If privacy protection is the goal, we might want governments to do quite a bit less, not more.

Marc Rotenberg's opening statement catalogues many things governments could stop doing if they want to aid our privacy protection. His organisation, EPIC, indeed fought the American National Security Agency's "clipper chip" proposal, which would have given authorities a back door into encrypted communications. The Federal Bureau of Investigation's "Carnivore" system likewise would have given the government an ability to "sniff" e-mail and other electronic communications. Total Information Awareness was an American government plan to aggregate every scrap of data about people—internet surfing, e-mails, phone calls, purchases, payments, auto tolls, travels and so on—then sift through it all looking for wrongdoing.

As Mr Rotenberg notes, EPIC now leads the charge against deployment of "strip-search machines", devices that reveal the naked body to government officials at airports and other checkpoints. In respect of airports, few locations so bristle with government intrusions on privacy—intrusions that are not a balanced response to the threat of terrorism. For example, the Department of Homeland Security collects ten fingerprints from foreign visitors (potential terrorists, all!). The US-VISIT programme holds this biometric data for an astounding 75 years.

Under the Western Hemisphere Travel Initiative, US citizens now must show a passport when they return from shopping trips to border towns in Canada and Mexico. The American government was a prime mover behind the "e-Passport", a computer-chipped travel document that allows its contents to be read at a distance by radio. Governments are experimenting with other RFID-chipped cards that allow people's identifying information to be scanned and entered on a database as they traverse borders and internal checkpoints.

If government ID cards do not capture people's movements, perhaps surveillance cameras will. Here, the British government seems to have the lead. Reportedly, there is one camera for every 14 people in the country, and 20% of cameras globally are in Britain. Governments worldwide are collecting DNA from their subjects for a growing variety of reasons.

We need not think only of direct surveillance, of course. Governments have a large role in creating structural bias against privacy in the protocols and technologies around us. Take the American Social Security number (SSN). Akin to many social insurance and national ID numbers around the world, it is a national identifier that has propelled forward the tracking that Mr Rotenberg rightly worries about. Immediately after mandating workers to apply for an SSN in 1936, the American government began promoting it for more and more uses: first state unemployment insurance programmes, then taxpayer identification, purchase of savings bonds, various welfare and entitlement programmes, and so on.

In 1970, America's Federal Bank Secrecy Act required financial-services providers to obtain their customers' SSNs and use them in reporting information to the government. The financial-services industry made lemonade from these lemons. It got much better at tracking customers for marketing and promotional purposes. As it consolidated in the early 1970s, the credit-reporting industry similarly organised itself around the uniform national identifier that had been created, propagated and promoted by the government over the preceding 35 years.

The practices Mr Rotenberg objects to are not just facilitated and propelled forward by government regulation and programmes. Governments are leading participants in this information economy. As Mr Rotenberg points out: "Government agencies are often the top clients of those companies in the data broker business. And what governments cannot buy they can often obtain through legal authority and data retention mandates."

In June, Mr Rotenberg participated in a debate in which he faced Mike McConnell, former director of the National Security Agency (NSA) and director of National Intelligence. Mr Rotenberg was rightly flabbergasted to hear Mr McConnell deny that the NSA had illegally conducted warrantless internet surveillance, even though a federal judge found it illegal earlier this year, and even though Congress two years ago saw fit to immunise the telecommunications companies that participated in the programme.

The American government, like others around the world, is a voracious information collector. It facilitates and promotes private-sector tracking and surveillance. It skirts and sometimes violates laws intended to restrain its snooping, and it cannot be held accountable when it does.

This does not seem like the kind of institution one would turn to for privacy protection. "Independent privacy agencies" and government bodies like the tiny, well-meaning American Federal Trade Commission do not tip the balance the other way.

People who want privacy have no better resource to turn to than themselves. Being more careful with personal information—learning how internet communications work, withholding personal information more often and meting it out carefully when appropriate—is the only reliable privacy protection. The next most important step is limiting government access to private-sector information, something on which Mr Rotenberg and I agree, though he may not prioritise it as much, preferring to pursue regulation of private business instead.