

No Terrorism Toll on Privacy -- Yet

Jay Cline

April 2, 2002 ([Computerworld](#))

Much ink has been spilled since Sept. 11 over the prospect of big brother rising from the grave to steal Americans' civil liberties. Tales of privacy lost and due process ignored have buried last summer's headlines about dot-com layoffs. Even calmer heads are ruing the unabated swing of the pendulum from privacy to security. But what has really happened to Americans' privacy since the declaration of war on al-Qaeda?

If a nationwide loss of privacy has occurred, we should be seeing at least one of the following scenarios: a widespread expansion in the scope of the government's collection of personal data, courts setting dangerous legal precedents or a surge in the number of people harmed by abuses of government-collected data. These are the speed bumps on the road from liberty to tyranny, and none has been crossed.

What has happened since Sept. 11? Some airports are reportedly screening travelers' faces against a database of terrorist suspects. If you're a terrorist, the cameras will be watching, thank heaven. But if you're everyone else, your mug is neither being stored nor adored by the men behind the lens. There simply aren't enough resources at cash-strapped airports to devote to such ambition.

Some cities, notably Washington, are following Britain's lead in deploying cameras in public areas. This certainly evokes images of George Orwell's *1984*. But the privacy of pedestrians strolling K St. -- if such privacy exists -- is no more affected by remote surveillance than it is by a lawyer peering out his window to the street below.

Computerworld recently reported that federal transportation officials are exploring a new system to screen airline travelers for suspicious

backgrounds and relationships ([see story](#)). They're probably hoping to spot Arab men flying on one-way tickets from New Jersey or Detroit to cities far away. But if you're a family flying to a spring break destination, your privacy won't be touched. Human eyes won't review your pooled data.

The Patriot Act, passed in October, gave the FBI new powers to monitor the e-mail of suspected terrorists. Internet service providers will reportedly cooperate with the FBI to conduct packet filtering of messages to and from previously identified individuals. So if you're mixed up with a terrorist suspect, your missives will be read and, I hope, an agent will knock on your door before it's too late. But the FBI certainly hasn't taken it upon itself to conduct random keyword searches of all the e-mail coursing through the servers of U.S. ISPs.

The Patriot Act also enables government agencies to share more law-enforcement information. Many Americans think the federal government already has a huge big brother computer file on each person. But the reality is that big brother is a hodgepodge of little cousins -- the same sort of motley collection of stovepiped and uncoordinated databases that most large corporations have.

So far in the war on terrorism, there has been no widespread increase in the government's collection of Americans' personal data. No perilous bridges have been crossed, and there is no pattern of government abuses of personal data stemming from Sept. 11. The congressional oversight committees have certainly been busier, but so far, we haven't seen any members seeking hearings on privacy abuses. It's a good sign when Congress can't find legs on an issue during an election year.

The privacy speed bumps haven't been crossed -- yet. But off on the horizon, a menacing silhouette continues to vanish and reappear. Proposals for a national identification card were dead until Sept. 11, but then were resurrected as a way to better control the border against terrorists. While good in theory, a national ID card would invite a

widespread centralization of personal data beyond the wildest dreams of ID thieves -- some of whom await their next orders to attack the U.S. ([see story](#)).

Our government workers are doing all they can to protect our freedom and our security. We can help them by not creating distractions from legitimate homeland defense.

Cline manages data privacy at Carlson Companies Inc., a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. Contact him at privacy@computerworld.com.