A Possible Approach to Analyzing Anti-Terrorism Proposals

by Assembly Judiciary Committee Counsel
California State Legislature
January 2002

Introduction

As the Assembly Judiciary Committee began to consider the types of legislative proposals that may be introduced in response to the attacks of September 11th, the Committee concluded that it would be prudent to develop a standard framework to assist it in analyzing anti-terrorism measures that might come before it. Such a "template" could help to ensure the Committee's efforts to address the issue in a consistent manner without unduly impinging on cherished rights and freedoms of Californians. The possible "template," along with two case examples demonstrating its application in practice, follows.

Analytical Template for the Judiciary Committee To Use In Analyzing Proposals to Address Terrorism

- ✓ **What is the proposal and what problem does it seek to address?**

- ✓ **Does the proposal appear to comply with the U.S. and California Constitutions?**

  U.S. Constitutional concerns: First Amendment freedom of speech and press; Fourth Amendment search and seizure issues; Fifth and Sixth amendment process issues; Fourteenth Amendment due process and equal protection, privacy rights.

  California Constitutional concerns: Express right to privacy, as to both government and private action. Protects "autonomy privacy" (right to make intimate decisions and conduct personal activities without observation or interference) and "informational privacy" (interest in precluding dissemination or misuse of sensitive and confidential information).

- ✓ **To what extent might the proposal be pre-empted by federal law?** (Examples: airline security, immigration control and border security.)

- ✓ **Even if it's not likely pre-empted, will the proposal likely cause confusion or other problems by overlapping with federal law in the area, suggesting state deference to federal law in this area?** (Examples: criminal penalties for terrorist acts and federal laws regarding law enforcement powers to investigate such acts.)

- ✓ **Is there existing California law that accomplishes, or could accomplish, the goals of the proposed legislation?** (Note current criminal laws on terrorist acts, powers of law enforcement to investigate and prosecute, along with existing state and local emergency powers.)

- ✓ **Have there been earlier attempts to legislate in this area, and how did they fare? What have other states done in this area?**

- ✓ **Is there any evidence the proposal will in fact address the identified problem?**

- ✓ **Will enactment of the proposal result in unintended consequences? Are there potential abuses that might arise if the proposal is enacted? Potential discriminatory application? Unnecessary invasions of privacy? Do the benefits outweigh any potential harms?**

- ✓ **Are there ways to protect against any potential abuses? Might it be appropriate to include a sunset provision? Does the proposal call for a study component?**

Development of the possible template for analyzing proposals to address terrorism

Constitutional Issues

As with any legislative proposal, analysis of anti-terrorism measures typically begins with an examination of the proposal and the problem it seeks to address. The next immediate task often is an analysis of relevant Constitutional issues to determine whether the proposal is consistent with the rights guaranteed under the U.S. and California Constitutions. Some examples of Constitutional concerns have already arisen with regard to some recent federal anti-terrorism actions. One such example is the federal Department of Justice's regulatory move to monitor communications between certain federal prison inmates and their attorneys, challenged as a violation of the Sixth Amendment right to counsel.[1] Concerns that may arise with some anti-terrorism proposals under the U.S. Constitution include First Amendment issues of freedom of speech and freedom of the press, Fourth Amendment search and seizure issues, Fifth and Sixth Amendment issues relating to the rights of persons accused of crimes, and Fourteenth Amendment due process and equal protection concerns. These issues also arise under parallel provisions of the California Constitution.

In addition, anti-terrorism proposals which affect personal privacy may wish to be considered in light of the California Constitution's express guarantee of the right of privacy.[2] In this light, it is helpful to recall that the California Constitutional right to privacy has been held to apply to both government and private action, and to protect so-called "autonomy privacy" (the right to make intimate decisions and conduct personal activities without observation or interference) and "informational privacy" (the interest in precluding dissemination or misuse of sensitive and confidential information).[3]

Existing Law

The next step of analysis that may wish to be pursued is a consideration of existing laws and governmental powers that may already address similar issues of public safety and the prevention of terrorism. The federal government of course plays a preeminent role in this area. Thus, for example, in the areas of immigration control and border security, it is federal rather than state law which governs, and it is possible any action California might wish to take in this area may be held to be pre-empted. In other areas where there is overlapping state and federal jurisdiction, federal law may be found not to pre-empt state action, but deference to federal law may be advisable to avoid confusion or other problems. The newly enacted USA PATRIOT Act appears to serve as a good example on this point. The PATRIOT Act expands the powers of federal law enforcement officials to use various means of investigation such as wiretap and Internet surveillance in certain cases. While California might not be held pre-empted from similarly expanding state law enforcement powers, in some areas, expansion might lead to possible confusion over whether a case should be handled by federal or state authorities, so policymakers may wish to consider whether it makes sense to legislate in that particular area.

