American Bar Association

National Security Law Report

Volume 27, Number 1 STANDING COMMITTEE ON LAW AND NATIONAL SECURITY February 2005

SPECIAL ISSUE: CONFERENCE REPORT

Counterterrorism Technology and Privacy

Report on the Cantigny Conference, sponsored by the McCormick Tribune Foundation

June 23–25, 2004

Overview

Stewart Baker, Committee Chair

Information technology is a tool with great promise in the fight against terror. At the same time, privacy is one of the freedoms that define what we are fighting for. Aggressive new uses of information technology raise questions about whether our privacy will be a casualty in the war on terror.

At first glance, the conflict between privacy and technology seems irreconcilable. If we must choose one or the other, the decision will be painful and divisive. Indeed, the last few years have seen numerous controversies (Total Information Awareness, CAPPS II, and more) based on the assumption that new uses of technology will inevitably mean new limits on privacy. In fact, that assumption is open to doubt.

On June 23–25, 2004, the McCormick Tribune Foundation sponsored a conference on counterterrorism technology and privacy. The conference, organized by the American Bar Association Standing Committee on Law and National Security, was part of the Cantigny Conference Series, which gathers groups of experts to advance debate and thought on critical issues facing the country. The objective of the conference was to identify the issues—and perhaps some common ground—on the use of counterterrorism technology. The conference attendees represented a cross-section of the debate. Some were officials from intelligence gathering or law enforcement agencies. Others came from civil liberties organizations and backgrounds. Participants included government officials; former Members of Congress; federal law enforcement and intelligence specialists; members of the legal, business, and academic communities; and the media.

The issues were debated with passion, and, in the end, resulted in a remarkable amount of agreement, even though the purpose of the meeting was not to produce a formal accord on the topic. Speaking off the record and in an atmosphere of candor and good will, a rough consensus was in fact reached on the principles that should apply as government seeks to bring information technology to bear on one of the most deadly challenges of the twenty-first century.

Following up on this surprising convergence, some of the participants produced a set of principles meant to capture the essence of the discussion. (*SEE THESE PRINCIPLES ON PAGE 14.*) Without suggesting that every participant agrees with every one of the principles, we are pleased to be able to offer the principles as a way for men and women of good will to find common ground on this difficult yet vital issue. This publication presents not just the Cantigny Principles, but also a summary of the proceedings that led to them.

This report presents views and versions of events as expressed at the time by conference participants. Remarks at the conference were not-for-attribution. The presence of descriptions of events and perspectives in this report do not mean that all conference participants embrace a given version of events or a given opinion. One sentence in this report may summarize views that were advanced by multiple participants. Because this report consists entirely of points, issues, and descriptions of events raised by participants at the conference, attribution phrases such as “it was discussed that...” are omitted where possible.

Conference Report

Introduction

Several years ago, the FBI alerted the Department of Defense (DOD) Office of Counterintelligence that a person working in one of the Department's laboratories had been identified as a spy. The Defense Intelligence Agency had previously known that a foreign intelligence source was trying to infiltrate certain classes of DOD activities, including the activity where the spy was located, but the information was not pursued. This case highlighted the reactive nature of DOD counterintelligence and led to a reappraisal of DOD practices in this area. The intelligence community, by contrast, took a more proactive approach and made use of various analytical methods to try to anticipate security to persons under particular suspicion include requiring the government to demonstrate probable cause before it can obtain warrants for searches and wiretaps. Requiring the government to demonstrate probable cause before gathering information on individuals suspected of membership in terrorist groups operating in the general population might be inappropriate. Rights to privacy in personal information is an area of less agreement. At least with respect to the government's use of such information, the expectation of privacy is high, but the government can access such information through searches/seizures authorized by the Fourth Amendment. Outside the criminal context, the issue of government access to a citizen's personal information is considered a threat to privacy, because of the possibility that the information could be used to embarrass or blackmail citizens. *Reasonable access to personal information* is governed by the Fourth Amendment-based standard of reasonableness, which balances the government's interest in access to information against the citizen's privacy interest in the same information. The concept of reasonableness bears directly on the government's right to obtain and review information about citizens collected by the private sector and maintained in commercial data banks.

Defining and Protecting the Right of Privacy

The public policy goal is to create a regime that allows the new technological tools required to fight the War on Terror and still meets the public's expectations of privacy. The concept of privacy involves elements of secrecy and confidentiality, along with concepts of control and fairness.

Some advocate new rules to control government access and use of personal information. The elements of new rules might be found in the Privacy Act of 1974, which establishes concepts of privacy based on Fair Information Principles that remain relevant. The Principles include: notice to an individual before personal information can be collected; the collection of only so much information as required for the task at hand; use of the information only for the purpose for which it was collected; insistence on data quality, accuracy, completeness and timeliness; access for citizens to their own information and an opportunity to correct errors; redress for citizens who suffer adverse consequences as a result of the use of their data; and security and enforcement mechanisms commensurate with the sensitivity of information that is in the system. Since 1974, this language has also been incorporated into other privacy statutes, like the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.*, and it can be argued that the private sector is subject to more stringent regulation to protect privacy than the government.

New rules could require that no data can be collected on an individual until that individual has been notified that information is being collected; that all such data be of good quality; that the data be relevant to the task at hand; and that the data be subject to audit / security protections to prevent unauthorized access / distribution.

When Congress passed The E-Government Act of 2002 (H.R. 2458), it enhanced personal privacy by requiring, in Section 208, that federal agencies should publish Privacy Impact Assessments before deploying new information technology programs for the collection of personally identifiable data. Section 222 of the Homeland Security Act (H.R. 5005) contains new privacy protections including the establishment of a "privacy officer" in a cabinet level department. Congress directed the privacy officer to promote best practices with respect to privacy and to ensure that the use of technology by government enhances privacy protections for personally identifiable data. The existing

THE ABA NATIONAL SECURITY LAW REPORT
<http://www.abanet.org/natsecurity/>

EDITORIAL BOARD
Suzanne E. Spaulding
Stewart Baker
Richard E. Friedman
Elizabeth Rindskopf Parker
Pamela Parizek
Holly Stewart McMahon
Matthew Foley, *Editor*

The *National Security Law Report* (*N.S.L.R.*) contains articles concerning the law relating to the security of our Nation and associated topics. The *N.S.L.R.* is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee, the ABA, or any governmental agency or private enterprise.

To receive the *N.S.L.R.*, contact Holly Stewart McMahon at 740 15th St., NW, Washington, DC 20005-1009; (202) 662-1035; FAX (202) 662-1032; or hmcmahon@staff.abanet.org.

structure for protecting privacy, especially as modified by recently passed legislation, is regarded by some as a sound basis for ensuring that personally identifiable information collected by the government is protected.

Participants diverged as to whether the "mere viewing" of personal records violates a person's right of privacy in those records, when there is no consequence from the inspection and when the person may not have been aware that the inspection took place. Some felt that, because the act of collecting and retaining personal information in an electronic database creates the "opportunity for abuse" that unauthorized inspection would constitute a violation of a person's rights. On this view, the collection and maintenance of personal information creates a "general sense of chill" that may alter a person's behavior.

