Re: Comments on Total Information Awareness Program

I hope my unique perspective adds something to the debate. These are comments, not arguments. I'm not arguing for or against the program, just providing some different ways of looking at the problem.

While in an ideal world, government would not have the right to collect personal information, the problem is that the technology to do so exists. So long as the technology exists, it will be used. It is simply not possible to "put the genie back in the bottle."

Now, I am not suggesting that the President, the Joint Chiefs of Staff, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation or the Director of the National Security Agency will break the law. Such people are generally (although not universally) disinclined to do anything unlawful. (You are probably more skeptical than I on this issue.) Their subordinates, however, are another story.

If a low level investigator for the counterintelligence branch of the FBI is tasked with determining whether you or I are terrorists, he has two choices. He can get up early, tail us, work long hours, interview lots of people, follow up on many leads, etc. That's hard work. Alternatively, he can call a friend with access to the technology to tap our phones, read our email, and get copies of our credit card statements. That's unlawful. But, he's never going to get caught and it's a lot easier. I guarantee you he does it the easy way.

Look at your own organization. Suppose you want a new desk and you ask your administrative assistant to get you one. He or she is probably supposed to fill out some kind of form requesting a capital expenditure, submit it to some obscure bureaucrat, make numerous phone calls working it through the system, and respond to your exasperated inquiries for months. Of course, anyone effective as an administrative assistant makes friends with the facilities management folks and simply calls them and asks them for a favor. The financial records of the enterprise are misstated to the extent of a capital expenditure not properly recorded, or the inventory of the assets of the enterprise become even more inaccurate as assets are relocated without corresponding records. But, you get a desk.

My experience as in-house counsel for several large companies has convinced me that senior management has little control over the acts of employees more than one level below them, and those employees will often do the wrong thing. I suspect that this is as true in government as in the private sector.

Sometimes employees do the wrong thing for "good" reasons. They will rationalize violations of antitrust or environmental law, financial reporting or accounting standards, or – in the case of government employees – the rights of citizens as being for the common good.[1] Others, of course, do the wrong things because they benefit from doing so. Regardless of motivation, employees take short cuts.[2]

---

[1] Academically, this is the problem of excessive risk tolerance by individuals with insufficient liability exposure, either because they are the beneficiaries of corporate risk management programs (insurance and indemnities in corporate by-laws) or sovereign immunity, or their assets are so small in relation to the magnitude of potential liability so as to eliminate personal liability as a practical matter, or both.

[2] I have a somewhat non-traditional background. I had a client that brought an a patent infringement case involving a chemical process patent. The defendant sought to minimize its damage exposure by claiming that as soon as it discovered my client's patent, it changed its process. I told our litigation team that there is no way they changed the process. When they asked how I could be so sure, I asked if any of them had ever worked as chemical operators in a chemical plant. Of course, none had. I, however, spent more time than I care to

To some extent, regulation improves control. By authorizing, and regulating, what is going to be done anyway, society improves its knowledge of what is going on and its control over the disfavored activity.

Then, there is the question of why our government should not know what other governments know. Your phone calls, email and credit card records may be nobody's business but yours, but there are a lot of folks looking at them. If our government does not review this email before you read it, Mossad and MI6 (and probably the French, the Russians and maybe the Chinese) certainly will.

Over the course of my life I have had several occasions to bump into our government's intelligence apparatus and covert activities, and all I can say is that truth is far, far stranger than fiction.[3] Both our government and the KGB were monitoring all international data and voice traffic in the 1960's. There is no reason to believe that Mossad, MI6 and a host of others cannot monitor data and voice traffic within the United States now. [In fact, my hypothetical FBI counterintelligence agent investigating whether you or I are terrorists would call a friend at Mossad, not NSA.]

Finally, privacy is an issue of recent concern because citizens see the power of technology. But, privacy in fact disappears as soon as records are kept.[4] While the volume of data has increased with increasing use of computer technology, privacy has not diminished. The precision of personal information has perhaps improved (I will refrain from expressing any opinions about accuracy), but there has been no appreciable privacy for the last 40 years.

---

remember in such a job and I learned that if the chemist for the process told the workers on Tuesday that they were going to make the same product as on Monday, but had to add an additional step, they would do it as instructed on Tuesday, and maybe on Wednesday. But, by Thursday, they would "forget" the new step to see if anyone noticed. After all, the workers are uneducated, but they're not stupid and the new step cuts into valuable break time. I told the litigation team not to waste a lot of time deposing the chemists (I believed that they were telling the truth.). Instead, I instructed them to thoroughly audit the batch sheets looking for time inconsistencies. Turns out that the defendant only used the new process 20 days in 3 years (the first few days and then from time to time when the big shots were watching, like when the customer came to visit).

[3] I first learned of BZ, the drug possibly used by the Russians to overpower the kidnappers in Moscow recently, in 1974 or so. It is (basically) a hallucinogenic drug that is universally unpleasant and debilitating and was developed by our government back in the early 1950s (it was the subject of a classified patent in 1953). Ever heard that the CIA and the Army administered LSD to soldiers and citizens? Never happened. The drug was BZ, not LSD. Worried about anthrax or smallpox? Don't be. There are antidotes and vaccines for these. Imagine a virus, universally fatal, transmissible by inhalation and for which there is no human vaccine for general administration – even in development. Such a virus is available and information about it is not classified (it is the subject of a lengthy reported district court opinion in a products liability action brought by an unfortunate researcher).

[4] Back in the mid-1980s I represented a number of clients in a large environmental matter involving a hazardous waste hauler operated by organized crime (real big in metropolitan New York where I'm from). The principals of the waste hauler had all gone to prison (except for one, which is another amazing story that taught me a lot about how government operates, but that's another story) and the company had been the subject of a Chapter 7 proceeding 13 years earlier.

I had to determine the extent of my clients' transactions with this company in great detail. In fact, my defense was premised on the routes used by the truck drivers employed by the waste hauler and the sequence of their pickups and deliveries. I found the company's financial records at a Navy storage facility used by the bankruptcy court on a pier in Bayonne, New Jersey. Using these as a starting point, I was able to locate additional records from diners, truck stops, etc. In the end, I knew when each of the drivers had taken an extra 15 minutes for lunch. The Mob enterprise that was the subject of my 1980s case ceased operation in 1972 and, I promise you, had no computers. Recordkeeping was not a priority. Yet, the employees of that company had no privacy. Any government agent could have done the same investigation I did.