

The background features a large, light blue watermark of the Potomac Institute for Policy Studies logo. The logo is circular with a scalloped outer edge and contains the text 'POTOMAC INSTITUTE' at the top and 'POLICY STUDIES' at the bottom. In the center of the logo is a stylized graphic of a shield with a sword and a scale of justice.

Project Guardian

Maintaining

Civil Liberties in the

Information Age

Dan Gallington
Potomac Institute

The Technology Challenge to Privacy

- We want to stop terrorists before they attack.
- Technology facilitates *more rapid* collection and analysis of “publicly available” data to identify potential terrorist activity.
- Much of the relevant information involves “U.S. Persons”

The Challenge to Information Sharing

- Different agencies collect and disseminate different categories of information under different rules and procedures.
- Those rules reflect the mission of the agency.
- The problem: agencies do not share information because they may be legally precluded from doing so, they perceive other information as “unhelpful” to their mission, there are a lack of vehicles for information sharing, and bureaucratic culture.

I. Introduction to Project GUARDIAN

The Development of Structures and Processes that Guarantee our Civil Liberties and Privacy while Accessing Vast Amounts of Data in the Pursuit of Terrorists.

Goals

- **Provide a public forum for the discussion of protecting privacy and personal liberties, while aggressively pursuing those who would bring harm to the US.**
- **Drive the discussion to produce practical and implementable options for accomplishing both missions (protection of civil liberties and aggressive pursuit of terrorists).**
- **Ensure development of realistic options that will be considered and implemented by involving civil libertarians, government and congressional leaders.**

Issues

- **Use of vast amounts of data for the protection of the public against terrorists.**
- **Development of policy and process to guarantee the information is used appropriately.**
- **Development of processes to continually review and oversee use of data to facilitate enforcement of policy.**
- **Laws, regulations, and precedent for sharing data within government and between the private sector and government.**

Process

- **Design and conduct several forums (round table discussions, seminars, public presentations, etc.) to serve as a vehicle for the development, presentation, and discussion of various options for accommodating both civil liberties and pursuit of the terrorists.**
- **Consolidate the best options into a set of recommendations that can be acted on by Congress and the administration (legislation, EO, regulation).**
- **Publish the results in forums designed to raise public awareness and support (press conferences, public hearings, etc.).**
- **Provide the results of the above to Congress in the form of testimony and briefings to members.**

Developing a Solution

- Define new categories of information with different legal status.
- Use existing precedents and processes for information collection and dissemination as models, i.e. current structures of judicial and Congressional oversight.
- While the technology is still in a formative stage, evaluate and set certain standards for privacy protection that can be built into the new technologies, e.g. anonymization.

II. Core Concepts

- **Anonymity**
- **Security**
- **Identity**
- **Privacy**

“Rights” to be Anonymous

- Where do they come from?
- Are they Constitutional? If so, which?
- What does “anonymous” mean? –
distinction from “privacy”
- What is the interest of the State?
- Effect of impersonation, deception or
conspiracy

What are the Security Interests?

- The assurance that people are (in fact) who they say they are.
- A way to link databases to find out what is known about a specific person.
- Economic impacts of terrorist attacks (and preventing them).
- Ensuring identity and accountability in commercial transactions.

European Experience

- Population Control Acts
- Identity Cards/Passports
- Wartime Experience
- Preference for Government, vice
Commercial custody of Personal data
- Has it in fact resulted in better security?
 - E.g. Madrid

Oversight and Public Confidence

- What are the minimum public assurances?
- What are the maximum inconveniences?
- What are the costs and tradeoffs?
- What are the risks and how well can they be articulated?
- How should oversight be structured?
- Role of Congress, Courts and technology?

III. Relevant American History

Congressional Reactions to

- **Criminal Process– “activist”
Supreme Court of the 60’s**
- **Watergate Investigation**

Criminal Process: “activist” Supreme Court of the 60’s

**Criminal due process cases (searches,
confessions, probable cause)**

- **Safe Streets Act of 1968, Title III**
- **Federal Rules of Criminal Procedure**
- **Federal Rules of Evidence**

Watergate Fallout

- **Church/Pike**
- **SSCI/HPSCI**
- **FISA**
- **FOIA**
- **Privacy Act**
- **Executive Orders on Intelligence**

Key Similarities

- **Legislated involvement of all three branches of government (more or less) in “solutions”**

Compelling Conclusions

- **We (still) have a “system” based on events/threats/abuses of the 60’s and 70’s.**
 - **Amendments grafted/patched as required— e.g. spy cases of 80’s and 90’s.**
 - **Patriot Act**
- **We have always taken a balanced approach.**
 - **Can be seen in most every issue.**

Key Threshold Questions

- Has 9/11 “changed everything” or are we still assuming to work within existing system?
- With each specific issue, what is the “exclusivity” of the existing regime?
e.g. FISA