Focusing on the potential for abuse, a participant noted that the government, while collecting information on potential terrorists, collected information on Muslim immigrants simply because they were Muslim. The challenge to civil liberties comes from the risk that government will use the data against people who may be included in that group but who, while not terrorists, may be vulnerable to prosecution for other reasons. Some argued that a system for collecting and analyzing data must be designed so that data about groups can be collected in searching for terrorists, but that the government cannot use that data against members of the group who are not terrorists.

Some offered the view that citizens are aware that personal information is collected about them every day and their expectation of privacy must be balanced against the society's need to protect itself. "It is rational to have some additional level of scrutiny of people from terror-sponsoring countries," one participant said. The voluntary surrender of personal information in return for the convenience of using a credit card is a balancing judgment that affects the person's expectation of privacy in that information.

Some called for a clear definition of privacy rights in order to balance the consequences of taking action to solve a societal problem, such as terrorism, against the possible encroachment on concepts of privacy and individual liberties. Working across jurisdictional lines complicates this problem. The failure to provide a working definition could undermine the effort to establish rules and procedures that will allow the balancing to proceed.

Ensuring that Information Gathered for One Purpose is Only Used for That Purpose

Participants expressed concerns about the temptation to use information collected for one purpose for another purpose, but it was generally agreed that effective safeguards, with public notice and invitation for comment when an expansion of the use of personal information was contemplated, would allow the problem to be successfully managed.

In a recent Department of Justice counterterrorism initiative, people from some predominantly Muslim countries were asked to come in and register; when they did, some were arrested for unrelated violations. A "hold harmless" rule where a person who cooperates in a terrorism investigation would be held harmless from other consequences of being investigated might be necessary. It was generally agreed that such a rule would be likely to increase the effectiveness of such an investigation by encouraging participation.

Effective Use of Data Mining

Concerns were also expressed that an irrational fear of computer technology, as evidenced by the conflict that engulfed the Total Information Awareness (TIA) program, threatens to diminish information gathering in the War on Terror.

The recent Technology and Privacy Committee (TAPAC) Report, intended to give the Secretary of Defense guidance on the use of data mining in the War on Terror recommended that before using computers to analyze intelligence data that may contain personal information on a US person, the Department should obtain the approval of the FISA Court; and that defense analysts be required to get Head of Agency approval before using Google or other web surfing tools.

Some argued that data mining is no more than the automation of human data analysis. On this view, data mining simply changes the medium of observation from the street to a database, but does not change the purpose of the investigation—looking for suspicious patterns of behavior. Pattern identification has always been part of preventive policing and it keeps law enforcement from being purely reactive. Computers can be programmed to perform searches in ways that preserve the anonymity of those being investigated more effectively than humans. Some critics of data mining were themselves criticized as focusing exclusively on worst-case scenarios, undermining public confidence. Instead, it was suggested that acceptable privacy controls on data analysis systems should be devised so that all of the nation's technical capabilities can be focused on defeating terrorists.

Two principles that might guide the development of counterterrorism and crime technology are: (1) that the government should be allowed to use all available technologies to combat terrorism; and (2) that the burden of proof to justify the use of technology to analyze personal data should be no higher than human access to such data.

In response, some noted that citizens are skeptical of the government when it comes to their privacy and that, after the demise of TIA, are still suspicious about the government's intention to further intervene in their lives to combat terrorism. It was generally agreed that the government must do a better job of explaining its intentions so it will be able to secure the authority to use innovative technologies and do so in a way

Continued on next page

that honors the Constitution and protects civil liberties.

Other participants raised concerns about data mining, in particular because of the risks to citizens and residents from the Middle East. The issue was framed in terms of how law enforcement searches for patterns of suspicious activity and follows those patterns to create lists of suspicious people. If the objective of using data mining is to produce lists of suspicious people, how can that be accomplished without simply coming up with lists of Muslims? In response, one participant with a background in technology suggested that any pattern search that produced "nothing more than a list of Muslims" was flawed from the outset. The issue in such cases is what the technician programming the computer tells the computer to do. There is an important difference between a computer that is searching a large database and a computer that is searching that database under the control of a narrowly crafted set of instructions.

One participant maintained that people will always be at risk of doing the wrong thing but, with proper training and systems to oversee and, when necessary, punish misbehavior, they can also do it right. If we cannot get beyond the risk that people may do the wrong thing (and therefore violate someone's privacy) we risk handicapping the whole effort to use technology to find terrorists before they strike.

If in the early stages of the investigation the terms of a search were devised so there was no identification of individuals, pattern searches using data mining could be conducted while protecting individual privacy. The government is not using such techniques to track individuals traveling between the U.S. and Middle Eastern countries, for example, because it does not have access to flight data. Such information is only available from the airlines with their cooperation. Federal law enforcement does not regularly receive information on individuals from either U.S. Customs or the Immigration and Naturalization Service.

Data mining would reverse law enforcement's usual course, beginning with general questions and working back to individuals rather than starting with a known individual and linking him with others. Law enforcement agencies are more concerned about automating data they already have. The goal is greater efficiency in using data already collected, not collecting more data because it may be needed in the future.

Data mining was described as a method of identifying behavioral characteristics of people who are identified as terrorists. As more such characteristics are collected, patterns emerge which can be applied to larger pools of data to identify others as targets for further investigation. At the first level, it was argued, such searches have no consequence because no actions are taken, except to establish that some individuals should be the focus of more penetrating examination at the next level. Overrepresentation of some groups among those identified for further investigation would be "correlation as a matter of effect, not as a matter of intent."

It was generally agreed that the shift of operational method makes people uncomfortable. Instead of focusing, as the criminal justice system usually does, on punishing conduct that has already occurred, the goal is prevention.

Preventing the Government from Abusing Personal Information

Participants called for a new set of rules to instruct government employees about how new technologies can be used. The focus on whether to take action reactively (after events) or preemptively (before events) misses the point, some said, because intelligence cannot know ahead of events what will be actionable. It was argued that, if the government is not permitted to use the new tools, the private sector will respond to the opportunity to gather and analyze information and government agencies will end up buying information that the agency is not allowed to collect on its own.

The concept of privacy can confuse secrecy with anonymity. Privacy may not have disappeared, but the ability to live in secrecy largely has, so it is time to create new rules of privacy that will dictate to government agencies the consequences of improper use of personal information.

There was general agreement that, while we must be alert for abuses, it would be a mistake to let the fear of abuse prevent the government from taking action. There was further agreement that the risk of abuse must be balanced against good results. Work was suspended on TIA before it was understood what the system was capable of doing. As a system, TIA may have proved to be inadequate and would have led to the elimination of TIA. However, it was agreed that the emphasis should remain on balance - and it was generally agreed that a workable balance between privacy and the uses of technology was possible and necessary.

Since 9/11, the government has assumed significant new powers over personal information that affect privacy, but the use of those powers has been largely hidden from public view. One participant said that the government declined to make any information available about some detainees taken into custody after 9/11. That characterization was disputed, however, and it was argued that because there must be some secrecy in the War on Terror, which is quite different from a criminal prosecution, "complete transparency" in everything the government does should not be expected. The USA PATRIOT Act (H.R. 3162) requires the government to report to the House of Representatives on its activities.

Law Enforcement vs. Intelligence / Preemption

The Need for Collaboration

September 11, 2001, caused a total reevaluation of the relationship between the law enforcement and intelligence communities. The reevaluation is continuing, but it is now clear that the old distinctions between international threats

to national security and domestic threats from terrorists have lost much of their meaning.

