Biography of Daniel J. Gallington

Daniel J. Gallington is a Senior Research Fellow at the Potomac Institute for Policy Studies, in Arlington, Virginia. At Potomac, he leads and supports studies and projects related to the dynamics between technology, privacy and national security. Mr. Gallington most recently served as Deputy Assistant Secretary of Defense for Territorial Security in the Office of the Secretary of Defense while also serving as Special Assistant for Special Operations and Combating Terrorism to the Undersecretary Defense for Policy, among other positions and was awarded the Secretary of Defense Medal for Outstanding Public Service. He was Chief Counsel to the National Commission for the Review of the National Reconnaissance Office, General Counsel to the Senate Select Committee on Intelligence, Deputy Counsel for Intelligence Policy at the Department of Justice, Legal Advisor for Intelligence Oversight in the Office of the Secretary of Defense, Executive Director for the Defense Policy Board, as a member of the U.S. Delegation to the Nuclear and Space Talks with the (former) Soviet Union. A former Air Force Officer, Mr. Gallington served tours in Europe, Asia, the Pacific, and with the Strategic Air Command. Mr. Gallington received B.S. and J.D. degrees from the University of Illinois, and an LL.M degree in international law from the University of Michigan Law School.

Statement of
Mr. Daniel J. Gallington, Senior Fellow, Potomac Institute for Policy Studies
Before the
U.S. House of Representatives
Permanent Select Committee on Intelligence
April 9, 2003
"Securing Freedom and the Nation: Collecting Intelligence Under the Law"

Chairman Goss, Congresswoman Harmon, and other distinguished Members of the Committee, thank you for inviting me to talk about Project Guardian, which we started at the Potomac Institute for Policy Studies last year. This project serves as a national forum for debate on the dynamics between civil liberties, and new, primarily informational technologies in context of the war on terrorism.

I have provided a statement for the record, and have attached a number of materials that have been produced by the project, which is continuing. In fact, our next event is May 8th, and will address the evolution and dynamics of the authority for collection of information about "U.S. Persons"—we hope that you can attend or send a staff member.

What I have for you here are a few comments and preliminary observations; these assessments are my own, and I don't want to associate them with the Potomac Institute or Project Guardian—we still have a long way to go in our work.

First: I am pleased to report that we encountered more basic agreement than I initially thought was possible—however, I won't speak for the various individuals and

organizations that we have asked to participate. I encourage you to ask for a wide spectrum of views on these issues, as we have.

An example of basic agreement is that we have to do two basic things simultaneously—evaluate and enable new technologies, and protect our civil liberties—and not do one at the expense of another.

Well, the Devil is in the details of how we do both, but even then the various approaches are not necessarily inconsistent. There are a number of ways to evaluate technologies in this context, and I suggest that we take a closer look at the way laboratories in the intelligence community create and evaluate technology that could affect civil liberties. As we know, such laboratories have in existence approved guidelines and procedures which this committee reviews, and which address these dynamics.

I'm not suggesting that this research should be done in intelligence laboratories, it should be done in the labs and organizations best suited for the work, wherever that is. I am saying that we have some very good models to follow and we should follow them.

Second: With regard to all new technologies that affect the privacy of Americans, we should stick with what we know; and again, I believe that we should look to the whole intelligence community and apply its thirty years of experience in dealing with "U.S. Person" information: what it is, who can collect it and under what circumstances, how it

is disseminated and controlled. This is at least a place to start—even though these new technologies may well end up in some non-intelligence context.

Third: We should remember that there are significant differences between the *technology* to collect information, and the *authority* to collect it; also, that all information collection regimes need to be policed, and audit trails need to be created for which a senior person is accountable. In this context, new authorities may be needed for new technologies.

Finally, we also need to understand that the generalized assembly or collection of data is different than targeting a person or an activity. In fact, with so much data, and the technical ability to look at so much of it, the operative, and I submit, the legally relevant act, is ultimately as much how the data is associated with an identity as it is the limitations on collecting or initially sorting the data.

In short, what we have with regard to new information technologies is far closer to the dynamics we have already confronted with regard to the collection and use of SIGINT—and we should look to how we have structured that oversight regime for models, for new oversight regimes, if we determine they are needed for new technologies. Thank you.