# Craig S. Mullins
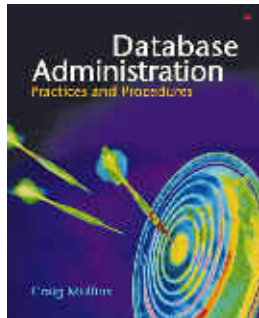
April 2006

## The DBA Corner
*by Craig S. Mullins*

### Data Security and Privacy: Concerns of the DBA?

As organizations and governments acquire more and more data, all the while clamoring for even more data, DBAs will likely be drawn into areas that heretofore mostly have been foreign to them. DBAs will be asked to move away from their tried and true technical comfort zone, into the more ambiguous gray area of ethics and morality as it concerns data.

One of the biggest growing concerns for those of us who deal with data on a daily basis will be the impact of analyzing and mining large volumes of data. This brings along with it many issues including security, personal privacy, and the potential for abuse.

It is one thing for companies with which you do business to maintain data relating to your transactions. It is another thing if your personal information is to be gathered from multiple sources and analyzed for details of your personal life – details that can make it easier for someone to assume your identity or to eavesdrop on your actions. But technology and the US political climate are collaborating to makes such analysis more common place.

Consider for example, a recent story in the Christian Science Monitor, ([US Plans Massive Data Sweep](#)). This article describes a US government effort called ADVISE, an acronym for Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement. ADVISE is a little-known system that is basically a big data mining program gathering information from multiple sources (blogs, government records, intelligence reports, and so on). When I first read this article, I immediately thought about George Orwell's *1984* and drew dire implications for personal privacy.

However, if we think about this a little bit longer and deeper we can perhaps conjure up more reasonable thoughts. It should not be a big concern when an operation such as ADVISE is sifting through data in the public domain. But it can become potentially problematic when data that

you think is personal becomes public. My e-mails, my purchases, the books I check out of the library - these are things I hope to be personal. Assuming that this is so, or will be so in the future, seems to be naive.

But what responsibility does a company have with its customers concerning their data. Should my ISP be able to guarantee the security of my e-mail such that no one can access it? Perhaps on their servers but can anyone guarantee what happens to data as it floats through the ether from originator to destination? And is it unreasonable to assume that the government might try to force ISPs to turn data over? This is not that far-fetched given the recent attempt by the US government to get Google to hand over data from its search operations.

Shouldn't the details of my credit card records be only between me and the credit card company? I can understand a credit bureau needing information on current balances, but no one should be able to gain access to what I bought and where I bought it. Should they?

Even more to the point, shouldn't the details of our financial transactions be private? Once again, they are not, even today – for example, the US federal government is informed about every transaction exceeding $10,000. Given today's political climate, your data will likely continue to be made more "available."

Much of the drive to assemble information from multiple sources and mine it seems to be driven by efforts to combat terrorism. Now I

understand the desire to catch and thwart terrorists. I am all in favor of that. I just don't know how much freedom we should be willing to give up in order for that to happen. As Ben Franklin put it, much more elegantly than I ever could, "Those who would sacrifice freedom for security deserve neither."

So what can a DBA do about all of this? Well, perhaps not much at this juncture. But be prepared for some extreme requests on your data. It looks like the government will be asking for it – and in more ways than just this one, especially when you take a look at government regulations and compliance requirements, such as the Sarbanes-Oxley Act. But that is a whole different kettle of fish, which frankly, I applaud. I like it when government regulations force companies to take care of their data as they should already be doing. I just worry a bit when the government (or a private corporation, for that matter) decides it wants to know *everything* about me.

From Database Trends and Applications, April 2006.