Closer collaboration between the two communities is the goal, but conferees were reminded that the two communities have very different methods of operation. Intelligence tends to collect information from numerous sources, often of varying quality, and bases its recommendations on that imperfect information. Law enforcement tends to insist on real proof and hard evidence and usually excludes information that fails to meet that standard. The difference in methods arises from the fact that law enforcement must ultimately subject its results to the criminal justice system, while the intelligence community does not.

Interaction between Law Enforcement and Intelligence

Many now recommend that the Central Intelligence Agency (CIA) assist in the collection of intelligence on U.S. persons. The National Security Act of 1947 (50 U.S.C. 404) provides CIA's fundamental legal authority. The Act authorized CIA to gather intelligence, but specifically prohibited the agency from exercising any domestic police, subpoena, law enforcement or internal security functions. The Act is silent on the issue of CIA collecting, retaining, or otherwise handling information about U.S. persons. Executive Order 12333, issued by President Reagan in 1981, grants those authorities to the agency, but only under procedures approved by the Attorney General. CIA operates under procedures established by the Attorney General 22 years ago. It was suggested that those procedures have handicapped the agency's ability to accommodate today's emerging technological capabilities.

The USA PATRIOT Act significantly altered the intelligence landscape. CIA has provided intelligence about domestic criminal activity to the law enforcement community for years, but the USA PATRIOT Act requires the law enforcement community to provide CIA with foreign intelligence that is discovered during the conduct of domestic criminal investigations. Intelligence now flows both ways and CIA can now collect intelligence on U.S. persons, as long as it complies with the Attorney General's rules. In this changing environment, CIA now labors to take advantage of the latest technologies to accomplish its objectives while conforming to restrictions placed in its governing rules years ago.

While law enforcement is traditionally viewed as looking backward to reconstruct crimes that have already occurred, intelligence gathering is regularly done by law enforcement as part of its investigative work. There are real distinctions, however, in the way the communities are motivated. Law enforcement is judged by whether investigations lead to the successful arrest and prosecution of criminals. Because that process usually leads to a trial, officers are motivated to follow the rules; otherwise, the prosecution is likely to fail. Intelligence investigations are conducted with the expectation that the actions of investigators will remain secret. This does not mean intelligence investigations ignore the privacy interests of their targets, but it does mean that a target's privacy rights are likely to receive more attention in a criminal investigation. It was argued that, because of these distinctions, the objectives of the intelligence and law enforcement communities should not be combined, but that the exchange of information authorized by the USA PATRIOT Act should continue and expand.

Some believe that a new entity, similar to the UK's security intelligence agency (MI5), might now be necessary to lead domestic counterterrorism investigations, rather than the Federal Bureau of Investigation (FBI). It was noted that the FBI has a history of refusing to share information developed in its investigations with other agencies. In the past, this refusal was based on the restriction against sharing Title III information outside of law enforcement; or on the restriction against sharing grand jury material. The USA PATRIOT Act removed these barriers, but this has not yet resulted in the full sharing of information. There was general agreement that the creation of a limited purpose agency, like an MI5, risked establishing new walls of separation between law enforcement agencies. Instead, more favorable attitudes within existing agencies to sharing of information would allow for more effective use of new technologies that would make the entire system more effective, while protecting civil liberties.

Legal Status of the "U.S. Person" Distinction

Participants expressed a number of views as to whether the U.S. person distinction might now be seen as obsolete, at least in the context of data analysis. There was general agreement that there are no rules that now require a differentiation between U.S. persons and non-U.S. persons with respect to data analysis. The difficulty in dealing with commercial databases is that such collections contain personal information on U.S. and non-U.S. persons, but the national status of those persons is not a data attribute. Therefore, the rights those persons are entitled to under U.S. law differ according to their status. A participant raised the additional issue of data sharing with non-U.S. agencies and the difficulties that arose from different rights accorded to persons under differing legal systems, which might require new international rules allowing for the review of data without tying the data to a particular person until a later stage of the investigation.

Inadvertent Collection of Information

Sharing of too much information between agencies could undermine search limitations and lead to the violation of privacy rights. While the issue of how to handle incriminating information that is gathered inadvertently is a policy question, the decision could be used to make the extension of search authorities more acceptable to the public. It was argued that agencies should not be forced to ignore evidence of significant criminality that is inadvertently discovered and that the best way to prevent abuse was to limit the use of

Continued on next page

evidence collected on a search to the prosecution connected with the original purpose of the search.

Selective Prosecution

Participants had varying views on selective enforcement. For one participant, the pursuit of particular individuals or groups was simply a decision about where to concentrate limited prosecutorial resources. Such decisions could always be justified, as long as defendants were being prosecuted for real crimes. Others were less convinced, arguing that as long as the focus was on particular groups, such as Muslims, the decision to prosecute those individuals or that group was inherently suspect. As an example of selective prosecution, a participant offered the federal "absconder program" which is intended to find and deport aliens whose papers have expired, but who have remained in the country. With an estimated 300,000 absconders in country, the majority of whom are thought to be Hispanic, the enforcement agency placed a priority on Arab and Islamic absconders. It was argued that this was an instance where ethnicity was unlawfully used by the government to focus an investigation.

Liability for Funding of Terrorist Activities

New rules might be necessary to protect U.S. financial institutions from the liability associated with the handling of funds that appear to be owned by legitimate organizations but which turn out to be funds used to underwrite terrorist activities. Banks that sufficiently investigate suspected individuals and "charities" would not be found liable. Government agencies might not be likely to share information about these "charities" with private sector financial institutions, but government agencies are already purchasing such information from private sector data aggregators. Private sector financial institutions might spend more than $10 billion on customer compliance issues over the next 10 years. The financial industry recently formed the Regulatory Data Corporation to sell "know your customer" services intended to help the industry avoid the criminal and civil liability they are now exposed to in several statutes.

Surveillance Technologies

Introduction: Technology Threatens Privacy Rights

Panelists debated the premise that there was no difference between data pattern analysis performed by computers and by humans. The power of the computer allows for the analysis of so much data that its use alone makes our privacy less secure.

A recent Supreme Court opinion, *Kyllo v. United States,* 533 U.S. 27 (2001), dealt with the relationship of technology and privacy. The issue in *Kyllo* was whether the Fourth Amendment required a warrant for law enforcement to use an infrared camera to take pictures of the exterior of a house in an effort to determine if marijuana was being grown in the garage using special lamps. The Court held that a warrant was required and relied on separate rationales in reaching its decision. One rationale was based on traditional privacy and sanctity of the home principles. The other rationale, which could have ramifications for the future use of technology, held that a warrant was required because technology was being used to obtain information about an individual's personal activities that could not have been obtained without the use of that technology. The Court could define *privacy* as the ability to be insulated from technical intrusion. Such a line of reasoning could say to law enforcement that it is free to analyze any information, as long as it is not gathered using prohibited technology.

Total Information Awareness (TIA)—Can Surveillance Guarantee Privacy?

The Total Information Awareness (TIA) program was meant to develop technologies to address emerging national security problems and the decision-making issues associated with them while protecting privacy. But the TIA program encountered significant public relations problems and was terminated. Nonetheless, it was argued that, even in failure, TIA has provoked essential discussion about the nature of the problem we face – how to effectively use our technology to find terrorists who may be planning attacks in the United States.