Analysis of any proposed law generally also considers the presence of existing law on the same subject to determine whether action appears necessary. Thus the proposed analytical template being considered for use by the Committee asks whether existing California law is sufficient to accomplish the goals of the proposed legislation. For example, in the area of criminal penalties for terrorist acts, California updated its laws before the September 11th attacks, with passage in 1999 of AB 140 (Hertzberg), which provided enhanced criminal penalties for the use of weapons of mass destruction and biological weapons. In other areas as well, it may be concluded that existing law is sufficient to achieve the goals sought.

The last several questions of the possible template under consideration are simply those which are generally considered as part of analyzing most bills. Such analysis generally reviews past legislative attempts to address the suggested problem, and looks for evidence that the proposed solution will help address it. This analysis looks at possible ill effects or abuses under the proposed legislation, whether there may be ways to avoid unintended consequences, and if not, whether the hoped for benefits of the bill may outweigh potential downsides.

In order to demonstrate the application, and possible benefits of this particular analytical tool, the remainder of this report consists of two "case study" examples. The possible analytical template is used to analyze the issues of 1) mandatory identification cards and 2) the use of facial recognition technology.

Case Study #1: Mandatory Identification Cards

One proposal widely discussed following the events of September 11th has been the creation of a national identification card system. Most notably, Larry Ellison, the CEO of Oracle Corporation and Scott McNealy, the CEO of Sun Microsystems, have suggested the possible benefits that a system of digital identification cards may provide, including that it could tap into a national database of information. Ellison and McNealy suggest that such a system would make it relatively easy to detect persons travelling under false identities and to discover if a person who seeks to board a plane is on any kind of law enforcement watch list.[4] In addition, airline officials have also proposed a voluntary travel card that would use biometric technologies to verify passenger identity, allowing passengers with such a card to get through pre-flight screening more quickly.[5] And, administrators of state DMVs have proposed linking drivers' licenses to a national database.[6]

On November 16, 2001, the House Committee on Government Reform's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations held a hearing on the issue of national identification cards. While the idea of a national identification card met with generally tepid support, at that time, several lawmakers expressed interest in the idea of using state driver's licenses to tie in to a national identification system,[7] so this issue may be considered in the California Legislature this year.

Creation of a national identification card system, or utilization of existing means of identification to tie into a national database, would appear to call upon the state to make numerous decisions regarding the implementation of such a system. If, for example, Congress were to decide to

require states to tie driver's licenses into a national database, the state may be required to take action to implement such a system. There might be new federal requirements as to the format of the license (for example, requiring the use of biometric identifying information) or for the management of the DMV database of license information. Indeed, in California two bills have already been introduced this session to address the problem of fraudulently issued drivers' licenses by requiring fingerprints taken for a drivers' license application to be cross-referenced against a database. As to any national system, California policymakers may need to make decisions as to how the identification might be used at the state level: Could the state require citizens to carry such a card at all times? Could such ID be required to gain access to public buildings, or to get public benefits? What follows is a sample analysis, using the analytical template under consideration by the Committee, showing some of the issues that might arise and how they might be analyzed with ID card-type proposals.

Application of the Anti-Terrorism Template to Mandatory Identification Cards

What is the proposal and what problem does it seek to address? As noted above, several different national identification proposals are already being considered by national and state policymakers. These proposals seek to aid in the prevention and investigation of terrorism by facilitating the screening of travelers to determine if an individual poses a threat and by stopping the use of fraudulent identification. According to news reports, several of the hijackers on September 11th were on law enforcement watch lists. Many used false identification in their efforts to elude law enforcement.