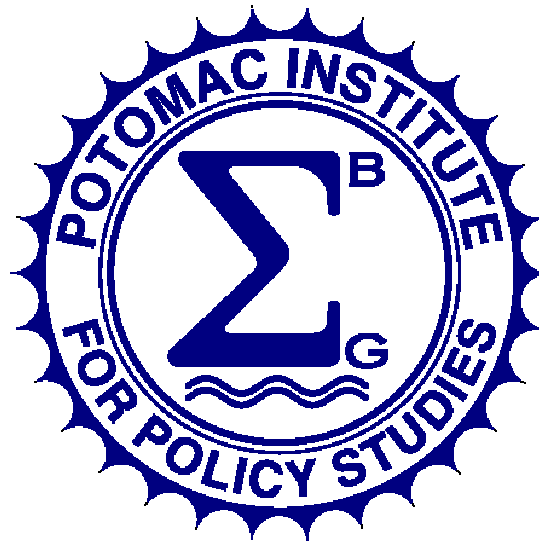
Assumptions for Analysis

- **That we will stay within the existing system and continue to graft changes.**
 - e.g. Patriot Act
- **However, we will not be constrained by the “exclusivity” of existing regimes.**
 - e.g. May be “new” regimes

IV. Proposals

A. Evaluation of New Information Technology

B. Terrorist Threat Information Categories



A. Evaluation of New Technology:

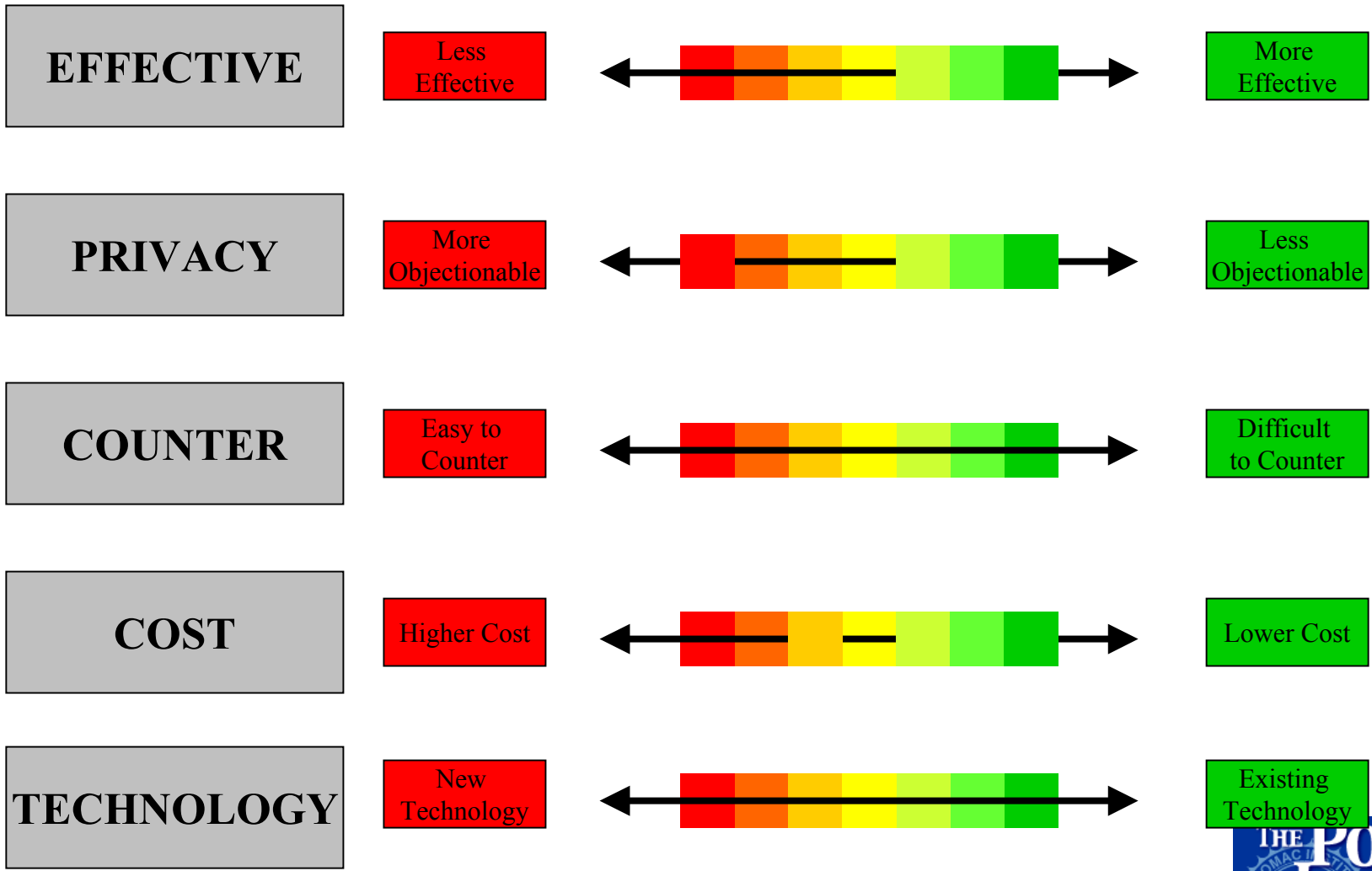
Key Issues

- **How to (objectively) evaluate “new” information technology in the post 9/11 environment?**

