Forbes

For International Travelers, Reviving The Fourth Amendment

By: Doug Bandow, Senior Fellow at the Cato Institute
May 27, 2013

I cross America's borders several times a year. May was especially busy, with four foreign trips. That's unusual, and my aging body is much the worse for wear as a result. But at least border agents may be less likely to search and seize my computer in the future.

Travelers, even citizens, enjoy few privacy protections when returning to America. In 1886 the U.S. Supreme Court ruled that border searches were exempt from the Fourth Amendment. Federal officials could look at whatever you were carrying or wearing. No evidence of wrong-doing was required.

The issue still came up from time to time, but in 1977 the high court stated that border searches generally were considered "reasonable simply by virtue of the fact that they occur at the border." In 2004 the Supreme Court reaffirmed the existing rule, citing the interest in protecting the nation from "unwanted persons or effects." At the same time, the justices opined that travelers were entitled to a lesser expectation of privacy.

Nevertheless, in 1985 the Supreme Court *did* limit the government's reach, ruling that "reasonable suspicion" of criminal conduct was necessary before detaining or strip-searching a traveler. Even Roy Altman, an Assistant U.S. Attorney who advocates wide discretion for border agents, called this "an understandable standard." However, the new rule was not applied to personal possessions, even those on which privacy might be expected, such as a password-protected computer, smart phone, or digital camera.

Only once in three decades of traversing the globe have I been forced to hand over my computer and provide the password. I suppose I could have refused the latter demand, but then my computer likely would have spirited away for safe-cracking elsewhere. And though the process was offensive, I really had nothing to hide.

My computer is filled with data files containing years of boring policy articles, such as this one. The music for my iPod is saved there, but that would pose a problem only if the border guards really disliked the Bee Gees, ABBA, and Motown. There also are some travel photos, but other than a few surreptitious shots of Afghan military sites and Israeli check-points, most of them are not very interesting either.

And, in fact, the customs official only spent a few minutes puttering around—looking at what I have no idea—before handing back my computer. It was irritating, but didn't spur me to action.

Over the years other people have gone through the same process and were sufficiently outraged to complain publicly. But efforts to get Congress to act went nowhere. Nor have the courts intervened. In 2005 the Fourth Circuit Court of Appeals in Virginia rejected a challenge to a computer search. More than 6500 routine computer checks were conducted between October 2008 and June 2010 alone.

However, it is far worse when the government takes the computer for more detailed review, often at another location if additional technical assistance is required. Two years ago The Constitution Project issued a report on the issue, "Suspicionless Border Searches of Electronic Devices: Legal and Privacy Concerns with the Department of Homeland Security's Policy."

The group explained: Customs and Border Protection and Immigration and Customs Enforcement "officers may detain electronic devices for significant periods of time. For CBP, detentions can be extended well beyond the minimum five-day guideline with supervisory approval. If the device is detained by ICE, the detention can last for 'a reasonable time,' which according to its Directive can last 30 days or more." Neither agency sets any firm time limit.

The Constitution Project argued that the issue goes beyond Fourth Amendment concerns. If reasonable suspicion of criminal activity is not required, how do federal agents go about deciding whose computer to search and seize? The Congressional Research Service acknowledged that "If a customs official could conduct a search without providing cause, it would be difficult to deter ethnic profiling because the official would not need to explain why he conducted the search." (Of course, some believe that ethnic profiling would improve law enforcement, but if so, it should be carried out openly.)

However, in April a case originating six years ago finally emerged from the Ninth Circuit Court of Appeals. *U.S. v. Cotterman* demonstrates how the law-abiding majority enjoy many constitutional liberties only because the law-breaking minority fights for those protections to avoid jail. The result often isn't pretty—and raises complaints about the guilty going free because of constitutional "technicalities"—but nevertheless benefits the rest of us.

On April 6, 2007 Howard Cotterman and his wife drove back from Mexico. Cotterman had been convicted of multiple counts of child sexual misconduct fifteen years before, so customs seized his two computers and three digital cameras, sending the computers and one camera with password-protected files on for forensic analysis. Child pornography was discovered, leading to his indictment. He sued to suppress the evidence.