Finding terrorist cells requires that law enforcement have the ability to pick up the signals the cell inevitably uses; to isolate the signal; and to terminate the cell. It is presumed that al-Qaeda cells are operating in the United States now. Those cells are the target and the challenge for a system developed to penetrate such cells is to model that target and determine how it reacts to its environment. A cell's reactions to its environment are crucial. If reactions can be picked up and identified, investigators will have located their signal. To do this, investigators must be able to conduct pattern-based searches.

Pattern-based searches focus on databases containing information that conforms to certain patterns of behavior. The identification of these databases was one of the first tasks undertaken by TIA. At the same time, an effort was initiated to develop "privacy appliances" that would filter the results of the searches and place the resulting information in government-owned repositories. The role of the "privacy appliance" was to confirm the identity and authority of the person requesting the search; to determine if the request was proper; and, presuming it was, to execute the search. Then the appliance would anonymize the data and deliver it to the party that made the request. As a case is built, more details would be revealed until, at the end, individuals would be identified. Finally, the appliance would create an audit trail. The development of the appliance was interrupted by the demise of TIA, but interest in the concept was stimulated and work continues in the classified budget of the Defense Department.

Whether such an appliance can be built remains unknown, but it was strongly urged that the research should continue. It was argued that any such appliance should have the

following characteristics: the ability to conduct pattern-based and subject-based searches; the ability to establish and authenticate the authority of the person making the request; and, most importantly, the language must be machine-understandable, so that the system can be automated. Because large volumes of data must be reviewed rapidly to thwart attacks, it was argued that the system will not work unless it is automated.

Other Technologies—More Threats to Privacy

Data mining is just one of many information-gathering technologies developed in recent years. The flow of information has been increased by the introduction of: (1) inexpensive and easily dispersible sensors that can be placed almost anywhere and have the ability to locate by detection; (2) new storage devices that have dramatically reduced data storage costs; (3) broadband and wireless communications with the ability to transmit large volumes of information at high speed and with high reliability; (4) dramatic increases in computational processing power; (5) the development of advanced algorithms which allowed for the development of data mining; (6) Global Positioning System technologies in cell phones, vehicles and PDAs: and (7) the Internet, which makes all this data accessible at any time from any place.

Given the growth of these technologies and their inherent impact on privacy, the following ground rules were offered for consideration by those making technology choice decisions: (1) objectives and applications—the technology is set to capture and identify signals at certain thresholds to distinguish them from the large amounts of background noise, while balancing false positives (which can net the innocent) against false negatives (which allow terrorists to escape the net). These thresholds are matters of choice so that, if maintaining privacy were paramount, the threshold would be set at a higher level than it would be if the goal were to find terrorists. For each level the threshold is raised and privacy is more protected, the likelihood of finding terrorists is lowered; (2) legal regimes—there are several, each with its own set of standards; (3) the quality of the target—depending on whether the target is cooperative or uncooperative, different surveillance technologies may be called for; (4) the sources of required information—is the information coming from public records or private databanks? Are warrants required? (5) accessing the data—will the effort to access the data be covert or transparent? Must the targets of the surveillance be notified? (6) Will the surveillance be asymmetric, i.e. the government watching you? Or bilateral, where both the government and the target have access to the data stream?

When the amount of data gathered to identify terrorists is very large, the challenge is to identify patterns of activity suggesting that the people connected with those activities are planning a terrorist attack without being sidetracked by false positives or negatives. Dealing with the issue of false signals is crucial to gain public support and it was argued that methods are available to combat the problem.

Some took the view that data mining was only one of many surveillance technologies currently in use, given the availability of vehicle identification and tracking, including GPS tags, OnStar systems and red light cameras; cell phones and security cameras; and remote sensing. Some information is generated online, meaning it will not be erased and is accessible to anyone who can get into the system. Each of these systems can contribute to the War on Terror and each one affects privacy in its own way. The world is changing and the challenges to protecting privacy are significant.

It was argued that the evolution of technology is causing dramatic change in the intelligence community. Intelligence has emerged from its traditional role supporting the other national security functions, diplomacy and military operations, into a coequal instrument of power. New forms

Continued on next page

of intelligence are emerging that must be effectively merged with existing practices, with effects on intelligence sources and methods. In the current environment, there is much discussion about the need to share information. Because of the need to accommodate new recipients, the sharing of information might require adjustments in the ways intelligence is gathered to protect sources. With the vastly increased information flows, many more hypotheses must be analyzed every day. The shortage of analysts means this challenge is not now being met and it was suggested that we risk another intelligence failure if this problem is not addressed.

Another challenge for the intelligence community is to find a way to convey information about these complex issues to decision makers who may not have the background or training to understand this complex information. Many of the same technologies and much of the same data are available to our adversaries and, because they have different, perhaps less precise standards, maintaining an advantage in information and technology will require greater effort.

Will Anonymizing Data Protect Privacy?

Participants posed a number of questions about whether the collection of data in anonymized form constitutes an invasion of privacy. It was agreed that, even if parties to such scrutinized communications were anonymous to begin with, it did not mean that investigators would not be able to identify them later. A participant returned to the issue of whether a person doing something in a public place has an expectation of privacy in that action. It was generally agreed that different levels of expectations attach to different levels of activity and that perceptions of privacy will continue to evolve.

Another participant objected to the characterization of any data as anonymized because that process can be easily reversed. On this view, the only way to protect the anonymity/privacy of those who are involved with scrutinized communications is to adopt procedures that carry punitive sanctions for their violation that are painful enough to persuade the agency that it would be better to follow procedures.

Participants noted that there is no expectation of privacy in the address information, such as the addressee or subject line of an e-mail. There is an expectation of privacy in the content of such communications; however, there is no such expectation in the fact that the communication took place.

It was noted that one of the functions of the USA PATRIOT Act was to eliminate anomalies and correct the way different kinds of communication were treated under the law. As soon as that was accomplished, however, another set of anomalies emerged. The evolution of technology moves faster than the law, and it was generally agreed that anomalies are a problem to be managed, not solved.

Pattern Based Searches and the Problem of False Positives

Critics have suggested that the problem of false positives is so severe that pattern based research is a waste of resources. One participant responded that some research in this area was promising, but cautioned that, thus far, all the research had been based on simulated data. Simulated data avoids privacy problems for researchers, but can also be misleading. The participant described the process of designing a "pattern template" identifying several actions a terrorist cell would take if it were planning an attack. Terrorist cells are small and they do things in certain ways, i.e., they exhibit patterns. These patterns can be discovered through the application of pattern analysis. The techniques of pattern analysis have been in use for years and that their effectiveness has been enhanced by the application of technology to what would otherwise be intimidating volumes of material. Pattern searches can also be thwarted by the cells, whose leaders are intelligent and experienced. They can be expected to vary their patterns to mislead investigators, so the effective use of pattern searches will invariably be painstaking and difficult.

Data Mining Technologies—Retention and Dissemination

Policy Implications of Data Mining

Law enforcement agencies were criticized after 9/11 for collecting information on how terrorists financed their activities without integrating that information and tracking the terrorists more effectively. Methods used by terrorists to move money, pay for their activities, and transfer money from one cell to another can be tracked and that data mining technologies will be part of that effort. The primary technical challenge is to identify the terrorists' signals and separate them from the background noise. Before solving that problem, decisions must be made about the technologies to be used, the targets, the agencies that will conduct the investigations, and the rules under which the investigations will be conducted. Some of those decisions are technical, but others are policy decisions.