Does the proposal appear to comply with the U.S. and California Constitutions? The constitutionality of a national identification system may turn on the particular uses to which it was put. Use of such an ID for airline screening, for example, could be found to stand up to challenge. Other uses might not. The U.S. Supreme Court has held that the U.S. Constitution permits a police officer to stop a person briefly for limited questioning upon reasonable suspicion of criminal activity, based on articulable facts.[8] However, a previous version of California's vagrancy statute, which made it a misdemeanor for a person thus stopped to refuse to identify himself, was found by the U.S. Supreme Court to be unconstitutionally vague, as it left it to the discretion of law enforcement as to what means of identification would be accepted.[9]

Importantly, however, the Court, in its decision, did not reach the question of whether the requirement of identification in itself (if the statute were adequately specific as to the type of identification required) would violate the Constitution. Justice Brennan, in concurrence, argued that it would, stating: "Merely to facilitate the general law enforcement objectives of investigating and preventing unspecified crimes, states may not authorize the arrest and criminal prosecution of an individual for failing to produce identification or further information on demand by a police officer."[10] Thus the issue of whether it is permissible for state law to require all persons to carry, and show upon demand, a particular form of identification, remains undecided, but may soon face state policymakers and the state's highest court.

Other potential uses for an identification card may also call into play other issues under the U.S. Constitution, such as the right to travel, or, if used discriminatorily, equal protection concerns.

California Constitutional issues also appear implicated as well by proposals for the use of more rigorous identification systems. The right to privacy under the California Constitution protects the interest in precluding dissemination or misuse of sensitive or confidential information.[11] Closely related questions were addressed by the California Supreme Court in Perkey v. DMV, although the holding in that case relied on statutory rather than Constitutional grounds.[12] In Perkey, the Court held that collection of fingerprints as a condition for issuing a driver's license was permissible, but found that under the state's Information Practices Act of 1977, the DMV could not allow third party access to these fingerprints, and was required to protect against misuse or improper disclosure of the prints. Under Perkey, state participation in a national identification system would thus at a minimum appear to require careful handling of the information collected.

To what extent might such a proposal be found pre-empted by federal law? If the federal government should choose to act to create a national identification system, states might be required to follow federal guidelines with regard to state action for implementation of such a system. Thus, if the federal government were to put into place its own requirements for state drivers licenses as part of a scheme to use licenses as part of a national system, state law on the matter may be found to be pre-empted to the extent necessary to allow compliance with the federal mandate.

Even if it's not found to be pre-empted, will the proposal inadvertently cause potential confusion or other problems by overlapping with federal law in the area, suggesting state deference to federal law in this area? Federal action to create a national ID card system might not be found to pre-empt action by the state to create a state ID card system. Such a system might be able to co-exist with the federal system (thus potentially requiring California residents to carry two IDs). However, creation of a state ID system in addition to a federal system might be considered a misuse and duplication of resources, and a potential source of confusion for individuals and law enforcement.

There is also a further question as to whether what is essentially a national policy decision as to ID cards should, as a matter of policy, be made at the federal government level. On the other hand, the states arguably could cooperate, independent of the federal government, to coordinate existing state identification systems and tie them to a national database system, as has been proposed by DMV administrators. Some DMV administrators have apparently suggested this is a natural extension of the de facto role of drivers' licenses today. But at least one law professor has argued that any such effort "should be discouraged in favor of a more deliberative decision of Congress."[13]

Is there existing California law that accomplishes, or could accomplish, the goals of the proposed legislation? Creation of a national system of identification is, of course, beyond the jurisdiction of the state of California. However there already are examples of existing state identification approaches. As noted above, the most commonly used form of state identification is the driver's license, or DMV issued identification card, and these are apparently already used for many of the purposes foreseen for a national ID card, such as identification of passengers

boarding an airplane. Under existing law, submission of a fingerprint or thumbprint is required in an application for a driver's license or ID card. However, these prints apparently are not cross-referenced to a database. Thus, a driver's license apparently cannot be used, as is proposed for ID cards, to check for any type of background information on a person, other than his or her driving record. Moreover, the existing system is subject to fraud that reportedly allows many to obtain false identification. Efforts to improve DMV's existing system could well meet some of the goals for a national system making it harder to obtain false identification and facilitating background checks.

Have there been earlier attempts to legislate in this area, and how did they fare? Is there any evidence the proposal will in fact address the identified problem? Two bills, AB 1474 (Koretz) and SB 661 (Dunn), are pending in the California Legislature that would require the DMV to create a searchable database of biometric identifying information submitted by those applying for drivers' license. Such a database conceivably could be coordinated with a national effort in this area.

Some proponents of a national ID card system have suggested that use of a national identification card, tied to a database with information from various agencies, may have allowed the September 11th hijackers to be identified and potentially kept from boarding the planes. A national ID system arguably could facilitate the investigation of terrorist acts and other crimes. Proponents also state that by including biometric information on ID cards, terrorists and other criminals could be unable to use fraudulent identification to evade detection and capture.