The federal district (trial) court agreed, only to be reversed on appeal by the three-judge panel of the Ninth Circuit. Then an "en banc" hearing with 11 judges was held. The 8-3 majority included Chief Judge Alex Kozinski, a Reagan appointee.

The majority acknowledged the federal government's broader than usual powers at the border, but noted that border agents' authority was not unlimited. In 1985 the Supreme Court ruled that privacy rights did not disappear but were to be "balanced against the sovereign's interests."

The majority pointed to the totality of the circumstances, noting that had the search simply involved a quick review of the laptop's contents there probably would have been no constitutional objection. However, "the search here transformed into something far

different," a "forensic examination that comprehensively analyzed the hard drive of the computer."

The intrusiveness of the search, ruled the majority, required "reasonable suspicion." Although the border review standards were different, they were not nonexistent. Concluded the majority: "Notwithstanding a traveler's diminished expectation of privacy at the border, the search is still measured against the Fourth Amendment's reasonableness requirement, which considers the nature and scope of the search."

The dissenters complained that the majority improperly treated differently someone who hid digital child pornography on his computer and "hid" printed child pornography in his briefcase. They asked: "is the mere fact that Cotterman chose to save his child pornography electronically, rather than print it out on paper, enough to invoke" the Supreme Court's expressed exception applied to routine border searches carried out in a "particularly offensive manner"? But there are important differences.

One is that international travelers know that their belongings are subject to visual search since the federal government may levy import duties, and therefore must be able to determine if one is bringing in new items, including printed materials. A briefcase and printed materials also are inherently less secure against private snoops as well as government investigators than password-protected computer files.

Moreover, as the appellate majority observed, "The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information." In addition, data remains encoded even after being formally deleted. While it is easy to separate the business and personal as well as the innocent and incriminating among personal effects, it is not so easy to similarly divide computer files. Concluded the judges: "A person's digital life ought not be hijacked simply by crossing a border."

Of course, Cotterman's offenses were horrid. Still, despite the government's strong interest in combating sexual crimes, noted the court, "legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information. Reasonable suspicion is a modest, workable standard that is already applied in the extended border search … and other contexts."

A separate issue was whether "reasonable suspicion" existed in Cotterman's case. That was a factual question to be determined in the eye of the beholder. No one likes allowing a child molester to go free, and this may have encouraged majority to rule that the border agents met a standard which they did not know existed.

Decided the Ninth Circuit: "we conclude that the examination of Cotterman's electronic devices was supported by reasonable suspicion and that the scope and manner of the search were reasonable under the Fourth Amendment." For that reason, the evidence was allowed to stand. (Ironically, the dissenters doubted the majority's answer to this question, calling—with the better case, I believe—the purported evidence "a rather weak lynchpin for reasonable suspicion.")

The Cotterman ruling—which may reach the Supreme Court, since the Fourth and Ninth Circuits are in apparent conflict—would not have prevented the cursory search of my

computer. But it does limit the intrusiveness of searches that the government can mount without the barest suspicion of criminal behavior.

Roy Altman complained that this modest limit would "make it harder for customs agents to protect the country when it is ever easier to smuggle contraband." Yet the internet allows the more sophisticated or better prepared to send contraband ahead or behind and avoid the border search entirely.

More important, every constitutional protection, including (indeed, especially!) the Fourth Amendment, makes it harder for government agents to "protect" the country in some way. The challenge is finding balance, and Americans always have placed a strong emphasis on liberty. The fact that some people are guilty is not a good reason to treat everyone as guilty.

Perhaps the best justification of the Ninth Circuit's ruling is the Department of Homeland Security's explanation last year of why it rejected any limit to its power. Speaking in the royal "we," DHS stated: "We conclude that CPB's and ICE's current border search policies comply with the Fourth Amendment. We also conclude that imposing a requirement that officers have reasonable suspicions in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits."

If the agency cannot discern the civil liberties benefits of keeping government agents out of my computer, then DHS desperately requires serious oversight and, more important, firm limits. Happily, the Ninth Circuit provided both.

Congress should codify the court's rules into law, while adding additional safeguards, both restricting when searches may be made and how information viewed may be used. Even without legislative action the Obama administration should issue new directives restricting suspicionless border searches and requiring warrants for extended forensic investigations. Traveling internationally should not require sacrificing one's basic freedoms.