The TAPAC Report

During the controversy over TIA, the Technology and Privacy Advisory Committee (TAPAC) was appointed by the Secretary of Defense to examine the legal issues related to TIA and the current state of American thinking about privacy values. The Committee spent considerable time on the question of how technologies like data mining, with all of their implications for privacy rights, related to American values. The Committee quickly discovered that government agencies were already using data mining, but, because no one was tracking those activities, it could not determine how often. The Committee also discovered that the laws governing the use of these programs were outdated and inconsistent with one another. It was noted, for example, that the Homeland

Security Act, passed in November 2002, required the Department of Homeland Security to engage in computerized data mining. Two months later, Congress specifically prohibited the Defense Department from doing the same thing.

The TAPAC Committee's Report presented to the Secretary of Defense in May, 2004, contained the following conclusions: (1) that data mining was critical to success in the War on Terror and that the only issues should be the types of data mining permitted and the rules under which the data mining should be conducted; (2) that in directing the Defense Department to cease all research on data mining, Congress had taken a step that should be reversed, because further research was immediately required on data mining, other related technologies and the policies that would guide such programs; (3) that policy level privacy officers should be placed in cabinet level departments, with the ability to access external advisors who would help to develop rational privacy policies; and (4) that audits should be conducted on a regular basis to assure compliance with departmental policies on privacy.

The Committee also recommended that agencies and personnel engaged in data mining be covered by a framework of rules requiring legal and technical training for the personnel and oversight responsibilities for the agency. Under the proposed framework, an agency would be required to secure written authorization from the head of the agency before engaging in any form of data mining; to comply with technical procedures regarding the security and audit trail of data; to comply with specified data minimization and data anonymization procedures; to comply with special procedures called for when seeking to move data to another area for which the data was not originally obtained, i.e. a different investigation; and, where appropriate, to seek the authorization of the FISA Court before taking any action requiring such authorization.

The Committee suggested the framework should apply to all government departments and agencies because so much data mining was already being done by federal agencies. The Committee called for a coordinated federal government privacy policy, to include privacy training for federal employees having responsibility for decisions with privacy implications; clearer and more sensible rules on the uses of data mining; expanded oversight of such activities by senior agency officials and external advisors; more explicit accountability within federal agencies undertaking data mining activities; and clarification of the role of Congressional oversight including the rationalization of the Congressional committee structure to accommodate this responsibility.

The MATRIX Program

Privacy groups have cited the Multi-State Anti-Terrorism Information Exchange (MATRIX) Program, designed to use technology and data mining in support of law enforcement, as an example of how not to run a government data mining program. According to program documents, MATRIX was designed with the capacity to search as many as 20 billion "public / private" record files as part of the effort to find terrorists. While MATRIX officials had declined to identify what was included under the category "public / private" records, MATRIX documents made clear that records searched would include "telephone calling records, cell usage and location data and financial transaction data." The program used data mining techniques to search personal records in order to find individuals with a "high terrorist factor." The same documents claimed to have identified 120,000 such individuals, which led to "scores of arrests."

The 120,000 figure seemed far-fetched, but it could not be determined from the MATRIX documents whether that number was supposed to represent suspects in Florida only, or in the entire country. Critics stressed that MATRIX was not authorized by the Congress, or by any of the states in which it did or still operates and that, while there are guidelines in the contract between MATRIX and the states specifying how the states can use the data, there are no restrictions in the contract about how the MATRIX program itself can use the data. The program lacks specificity regarding which state officials were authorized to contract for the use of MATRIX, had no system that allowed for the examination of government data bases and for separating information that identified individuals from the rest of the information that was subject to data mining analysis; and had no means of protecting individual anonymity. Nor does the program provide mechanisms for correcting false positive identifications or inaccurate information. Of the 16 states that originally joined MATRIX, 11 have withdrawn.

Is Greater Use of Data Mining Inevitable?

Arguments similar to those used against data mining now, regarding the potential for abuse, were used in the 1960s to thwart the development of technology to eavesdrop on telephone conversations. Then, the subject was privacy in our conversations and now, it is privacy in our personal information. It was asserted that now, as then, the key to the effective use of the technology is the prevention of abuse. The use of data mining is already common in some federal agencies (the Centers for Disease Control routinely uses it to look for patterns indicating the outbreak of disease). Continued technological developments, including enhanced databases and less expensive storage, are certain to encourage the trend. The technology is also commonly used in the private sector and it was suggested that, if the government refuses to use data mining technology, the private sector and government agencies will be forced to buy information from private sector data miners, who would use different standards with respect to privacy. It was also noted that, because the technology is internet-based, people outside the United States should be expected to continue development of the technology. The Chinese, for example, are working

Continued on next page

hard to develop data mining skills to locate dissidents in China. As a policy issue, it was suggested that the only choice for government agencies is whether they should get in now, or get in later. If the government waits until later, it will be required to use the system, but will have lost the opportunity to structure the framework. It was noted that partisan politics has always been a tool for limiting abuse by government and that, even though the structure for oversight has its flaws, it is largely in place.

Use of Data Mining (and MATRIX) in Law Enforcement Cases

Participants discussed circumstances in which it might be appropriate to use data mining technology in conventional (i.e. non-terrorist) cases. Using the example of a case involving serial child abductions, a case was made for using data mining to analyze more quickly the evidence available in public record databases to move the investigation toward a successful conclusion more rapidly. It was generally agreed that the use of data mining as described in the hypothetical would be appropriate and it was noted that the operators of the MATRIX program similarly describe their methods of operation. However, it was alleged that MATRIX routinely searches many more records, public and private, some of which should require a warrant.

Other participants objected to the claim that MATRIX was engaged in data mining. Rather, it was argued that MATRIX is really using "link analysis" after a crime, not pattern analysis. *Link analysis* builds on available evidence by searching public records to make connections that tie suspects to a crime. Participants also expressed a number of views about whether the MATRIX research had stopped after the list of 120,000 names was developed. It was argued that the list was reduced to 1,200 names, which was then used by the FBI for further investigation. It was argued that no one was arrested simply because their name was on the list of 1,200 and that, because the technique developed numerous leads for further investigation, the use of the technology in this case worked as it is supposed to.

Are Existing Privacy Protections Sufficient?

Given the capability of these new technologies to analyze data, a participant asked whether the TAPAC Committee had specifically considered how else the government might use these new capabilities. It was noted that the government's ability to access effectively more and more data would raise levels of discomfort and apprehension for many people, and it was suggested that these capabilities have so dramatically changed the landscape that a different type of privacy risk must be addressed. It was argued that the new technologies have created a need to completely revisit and upgrade privacy laws and that those developing the technologies should integrate privacy policy from the early stages of development.

Legislative Answers

It was generally agreed that legislation should address general principles, such as whether and in what circumstances government agencies would be allowed access to personal information. It was argued that technology-specific legislation is a mistake, simply because technology changes so fast that it will bypass and invalidate the effect of even the most far-sighted legislation.

The challenge of engaging Congress was also addressed. It was suggested that the recommendations of the 9/11 Commission and the re-authorization of the Patriot Act ensure that intelligence and privacy issues will be prominent in 2005. It was generally agreed that the best way to accomplish the necessary education was by working with Members of Congress individually or in small groups. There was general agreement that outreach of some kind would be worthwhile and necessary.