Objective Criteria for the Evaluation of New Technologies

- **Effective-** would have to measurably enhance security
- **Privacy-** could not be unreasonably intrusive
- **Counter-** Could not be easy to counter
- **Cost-** Would have to compete in budget process
- **Technology-** Can we do it now?

An “index” could look like this...



Other Key Issues

- **How much difference remains between non-U.S. persons and U.S. persons? Between activities inside/outside the U.S.?**
- **What thresholds of circumstances are assumed or required?**

Other Key Issues, Con't.

- **What uses of public information will be permitted/enabled and under what circumstances?**
- **What new exchanges of information inter/intra government will be permitted/enabled and under what circumstances?**

B. Oversight of Terrorist Threat Information

**Potomac Institute proposal of
June 2003**

Objective Criteria for New Information Technology Policy in the War on Terrorism

- **More and better “dots”**
- **Better “connection of dots”**
- **Better information sharing**
- **Better privacy**
- **Congressional oversight**
- **Public transparency/confidence**

“Terrorist Threat Information”

- **“*Terrorist Threat Information*”** is a new category of information defined by Statute and/or Executive Order. It *can* include *relevant*: foreign intelligence, foreign counter intelligence and law enforcement information (which could otherwise be lawfully obtained by or shared with federal law enforcement agencies or the Intelligence Community).

“Terrorist Threat Information”

Continued

- **“Terrorist Threat Information” *could also include* other specific categories of information (including public health, safety and environmental information) which the Federal Government otherwise had lawful access to, provided that the Director of Central Intelligence (DCI), the Secretary of the Department of Homeland Security (DHS), Attorney General (AG) and the Secretary of Defense (SECDEF) determined in advance that such categories of information were “relevant” to the “current terrorist threat”; such categories would be periodically reviewed, approved and reported to various Committees of Congress.**

Dissemination/Sharing

- **“Terrorist Threat Information” would be disseminated to certain approved federal, state and local agencies. [The DCI, the Secretary of DHS, AG and SECDEF would be required to initially approve the nature, extent and categories of dissemination and periodically report such determinations to various Committees of congress.]**
- **Necessary amendments to/waivers of the Freedom of Information Act (FOIA) and Privacy Act would be enacted/obtained.**

Threat Models

- **“Terrorist Threat Information”** would be also analyzed with technology that applied **“Current Threat Models”** to the data, such ***“Current Threat Models” to be established, periodically reviewed and approved*** by the DCI, Secretary of DHS, AG, and SECDEF; report of such determinations and reviews could be provided to select Committees of Congress.

U.S. Person Information

- **“U.S. Person” (as defined in current law) information obtained for and contained in the “Terrorist Threat Information” database would be, *at first intake and from whatever source*, protected by anonymous coding, which would indicate that the data is related to a U.S. person, but would not allow identification of the person, unless and until specifically approved by one of two procedures:**

U.S. Person Identity

- ***U.S. Person identity and information could be revealed and disseminated in the context of a Current Threat Model, provided such release was approved by a senior official; reports of such releases would be provided periodically to various Committees of Congress. Could be a judicial role (e.g. FISA court/magistrate)***
- ***In addition, U.S. Person identity and information relating to an “Urgent Terrorist Threat”, as defined, could also be revealed and disseminated on specific approval of the AG and the Secretary of DHS; reports of such releases would be given to the same Congressional leaders as identified in the “covert action” section of the National Security Act.***

FISA/ Reports to Congress

- **Approvals/court orders for specific U.S. Government collection of foreign intelligence/foreign counterintelligence concerning U.S. Persons would continue to be governed by existing authorities.**
- ***A comprehensive annual or semi-annual report of all activity* described above would be required in unclassified version for public release and a classified version to various Committees of Congress.**

V. Conclusions

- Laws, policies, and technologies have failed to protect us from the terrorist threat.
- At stake are values Americans hold dear:
 - Privacy
 - Security
- We must engage the technical community and policymakers to create technologies and an oversight structure that will increase security and protect privacy.
- We need to determine the appropriate role of government.

For More Information:

See our website at

<http://www.potomac institute.org/research/projectguardian.cfm>