Opponents, however, point out that authenticating the identity of individuals may tell one little about trustworthiness – reportedly, most of the hijackers were not on FBI watch lists. They further argue that the effectiveness of an ID card system in rooting out potential terrorists would depend on the databases linked to the ID card system. Some have also argued that it is unclear whether it is practically feasible to create a system that could provide a significant level of screening. In this vein, Ben Schneiderman, Professor of Computer Science at the University of Maryland, testified before the Congressional Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee as follows:

> We must ask whether there is now a secure data base that consists of 300 million individual records that can be accessed in real time? The government agencies which come close are the Internal Revenue Service and the Social Security Administration, neither or which are capable of maintaining a network that is widely accessible and responsive to voluminous queries on a 24 hour by 7 days a week basis.

Thus the question of feasibility of administration appears to remain an open, and important, one in this policy area.

Will enactment of the proposal result in unintended consequences? Are there potential abuses that might arise if the proposal is enacted? Potential discriminatory application? Unnecessary invasions of privacy? Do the benefits outweigh any potential harms? Opponents argue that creating an integrated identification system could result in numerous unintended consequences.

They point out that with any ID system, there is the potential for falsification of documents or forgery. ID card theft they say could also become an issue. The greater scope of an integrated national ID system would potentially increase the amount of harm that could be caused by such fraud, making it possible, they contend, for miscreants to carry out identity theft on a larger scale with less risk of detection. Proponents, in response, suggest however, that use of biometric identifiers or other safeguards could in fact reduce fraud in this area.

The ACLU, citing the history of identity verification requirements under the Immigration Reform and Control Act of 1986, argues that an ID card system would lead to wide scale discrimination against "foreign looking" citizens – Arab-Americans, Latinos, Asians, African-Americans and other minorities, who would, they suggest, become subject to more and more identity checks.[14]

Perhaps most worrisome to opponents of such measures is the potential threat to privacy inherent in creation of a comprehensive database. They assert the government can't be trusted to maintain the integrity of that database, and keep the information from being released. Moreover, use of the ID cards could, they contend, lead to the ability to track further information, making it possible, for example, to monitor or record an individual's travels.

Against these risks stands the potentially exciting opportunity for a safer society. However proponents suggest, for example, that an ID system could not only allow the potential apprehension of terrorists and prevention of terrorist acts, but could also make ID theft and other fraud more difficult, by creating a system linked to biometric information. Moreover, they state any such system would give law enforcement a powerful and needed new tool to use in the investigation of all types of crime. Although weighing the risks against the potential benefits for public safety can only be done on a case by case basis as to specific proposals as to how an identification system would work and the purposes for which it would be used. But there appears to be little doubt that if the country, and California, could enact an effective "real time" anti-terrorism database system, substantial safety benefits might accrue.

Are there ways to protect against potential abuses? Proponents of this possible new technology have recommended the use of appropriate technologies to guard against unauthorized access and argue that a centralized database with rigorous safeguards better protects individuals than most existing systems. Creation or state implementation of any identification system may be found to require specific and rigorous requirements as to the means of keeping information confidential, preventing fraud, and guaranteeing accuracy of information.

Case Study #2: Facial Recognition Technology

Since September 11th, facial recognition technology, like a national ID system, has gained widespread publicity as public officials have looked to the emerging technology to help improve security, especially at America's airports. In California, Fresno's municipal airport has been using facial recognition technology to scan passengers entering the baggage screening area.[15] Other California airports, most notably San Francisco and Oakland, have announced plans to test the technology.[16] And, Olympic officials recently announced that facial recognition technology will be used to scan hockey spectators at the upcoming games.[17]

Last year, the Committee considered SB 169 (Bowen), a bill to restrict the use of biometric facial recognition technology by both public and private entities. Seeking to protect both personal privacy and the security of the collected data, the bill prohibited government agencies from, among other things, collecting or using biometric identifier information obtained through the use of facial recognition technology. Law enforcement agencies, acting pursuant to a warrant, were exempted from the bill's restrictions. The bill was later amended, deleting the above provisions and instead setting forth the intent of the Legislature to establish public policy on the public and private uses of biometrics technology to ensure personal privacy and civil liberties. The bill is currently in the Committee, and may be reconsidered this year.

Given the recent terrorist attacks on America and the growing interest in facial recognition technology as a means to help improve security, proposals dealing with the issue may be put forth, and such proposals appear well-suited for application of the proposed analytical template being considered for use by the Committee noted above.

