Excerpts from

September 11 and the Imperative of Reform in the U.S. Intelligence Community

Additional Views of Senator Richard C. Shelby

Vice Chairman, Senate Select Committee on Intelligence

December 10, 2002

“Interestingly, an ongoing project by the Information Awareness Office (IAO) of the Defense Advanced Research Projects Agency (DARPA) suggests that while such data interoperability would be enormously useful, it may not be an absolute prerequisite for meaningful “deep access” data-mining within the Intelligence Community, the U.S. Government, or beyond. The SSCI has been following with great interest IAO’s work on what it calls its “Total Information Awareness” (TIA) project, for this project holds out the prospect of providing the technological tools to achieve radical analyst empowerment vis-á-vis the IC’s entrenched information-holders.

“TIA aspires to create the tools that would permit analysts to data-mine an indefinitely expandable universe of databases. These tools would not be database-specific, but would rather be engineered in such a way as to allow databases to be added to the analytical mix as rapidly as interface software could be programmed to recognize the data formats used in each new database and to translate queries and apply specific “business rules” into a form usable therein. Through this system, TIA hopes to enable an analyst to make search requests – either on a name-by-name basis or in order to apply sophisticated pattern-recognition software – to each among a “cloud” of remotely-distributed databases. Each analyst user would possess a complex set of individual “credentials” which would be embedded in each query and “travel” with that query through the database universe. These credentials would include information such as the user’s access permissions and the specific legal and policy authorities under which each query has been conducted; they would tell the system what sorts of responses that user is permitted to get.[71] Even when the user did not have authority to see certain types of information, the system would be able to tell the analyst whether any data responsive to his query existed in any particular database, allowing him to submit a request for access to higher authority.[72] Information responsive to user queries would then be passed back through the system to an automated data repository, where it would be stored for analytical exploitation.[73]

[70] *Id.*

[71] The TIA project also contemplates a system of “selective revelation of in formation,” whereby initial responses to a query would indicate merely the presence of responsive entries or patterns. Subsequent queries – and per haps additional levels of authority – would be needed for the analyst to “bore deeper” into the data.

[72] This helps analysts get avoid the “you don’t know what you don’t know” dilemma, yet without compromising particularly sensitive information to unauthorized individuals.

“The TIA approach thus has much to recommend it as a potential solution to the imperative of deep data-access and analyst empowerment within a 21st-century Intelligence Community. If pursued with care and determination, it has the potential to break down the parochial agency information “stovepipes” and permit nearly pure *all* source analysis for the first time – yet without unmanageable security difficulties. If done right, moreover, TIA would be infinitely scalable: expandable to as many databases as our lawyers and policymakers deem to be appropriate.[74]

“TIA promises to be an enormously useful tool that can be applied to whatever data we feel comfortable permitting it to access. How broadly it will ultimately be used is a matter for policymakers to decide if and when the program bears fruit. It is worth emphasizing, however, that TIA would provide unprecedented value-added even if applied exclusively *within* the current Intelligence Community – as a means of finally providing analysts deep but controlled and accountable access to the databases of collection and analytical agencies alike. It would also be useful if applied to broader U.S. Government information holdings, subject to laws restricting the use of tax return information, census data, and other information. Ultimately, we might choose to permit TIA to work against some of the civilian “transactional space” in commercially-available databases which are already publicly and legally available today to marketers, credit card companies, criminals, and terrorists alike. The point for civil libertarians to remember is that policymakers can choose to restrict TIA’s application however they see fit: it will be applied only against the data-streams that our policymakers and our laws permit.

“I mention TIA here at some length because it represents, in my view, precisely the kind of innovative, “out of the box” thinking of which I have long been speaking – and which Americans have a right to *expect* from their Intelligence Community in the wake of a devastating surprise attack that left 3,000 of their countrymen dead. It is unfortunate that thinking of this sort is most obvious in the Defense Department rather than among Intelligence Community leaders, and more unfortunate still that projects like TIA are likely to encounter significant *resistance* from the entrenched information-holders at the core of the traditional IC. Nevertheless, projects like this represent a bright spot in the Community’s baleful recent history of counterterrorist information sharing.”

[73] IAO officials have told committee staff that DARPA envisions the possibility of supporting analysts with semi-automated functions that would “learn” from the behavior of large numbers of other users on the system, “pushing” data out to users working on specific topics in ways loosely analogous to the way in which the software at Amazon.com recommends books to browsers based upon what *other customers* who selected a particular title also picked.

[74] What’s more, the TIA architecture is being designed to create elaborate audit trails upon the initiation of each query. These audit trails, which would be accessible to intelligence oversight organs, would be specially encrypted and secured against tampering, and would allow overseers to hold each accredited user accountable for activity undertaken within the system and information gleaned therefrom. Moreover, developing TIA will apparently not involve the use of any data from actual per sons (*e.g.*, information about real Americans). IAO plans to construct a “virtual” economy filled with huge numbers of “synthetic” person al transactions by millions of hypothesized people. A “red team” would develop and “carry out” attacks within this virtual environment, role-playing the parts of individual terrorists in order to create transactional trails. The software developers would then try to develop programs to identify these pattern s of “terrorist” transactions, picking them out of the “noise” of the “synthetic” civilian transactions in which they will be embedded. This approach, DARPA hopes, will identify the best ways to identify real terrorists while minimizing the system’s intrusion upon the transactional records of *non*-terrorists.