Technology as a Tool to Protect Civil Liberties

Limits on Technology: A Historical Perspective

The Privacy Act of 1974 was passed in response to revelations about the collection of data on the political activities of American citizens by the military intelligence services, the excesses of Watergate, and the growing perception that the computer posed special threats to liberty. In passing the Act, Congress sought to promote respect for the personal privacy of citizens in the collection, computerization and use of personal data; to prevent the creation of secret data banks containing information about citizens; to prevent illegal and overly broad investigation and surveillance of citizens; and to promote accountability, legislative oversight and open government in the use of computers.

To accomplish those objectives, Congress directed that information about how a citizen exercises their First Amendment rights should not be collected or maintained without a strict review process; any information collected about citizens should be accurate, timely and relevant; interagency exchanges of personal data should be limited; data should be held securely and records kept of all disclosures and uses of personal data; agency personnel and contractors should be trained in accordance with Privacy Act requirements; and no new data banks or personal information systems should be created without the express authorization of the Congress. The Act has been modified, but its fundamental objectives remain unchanged.

The intrusion of the military into civilian affairs has been infrequent in U.S. history with, perhaps, the worst example occurring in the 1960s. During those years, the army collected personal data on about 100,000 citizens in an effort to surveil anti-Vietnam War demonstrations and protestors. Military agencies have been specifically precluded from domestic security activities since then, but recent changes in

technology have afforded military intelligence the opportunity to return to those areas. Neither Executive Order 12333 nor the Privacy Act specifically prohibits the military from collecting information online. The military can also collect and share personal information about citizens through its work with the Department of Homeland Security and the Terrorist Threat Integration Center. Some participants expressed concern about military intelligence playing any role in homeland security, beyond the support of military operations.

A Successful Strategy for Using Technology Based Surveillance

Technology based surveillance systems do exist and are successfully managed. The large volume of information flowing through these systems requires the capability to sort, filter and distribute the data. At the same time, the data must also be certified and evaluated, at least at the preliminary level. These are significant challenges for both the technology and the managers of the system.

Technical characteristics of a successful information management and surveillance system that should be written in before the system is built include:

1. Automation—everything that can be reliably done automatically should be done automatically. That includes audit trails, which can now be done automatically with a high degree of reliability.

2. Audits—to the extent possible, auditing functions should be made part of the operations function. This would allow audits to be conducted regularly, without disrupting operations. There will be exceptions to this, but exceptions requiring human intervention should be documented in a way that clearly establishes lines of accountability.

3. Access—access to databases should be restricted to those who must have it in order to perform their analytical tasks. All rights of access should be frequently and automatically reviewed.

The human characteristics required for the successful information management and surveillance system include:

1. Compliance with rules—a culture of compliance is essential to successful operation of a surveillance system. Acknowledgement of the importance of compliance must begin at the top and be fostered throughout the organization. The compliance function should be forced down through the levels of management, so that responsibility for compliance is dispersed to all levels of the organization. Compliance must become an aspect of daily operations and not be reserved to the oversight function.

2. Training—every function in the system is regulated and, to ensure compliance with regulatory procedures, training must be an integral part of operations. Such training should be rigorous, continuous and mandatory for all employees.

3. Oversight—an essential function that should be separate from other operational functions. Oversight must be consistent and thorough, always with the understanding that too much oversight can create undue caution and unacceptably slow decision-making.

Architecture—A Place to Connect Policy and Technology

The starting point for analyzing the impact of technology on civil liberties is to recognize that technology is a tool and it does not provide total security or privacy. Technology is a tool that is part of a technical system, which is itself a value-driven construction. The policy that establishes the technical system also establishes the values that will be used to manage that system. Technology is neutral and, because its use is value-driven, the correct values, including privacy and respect for civil liberties, should be incorporated into the policy that guides the system at the onset.

TIA was offered as an example of the wrong way to develop policy and technology. It was argued that the termination of TIA was a serious setback for security and only a pyrrhic victory for civil liberties. TIA was made up of seven programs and, when it was terminated, six of those programs were "classified" and the seventh, the privacy protection program, was abandoned. This decision had two results, neither of which advanced the cause of protecting civil liberties. The first was that a public, visible program was ended, along with an important opportunity to debate about the subject. However, the technology development that was at the core of TIA was not terminated. It was moved into classified programs, beyond the reach of public scrutiny. The second result was that the technology research being done under TIA was transferred from the Defense Advanced Research Projects Agency (DARPA), where the customers (i.e. government agencies) were in charge, to vendor companies trying to sell the same government agencies their product.

TIA challenged the notion that privacy is protected by the government's inability to analyze available data. In the new environment, data is always available and the analysis and storage of data becomes less expensive every day. In the new economics of information technology, it is less expensive to retain data than it is to reduce and manage its volume through selective editing. Data management is now driven by the ability to search large databases and there is less emphasis on editing as a strategy to retain only the data that supports a given function. The availability of all this data means that the privacy of any individual is vulnerable, so the question of selective attention by government agencies to an individual is more significant. The goal is a system that incorporates a distributed architecture based on web services that supports both privacy and the government's need to share information among its agencies.

Continued on next page

Privacy and Policy—Together from the Beginning

Participants expressed numerous views on the issue of when to integrate privacy principles into the development of technical systems. One participant argued that it was critical to include privacy considerations, along with security needs and compliance issues as fundamental system requirements, into the design of the system from the beginning. It was said that layering a privacy policy onto an already developed technical system was certain to leave gaps in privacy protection that were preventable. Another participant noted that government agencies were now in the market for technical systems and that systems offered by vendors had little or no privacy protections built in. In these cases, the privacy policy will have to be added onto the technology after purchase, resulting in predictable gaps in privacy protection.

The question of whether existing policymaking structures were equipped to manage the development of privacy policy was raised. It was generally agreed that the Judiciary was not a good choice (and would not want the responsibility in any case); the Executive was not sufficiently trusted by people that were opposed to the use of the technology; and that Congress was not particularly competent for the task and would be, in the best of circumstances, cumbersome to deal with. There was also agreement that, in the absence of a generally accepted method for making policy, government agencies would proceed on their own, most likely through the rule-making process, and that the results should be expected to be irregular and haphazard. It was also suggested that the policymaking process would be further complicated by security classification rules, which would prevent the transparent sharing of information, creating another reason for public skepticism.

Another participant suggested that the problem was more difficult since there was no centralized project, like TIA, around which a national debate could take place. For this participant, government agencies and departments would try to find a way to resolve the privacy-technology debate for themselves, but the larger issue of developing a framework to address these questions across all government agencies and departments would be an unreachable goal for the time being.

Errors and Exceptions

After acknowledging that technology guided by good policy could help protect civil liberties, a participant inquired how, if such a system were fully automated, the victims of misidentification and faulty inference would have an effective way of redressing grievances. It was argued that a centralized process for redress, supervised by people with appropriate training, should be a part of such a system and it was generally agreed that any acceptable system would have to provide a process for the correction of such errors quickly and effectively. The question of when it would be appropriate to allow for exceptions was then raised. It was suggested that rules are rational and only apply to situations anticipated by them, but that exceptions are different because they arise from new and unanticipated circumstances. The critical question then becomes who makes the decision granting an exception and what standards will be used. It was argued that, because impartiality is essential, the Judiciary is the best place for this power to reside. Other participants acknowledged the need but suggested that, because such decisions would be frequent and would need to be made quickly, the Judiciary was not the best place. It was suggested that a new type of judiciary, with real time access and secure networks, could be an answer to the need for rapid response. It was also suggested that an Office of Inspector General in an agency like the Department of Homeland Security could satisfy that need.