Brief background on facial recognition technology. With respect to this emerging technology, the Assembly Judiciary Committee's analysis of SB 169 (Bowen) this past year stated the following:

> Facial recognition technology is based on the theory that every person's face is a slight spatial deviation on 128 facial types, each of which is represented in a numerical code that can be quickly compared with the faces in a database of thousands. According to Viisage, … the Company's face-recognition technology both enhances existing identification solutions and offers opportunities for a variety of new applications. Using a sophisticated algorithm based on Principle Component Analysis (PCA) developed at the Massachusetts Institute Technology's Media Lab, the Company's software translates the characteristics of a face into a unique set of numbers, which is referred to as the eigenface.
>
> The eigenface is used by both identification and verification systems for face comparisons made in real-time. Identification involves a one-to-many comparison of an individual's face against all faces in a database in order to determine identity; and verification is characterized as a one-to-one match of an individual's face to his or her stored image for the purpose of confirming identity. The software can instantly calculate an individual's eigenface from either live video or a still digital image, and then search a database of millions in only a few seconds in order to find similar or matching images.

Application of the Possible Anti-Terrorism Analytical Template to Facial Recognition Technology

What is the proposal and what problem does it seek to address? As noted above, facial recognition technology has been suggested to help improve our nation's security. As a result, proposals dealing with the issue may be put forth in the coming year. Proponents of facial

recognition technology argue that the technology is an important tool to help catch terrorists before they act. On the afternoon of September 11th, Visionics, a New Jersey-based leader in facial recognition technology, sent an email to reporters stating that CEO Joseph Atick "has been speaking worldwide about the need for biometric systems to catch known terrorists and wanted criminals."

Does the proposal appear to comply with the U.S. and California Constitutions? The increased use of facial recognition technology appears to raise some important constitutional questions. The U.S. Constitution protects individuals under the Fourth Amendment against unreasonable searches and seizures and limits the government's ability to collect information about individuals, generally requiring a warrant based on probable cause before a person may be searched. Proponents of the technology have argued that restrictions on its use by state and local officials are inconsistent with U.S. Supreme Court case law holding that "what a person knowingly exposes to the public … is not a subject of Fourth Amendment protection."[18]

The California Constitution explicitly grants California citizens the right to privacy, providing in Article I, section 1 that: "All people are by nature free and independent and have inalienable rights. Among these are... pursuing and obtaining...privacy." The California right of privacy derives from an initiative measure, which stated it intended to "prevent government and business interests from stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve another purpose or to embarrass us."[19]

In Hill v. National Collegiate Athletic Assn. the California Supreme Court held the NCAA's drug testing program did not violate the plaintiff student athletes' state constitutional right to privacy[20]. In reaching this decision, the Court articulated the three elements of a cause of action for violation of this state right to privacy. First, a legally protected privacy interest must be identified. The Court noted that legally recognized privacy interests are generally divided into two categories: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy") and (2) interests in making intimate personal decisions of conducting personal activities without observation, intrusion, or interference ("autonomy privacy").[21] Second, in order to state a claim for a violation, the plaintiff must have a reasonable expectation of privacy in the circumstances and third, there must be a serious invasion of the privacy interest by the defendant. The court must then balance these privacy concerns against other, competing important interests.

While the Hill decision did not turn on informational privacy, the Court stated that, "if intrusion is limited and confidential information is carefully shielded from disclosure except to those who have a legitimate need to know, privacy concerns are assuaged. On the other hand, if sensitive information is gathered and feasible safeguards are slipshod or nonexistent, or if defendant's legitimate objectives can be readily accomplished by alternative means having little or no impact on privacy interests, the prospect to actionable invasion of privacy is enhanced."[22]

Thus, it appears evident that proposals seeking to expand the use of such facial recognition technology for anti-terrorism efforts will face constitutional questions. However, it is not at all clear such proposals will be found constitutionally flawed.

To what extent might the proposal be pre-empted by federal law? It may be argued that a proposal relating to the use of facial recognition technology in California's airports raises federal preemption issues. On the one hand, federal regulations promulgated by the Federal Aviation Administration mandate that airports meet specified security requirements, including that the airport carry out a security program that "provides for the safety and security of persons and property on an aircraft operating in air transportation … against an act of criminal violence, aircraft piracy, and the introduction of [a] deadly or dangerous weapon, explosive or incendiary onto an aircraft."[23] On the other hand, airports are locally run and, while mandated to meet specified federal security requirements, seem to have broad discretion in how best to meet the security goals of the regulations.

