we can best protect our borders while also minimizing the impact on privacy rights. Neither Canada nor the U.S.—whose systems are increasingly more closely intertwined—seem close to striking the right balance, experts argue.

Most travellers are all too familiar with the rather indelicate efforts by officials to manage security and privacy (U.S. privacy advocates have even adopted "Don't touch my junk" as their latest rallying cry in opposition to heightened screening). But is all this "creating security or just a sense of security?" asks Sukanya Pillay at the Canadian Civil Liberties Association. Not since new security measures were adopted after the 9/11 terrorist attacks has so much attention been focused on privacy concerns. Privacy champions maintain that border-security policies represent a bad bargain between privacy and security: we give up a lot of privacy, but it doesn't seem we get much security in return.

That's because a strategy based on massive personal data collection and identical screenings for 99 per cent of travellers is not very efficient at spotting an ever-changing terrorist threat, says Noah Shachtman, an editor at *Wired* magazine and non-resident fellow at the Brookings Institution, a think tank in Washington. Shachtman calls it "the assembly line process." Every airport passenger passing through security undergoes a number of tech-centric controls, such as screening, scanning and checks by highly classified algorithms (which security experts believe assess potential threats based on individuals' data such as travel history, arrest records and intelligence). Most of the time, though, airport passengers go through "with no question asked from a human being," says Shachtman. It amounts to chasing after the objects and methods that would-be bombers used the last time—as if they won't come up with something new—and using statistics for "searching for a needle in a haystack," according to U.S. security guru Bruce Schneier.

So does border security need a serious rethink? It's a question privacy advocates in Canada have made considerable noise about, but with little result. When it comes to national security matters, Canadian privacy watchdogs are struggling against not just their own government, but also that of their powerful neighbour down south, which, Pillay says, has been

influencing the terms of aviation and border security in Canada since 9/11.

Earlier this month, privacy and security experts met in Toronto to talk about Canada-U.S. border relations as part of the One Issue Two Voices debate series organized by the Woodrow Wilson International Center for Scholars. The discussion made it clear that when governments grapple with balancing security and privacy, the scales inevitably tip toward security. Ottawa's chief preoccupation on border matters has been to reassure America about Canada's ability to deal with terrorism threats, said Brian Stewart, a speaker at the event and a CBC host who has spent time inside the Canadian Security Intelligence Service. Levels of anxiety at CSIS about keeping Washington confident were "striking," said Stewart.

INTELLIGENCE SHARING TAPS WERE OPENED BEFORE WE HAD A TOOL FOR ASSESSING COMMON THREATS, SAYS WARK

This insecurity over managing the border with the U.S. seems to date back to the "Millennium Bomber" case of 1999, when Ahmed Ressam, an al-Qaeda operative who had claimed refugee status in Canada, tried to enter the U.S. with a car trunk full of explosives. Ressam had been able to remain in Canada for five years and evade deportation with a false Canadian passport—a failure that made U.S. officials queasy. But the incident held important lessons that both sides could have learned from. Ressam was caught at the U.S. border in Port Angeles, Wash., after a U.S. customs agent noticed that he was fidgeting and looked sweaty—the same type of behavioural assessment method that the much-vaunted Israeli airport security heavily relies on, and that some privacy and security experts say we'd be better off using.

Instead, governments went on an information gathering rampage. Eager to assuage U.S. concerns about Canada's ability to secure the border, Ottawa agreed to unprecedented levels of intelligence sharing with Washington without a clear idea of how best to use the information. "Intelligence taps were opened to maximum flow before we had a tool for assessing common threats," Canadian security expert Wesley Wark wrote in a report published by the Woodrow Wilson Center in advance of its debate series. (Canada's Public Safety Minister Vic Toews and U.S. Secretary of Homeland Security Janet Napolitano promised to produce a document outlining joint border threats, but it hasn't been released.)

Working against Ottawa's ability to address border privacy issues is the fact that Canada's privacy watchdog might not have enough teeth to influence government policy on crucial questions of security. Dragging federal institutions to court when they refuse to step in line on privacy issues is about the scariest thing the Office of the Privacy Commissioner can threaten to do. And although a spokesperson for the office noted in an email that "organizations typically implement the commissioner's recommendations," the federal privacy commissioner remains "a player on the peripheries of the national security debate in Canada—one still devoted to tilting at occasional windmills," according to Wark's report.

WHEN THE U.S. GOVERNMENT WANTS TO SUCK UP PRIVATE DATA UNNECESSARILY, 'I CAN SAY NO,' EXPLAINS CALLAHAN

South of the border, things look quite different, though not necessarily better. Mary Ellen Callahan is the chief privacy officer at the Department of Homeland Security and was Wark's counterpart in the Woodrow Wilson Center debate. When the department comes up with plans to suck up private data unnecessarily, "I can actually say no," thundered the U.S. official to a mostly Canadian audience. Rather than having an independent watchdog reviewing policies, she said, the U.S. has taken to embedding privacy officers right into federal agencies, so that they can vet and check new rules as the government thinks them up. Her ammunition, she added, includes powers to veto and cut funding to programs she's not "happy with."

But for all of the show of firepower by people with jobs like Callahan's, they don't seem to have had much of an impact on America's handling of privacy rights when it comes to security matters, according to security expert Schneier. Be it because privacy watchdogs haven't been using their powers to the extent that they should, or that a lot of the databases are actually exempt from their scrutiny, he says the government has been far too ready to stick its nose into citizens' private business—a view shared by many more libertarian Americans, and one that has been on full display in the current uproar over airport security.

Indeed, as imperfect as the Canadian system may be, the U.S. model is not one that should be looked on with envy, said Wark, who is also an associate professor of history at the University of Toronto's Munk School of Global Affairs. Privacy watchdogs operating inside government, he says, work "within the conventions of a bureaucracy and within the conventions of a pecking order," which probably undermine their effectiveness. The U.S. approach, he adds, also seems "very siloed," with each privacy officer scrutinizing their realms and unable to spot and address how initiatives cooked up by other agencies might impact their own department. Regardless of these finer institutional differences, anywhere in the world "national security policies in general are not shaped around privacy," says Wark.

But the current passenger backlash at underwear searches and flashes of nudity could mean governments might soon need to take another hard look at how to balance security and privacy. This time, we'll be the ones watching. **ERICA ALINI**

On the Web: The One Issue, Two Voices speaking series is presented by the Woodrow Wilson International Center for Scholars in co-operation with *Maclean's* and presenting sponsor IBM. Go to *macleans.ca/oneissuetwovoices* for links to the full text and video of Mary Ellen Callahan's and Wesley Wark's presentations.

PHOTOGRAPHS BY ANDREW TOLSON