How Much Transparency is Enough?

The demise of TIA demonstrated that transparency of process is critical to winning public trust and support for these programs. Concerns were expressed about how much transparency was needed. It was suggested that it may be necessary to conceal some of the databases searched/processes being used, at least in terrorism investigations, and it was questioned whether this would be tolerated by the public. It was also noted that, if too much information is revealed, people can counter-program their data, or otherwise change their behavior to avoid detection. It was argued that announcing what databases would be investigated, or deciding that some databases would be off limits in advance would undermine the successful use of the technology. To be effective, it was argued that pattern analysis must be able to scan large databases in search of unanticipated data anomalies, the location of which cannot be predicted. It was suggested that the government should not be dedicated to protecting personal secrecy, but should focus on protecting anonymity for First Amendment rights and personal autonomy through the exercise of due process rights. Others suggested that the public thinks more categorically and would want assurances that certain types of information, e.g. medical or library records, are simply off limits.

Conclusion

Next Steps: Forging a Consensus

The importance of reaching out to Congress was acknowledged and it was noted that, because Congress responds to its constituents, broadening the discussion to reach a larger, non-technical audience could stimulate public reaction and help move Congress to action. The difficulty of resolving the question of the meaning of privacy in America was also acknowledged and it was suggested that, if notions of privacy are as dynamic as they seem to be currently, then systems built to protect privacy must be flexible and adaptable to these changing notions. It was argued that the voluntary surrender of privacy in return for convenience was a case in point and, as such exchanges become more pervasive, the underlying concepts of privacy also evolve. It was noted that there may also be issues for

people who choose not to make such exchanges because they may be treated differently—and unfairly—if they choose not to surrender their privacy. Finally, it was observed that Americans are more comfortable sharing personal information with the private sector than with the government and, within the government, are more comfortable with some agencies than with others.

Starting Over: Context and Perspective

It was suggested that a new way of thinking about these issues is needed to better match the constantly changing realities. People dealing with these issues have spent their careers learning to specialize, narrowing their focus to concentrate on an area of specialty. Specialists tend to rely on certain basic assumptions that have served them in the past, even though the changing world calls for regular reassessment of those assumptions. As a starting point, a management approach called scenario building was proposed for consideration. Scenario building is a method of analyzing complex problems in order to reach decisions about priorities and resource allocation. Elements of scenario building include: (1) identifying the decisions to be made; (2) challenging underlying assumptions to ensure their validity; (3) identifying key factors in the decision environment affecting the decision; (4) setting priorities by ranking the factors according to the importance of their uncertainties; (5) selecting the appropriate logical or analytical tool for the scenario being analyzed; (6) identifying probable implications; (7) recognizing that beliefs, hopes and fears influence behavior as much as numbers and facts; (8) assessing the probability of each scenario to allow decision makers to allocate limited resources more effectively; and (9) identifying and selecting leading indicators to decide which, if any, of the scenarios is actually occurring. Finally, it was suggested that policy must, at all times, encourage the continuing development of technology. In the current environment and for the foreseeable future, it was argued that the best chance to deter terrorist attack is through the aggressive use of technology. It was emphasized that technology is neutral and that it is only in its application that ethical dilemmas regarding the abuse of technology arises. It was argued that success in managing these technologies will only come through the development of a clear process and the discipline to follow it.

Basis for Citizen Resistance

To make progress on the enhanced use of technology issue, it was argued that law enforcement must be prepared to sacrifice its claim to use information collected and analyzed in terrorism investigations against citizens who are not terrorists, but who may have broken other laws. Unless law enforcement is willing to make this concession, it was argued that resistance to the employment of advanced technologies should be expected to continue. It was also argued that the resistance of citizens to the enhanced use of technology by government agencies was the result of repeated overreaching by the law enforcement community. It was suggested that skepticism about government motives come from many sources, but that overreaching was a common thread. The USA PATRIOT Act was cited because it was passed as an antiterrorism measure, but contained several provisions that expanded law enforcement powers in the domestic area. Similarly, the CAPS II program was sold as a way to look for foreign terrorists, but its authority soon expanded to include persons who had committed ordinary domestic crimes. The participant argued that sacrifice was necessary to be successful in the War on Terror, but that constitutional principles, including the principles of particular suspicion and probable cause, must remain paramount.

Strategies for Going Forward–Issues and Ideas

It was suggested that any strategy for going forward must focus on both the need for effective communications and the substance of what is to be communicated. Substantively, it was argued that public support would be available for a program containing the following elements: (1) clear legal limits on the uses of data mining and related technologies; (2) clear and understandable oversight mechanisms; (3) an open process allowing for the participation of interest groups; and (4) mechanisms for the redress of grievances by those who may have been adversely affected by the application of the technology.

It was also suggested that the following elements would be critical to an effective communications strategy: (1) positive explanations of technological proposals to the public and the press; and (2) restraint in public statements, i.e. using care in communications and restraining the urge to over promise.

Another participant agreed with the notion of educating the press. It was observed that journalists routinely reach large audiences and that, while favorable coverage is good, unfavorable coverage can be fatal to a program. It was also suggested that members of the press should be educated about the subject matter and be cultivated, because it may be necessary to contact them to respond to inaccurate stories or supplement coverage. It was particularly noted that care should be taken in presenting information to the press to ensure more accurate and effective coverage. Finally, it was suggested that maintaining credibility with the press is crucial because, without credibility, no useful relationship can continue.

Success will require more than better public relations skills. When it comes to data mining and other technologies, there is real resistance among citizens to the principle of government having the power to conduct such operations, and it may be better to advocate an incremental advance beyond what is being done now.

The Cantigny Principles on Technology, Terrorism, and Privacy

Introduction

Technology permits governments and businesses to collect, store, analyze, and disseminate very large amounts of routine and sensitive information about daily human transactions. This information is stored worldwide in open-source and limited-access databases controlled by governmental and commercial entities. Access to relevant information is critical for government and corporate decision-making; however, simple access in a world of terabyte storage is often not enough. Automated tools can be used to effectively extract correlative and predictive analyses from multiple databases that will provide government officials and corporate executives with information products to make important business, risk management, and security decisions. Governments and businesses are already using automated search and predictive tools for purposes that range from intelligence analysis and law enforcement to customer behavior and market analysis.

A government has no greater imperative responsibility than to use all available and lawful tools to protect its citizens from the illegal enterprises of terrorists. Powerful automated data mining applications that analyze a broad range of multiple, diverse databases may prove to be effective tools to fight terrorism and crime. Indeed, these analytical tools may help to "connect the dots" before another catastrophic act of terrorism occurs.

Yet, the use of powerful new technologies also poses certain concerns. Access to such a broad array of existing databases and a powerful capability to aggregate and analyze information on a specific person or groups of people, however, raises serious privacy issues. For example, existing laws do not regulate the government's use of commercial data for counterterrorism purposes. When the ability to aggregate data is weak, members of the public consider themselves anonymous in their daily activities, reflecting a "practical obscurity." As we deploy new technologies that eliminate that obscurity we must come to grips with the implications for Americans' sense of privacy and the lack of statutory guidance in this area, and establish strict guidelines to ensure that those who face adverse consequences as a result of those technologies have adequate redress mechanisms.

