CENTER FOR ADVANCED STUDIES IN SCIENCE & TECHNOLOGY POLICY
INFORMATION • TECHNOLOGY • NATIONAL SECURITY

Spring 2006
Volume VI, Issue 2

CAS Newsletter

FISA is Inadequate

In a recent essay, *Whispering Wires and Warrantless Wiretaps*, in the NYU Review of Law and Security (Spring 2006), Mr. Kim Taipale, executive director of the Center for Advanced Studies, explains why the Foreign Intelligence Surveillance Act (FISA) is no longer adequate to address certain foreign intelligence needs and recent technology developments, in particular, the transition from circuit-based to packet-based communications; the globalization of the communications infrastructure; and the development of automated monitoring techniques, including data mining and traffic analysis.

"One thing is clear in the current debate over whether the President has the inherent power to authorize the National Security Agency to monitor international communications with suspected terrorists – even the most strident opponents concede the need to identify and monitor the communications of terrorists and stop them before they can act," said Mr. Taipale at a Global Information Society Project forum in New York, "unfortunately, FISA currently makes it impossible to use advanced information technologies to help do just that. By all means let us debate who should have the authority to authorize and oversight such intelligence gathering programs, but let us not forget that *someone* must, and the existing mechanisms – including FISA – are inadequate."

Continued on page 2.

Policy Appliances

In *Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties,* a chapter in the recently published book Emergent Information Technologies and Enabling Policies for Counter Terrorism (Robert Popp and John Yen, *eds*., Wiley 2006), Mr. Taipale writes that there is no inherent *technical* design conflict at all between security and privacy in government information sharing systems as the technical features required to support privacy policy are in large part the same technologies required to meet operational information assurance and data security needs. Both national security and privacy policy require (i) that shared information be *useful* (that is, that data is accurate, reliable, and timely, and that it can be up-dated or corrected as needed), and (ii) that information be *used appropriately* according to policy rules. Technical features to support these concordant policy needs in information systems include rules-based processing, selective disclosure, data quality assurance, error correction, and strong authorization, logging, and audit functions.

This chapter discusses policy-enabling systems design based on an *enterprise architecture* for *knowledge management* that includes *policy appliances* (technical control mechanisms to enforce policy rules and ensure accountability in information systems), interacting with *smart data* and *intelligent agents*.

More at http://policy-appliances.info/

CENTER FOR ADVANCED STUDIES
IN SCI. & TECH. POLICY

CAS NEWSLETTER
VOLUME VI, ISSUE 2

K. A. TAIPALE
EXECUTIVE DIRECTOR

ALANA TATE
MEDIA CONTACT

•••

PHONE:
212-966-5801

FAX:
212-334-5064

E-MAIL:
INFO AT
ADVANCEDSTUDIES
DOT ORG

•••

COPYRIGHT © 2006

Calculus of Reasonableness

In a forthcoming book chapter, *Why Can't We All Get Along? How Technology, Security, and Privacy can Co-Exist in the Digital Age*, to be published in Cybercrime and Digital Law Enforcement, (Jack Balkin, *et al., eds.*, NYU Press, forthcoming 2006), Mr. Taipale examines how identification, data aggregation and analysis, and collection technologies intersect with privacy and security needs, and suggests certain strategies premised on separating *knowledge of behavior* from *knowledge of identity* to help protect individual autonomy while still meeting security needs. Mr. Taipale describes the need for applying a “calculus of reasonableness” to govern when the *privacy divide*—that point where attribution of behavior and identity occurs—can reasonably be breached consistent with existing notions of *due process*.

Mr. Taipale describes the four factors instrumental in determining due process: the reasonableness of the *predicate* for action, the *practicality* of alternatives, the *severity and consequences* of the intrusion, and the procedures for *error control*, and argues for a dynamic assessment within the particular context.

For more info, contact us.

FISA continued from page 1

Mr. Taipale's FISA essay has already received wide circulation in policy circles and has been reported in several news articles, including a recent article by Shane Harris in the National Journal (republished in GovExec.com) in which he writes: “Taipale's essay … has attracted some early response. One FBI official called the analysis of FISA's deficiencies ‘brilliant,’ and a former government official experienced in intelligence-gathering called Mr. Taipale's recommendations ‘right on the mark.’ ”

See http://whisperingwires.info/ and http://www.govexec.com/dailyfed/0406/041006nj2.htm .

About the Center for Advanced Studies

The Center is an independent, non-partisan research and advisory organization focused on information, technology, and national security policy and related issues.

The Center seeks to inform and influence national and international policy- and decision-makers in both the public and private sectors by providing sound, objective analysis, insight, and advice; in particular by identifying and articulating issues that lie at the intersection of technologically enabled change and existing practice in public policy, law, and industry

More at www.advancedstudies.org.

> “By all means let us debate who should have the authority to authorize and oversight such intelligence gathering programs, but let us not forget that *someone* must” — Kim Taipale