Information is our first line of defense, and determining the U.S. government's access to and its lawful yet effective use of information is the single most important core element of reorganizing our Nation's defense infrastructure and counterterrorism efforts after September 11, 2001. The purpose of the Statement of Principles is to provide guidelines to govern the government's use of information that will balance the responsibilities of our democracy in protecting the privacy and safety of all U.S. citizens and resident aliens. These principles are intended to steer reorganization efforts and government policies to permit robust access and use of all available information for national security and law enforcement purposes while forcibly safeguarding an individual's interest in privacy. They are a distillation of the vigorous debate that occurred during the McCormick Tribune Foundation's Cantigny Conference on Counterterrorism Technology and Privacy, but they do not necessarily represent the agreed views of every participant.

Statement of Principles

Core Principles

1. Government should infringe on privacy *only* as an imperative to protect the safety of U.S. citizens and resident aliens.

2. The legislative and executive branches share the fundamental Constitutional responsibility to protect the privacy and safety of all U.S. citizens and resident aliens – and should act in partnership.

3. The legislative branch should provide the statutory authority for the government to have appropriate, lawful access to and use of information stored in government and commercial databases for national security and law enforcement purposes. This authority should also protect privacy, differentiate between national security and law enforcement uses, and establish a streamlined, robust Congressional oversight mechanism to support its Constitutional responsibilities.

4. The executive branch should have clear and robust statutory authority to access and use all relevant information stored in government and commercial databases in support of its Constitutional responsibilities and subject to its Constitutional limitations, and to routinely share that information as needed between law enforcement, intelligence, and national defense agencies.

5. Both law and technology can and should be integrated to provide complementary protections for the privacy and safety of all U.S. citizens and resident aliens.

Continued on next page

6. The government should maintain an open dialogue with domestic and international private sectors concerning access to and use of commercial databases.

7. The government should keep the public well informed about how personal information is being collected and used for national security and law enforcement purposes and what safeguards are in place to protect their privacy.

The Collection and Storage of Information—A Distributed Network of Databases

8. Information collected and stored in government and commercial databases should be as reliable and accurate as practicable.

9. Regulatory guidelines should be established to ensure information stored in government and commercial databases remains as current, accurate, and useful as practicable.

10. Regulatory guidelines should be established to provide for an adjudication process in the event any adverse consequences result from the use of information stored or used by the government. This regulatory process should not preclude eventual judicial review.

11. Best business practices should be established by regulatory guidelines to ensure the information maintained in government databases are adequately secure from theft or unauthorized access.

12. Best business practices should also be established for data retained or used by the government to ensure the continued availability of relevant information and to ensure that information that has lost its value over time is not used.

13. Personal information on U.S. citizens should be separately identified whenever possible and provided additional security and privacy protections.

14. Information stored in government databases and the use of new technologies should remain subject to the Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

15. Information stored in government and commercial databases that is relevant and useful for national security and law enforcement purposes should remain decentralized but be organized by a centralized directory within a distributed network with layered access levels so as to avoid consolidation into massive databases solely for the purposes of national security and law enforcement searches.

The Analysis and Dissemination of Information—Limited and Controlled Access

16. National security and law enforcement agencies have a diverse range of needs to access and analyze various types of databases, and should have ready access to databases depending upon their respective missions and specific requirements, but they should only be granted access to information directly relevant to their agency's mission.

17. To facilitate and control access, an infrastructure should be established by law and regulation that permits a cadre of specially cleared personnel throughout the federal, state, and local government levels who are specifically authorized in the performance of their duties to use automated search and predictive tools on this distributed network of government and commercial databases for limited national security and law enforcement purposes.

18. The government should provide appropriate monetary compensation and preserve the confidentiality of commercial databases when it obtains access to such databases.

19. This infrastructure should not be a separate department or organization, but a cadre of personnel within federal, state, and local government offices who have been granted access and requisite permissions to the centralized directory and distributed network of databases who will be authorized to use automated search and predictive tools only on the databases within this distributed network that are relevant for the mission of their organization, and who shall be subject to audits, rules, and limits to this access.

20. A cadre of representatives within federal, state, and local government offices are in the best position to identify the relevance, utility, and reliability of the databases they desire to search from the range of databases within the network to which their office has been granted access.

21. This cadre of representatives should be able to choose what databases within this distributed network of databases are relevant to their search by having access to the centralized directories.

22. To the greatest extent possible, the centralized directory as well as automated search and predictive tools should be utilized in such a way to provide anonymity unless and until a particularized basis for piercing the veil of anonymity is demonstrated.

Continued on next page

23. The highest standards of security, logging, accountability, and other best business practices should be applied to controlling access to and monitoring the use of this distributed network of databases to ensure all reasonably available policies and technologies are used to safeguard the privacy of individuals and security of the network.

24. Appropriate standards of business continuity and disaster recovery procedures and capabilities should also be applied to this distributed network of databases.

25. This infrastructure should have an Inspector General responsible for the oversight of the privacy and security of the centralized directory and distributed network of databases and who should conduct periodic security and privacy inspections and audits.

26. This infrastructure should also have an ombudsman whose responsibility is to assist in the development of privacy safeguards.

27. All access and searches on this distributed network of databases should be electronically recorded in a permanent file that the cadre of specially cleared personnel does not have access to and which discloses tampering if impermissible access is attempted.

28. The executive branch should implement regulations ensuring that appropriate officials throughout the local, state, and federal governments who are responsible for national security and law enforcement have appropriate and timely access to information and the analyses that result from automated searches of that information.

29. Once information has been lawfully collected and stored in a government or public database, no additional judicial authorization should be required for this cadre of specially cleared personnel to analyze or use automated search and predictive tools on that information for legitimate national security and law enforcement purposes.

30. Once information has been lawfully collected and stored in a commercial, non-public database, the cadre of specially cleared personnel should provide notice of access to the commercial data-holder prior to analyzing or using automated search and predictive tools on that information for legitimate national security and law enforcement purposes.

31. This cadre of specially cleared personnel, and all other persons within the legislative and executive branches of government as well as state and local officials, with access to the centralized directory and this distributed network as well as the analyses that result from automated searches of that information should receive periodic briefings and training on privacy issues and be subject to criminal prosecution and civil liability for the unauthorized release or use of that information.

Research and Development—Supporting Privacy, Security and Mission Functionality

32. The executive branch should develop and retain a robust research and development capability that aggressively focuses on emerging technologies to ensure the protection of privacy, security of information and access, and capabilities in support of legitimate national security and law enforcement purposes.

33. Research and development initiatives should have the freedom to explore all conceivable technologies and tools, and no adverse consequences for individuals should result from their authorized research and development activities.

34. Research and development initiatives should be conducted in parallel with applicable implementing policy including addressing privacy protections at each step of the development process. These policies should be vetted through a policy and technical review committee that should include experts from the following disciplines: technology, security, privacy, and public affairs as well as representatives from the legislative branch and the private sector.

35. The legislative branch should be regularly kept informed of ongoing research and development initiatives and the corresponding policies under consideration.

36. The legislative and executive branches should institutionalize relationships and work hand-in-hand with the private sector, think tanks, universities, research labs, non-governmental and intergovernmental organizations, foreign countries, and other entities both domestically and internationally in establishing research and development initiatives.