Even if it is not likely pre-empted, will the proposal likely cause confusion or other problems by overlapping with federal law in the area, suggesting state deference to federal law in this area? It does not appear that federal action in this area has been so great as to require, or even suggest, state deference to federal law, though future federal legislation or regulations in this area might trigger such analysis.

Is there existing California law that accomplishes, or could accomplish, the goals of the proposed legislation? Existing law does not appear to prohibit or significantly regulate the collection of biometric data by government and private businesses in other circumstances.

Have there been earlier attempts to legislate in this area, and how did they fare? Is there any evidence the proposal will in fact address the identified problem? As noted above, last year the Committee considered SB 169 (Bowen), a bill to restrict the use of biometric facial recognition technology by both public and private entities. The bill prohibited government agencies, except for law enforcement, acting pursuant to a warrant, from collecting or using biometric identifier information obtained through the use of facial recognition technology. The bill permitted private entities to use the technology subject to certain conditions. SB 169 was heard by the Committee and failed passage. The bill was then heard on reconsideration, and a vote was postponed at that time. The bill has since been amended, deleting the above-noted provisions and instead setting forth the intent of the Legislature to establish public policy on the public and private uses of biometrics technology to ensure personal privacy and civil liberties.

With respect to whether the proposal will address the identified problem, supporters of the technology suggest that facial recognition technology would help improve security, particularly at our nation's airports. Proponents of the technology argue that biometric systems will assist law enforcement and others in capturing known terrorists and wanted criminals. Joseph Atick, CEO of Visionics, stated recently, "In the war against terrorism, especially when it comes to the homeland defense, the cornerstone of this is going to be our ability to identify the enemy before he or she enters into areas where public safety could be at risk."

Privacy advocates and other civil liberties groups, however, have raised some concerns regarding whether facial recognition technology will in fact help make our airports safer. On this point,

concerns have been raised regarding the reliability of facial recognition technology. The ACLU argues:

> [I]t is abundantly clear that the security benefits of such an approach would be minimal to non-existent, for a very simple reason: the technology doesn't work. … Facial recognition software is easily tripped up by changes in hairstyle or facial hair, by aging, weight gain or loss, and by simple disguises. A study by the Department of Defense found very high error rates even under ideal conditions, where the subject is staring directly into the camera under bright lights. The study found very high rates of both "false positives" (wrongly matching people with photos of others) and "false negatives" (not catching people in the database). That suggests that if installed in airports, these systems would miss a high proportion of suspects included in the photo database, and flag huge numbers of innocent people - thereby lessening vigilance, wasting precious manpower resources, and creating a false sense of security.

Will enactment of the proposal result in unintended consequences? Are there potential abuses that might arise if the proposal is enacted? Potential discriminatory application? Unnecessary invasions of privacy? Do the benefits outweigh any potential harms? As noted above, opponents of the increased use of facial recognition technology dispute the technology's effectiveness and raise concerns that innocent people will be falsely accused and wrongdoers will still evade detection. As a result, they argue unnecessary invasions of privacy may flow from this as "false positives" trip up misidentified individuals who may then be detained while their real identity is confirmed.

Civil liberties groups have also raised concerns regarding the databases the technology uses to scan for individuals suspected of a crime. Lee Tien, an attorney for the Electronic Frontier Foundation, stated recently, "A lot depends on the accuracy or completeness of the database against which you're matching. … who's in the database in the first place? Do they just have terrorists in it, or is anyone who's been suspected of a crime?" The question of whether an adequate database of terrorists is available to authorities is an important one since, as has been pointed out recently, pictures of Timothy McVeigh and Theodore Kaczynski were not available to authorities until they committed their criminal acts. Also, of the 19 terrorists suspected of the hijackings on September 11th, only two of them were apparently previously known to authorities. Thus, the argument goes, the technology is only as good as the database it relies upon.

On the other hand, advocates of the technology argue that the possible benefits of the technology outweigh any potential harms and note that if Osama bin Laden were to walk through the Fresno airport, their facial recognition technology system would be ready. They also point out that authorities had photographs of two of the suspected hijackers, and argue that a facial recognition system would have caught them before they boarded the doomed airliners. On this point, Tom Colatosti, president and CEO of Viisage Technologies, stated "… this technology could make the most impact. After all, two of the hijackers on September 11th were on an FBI watch list. If their faces had come up as a match, things might have turned out differently."

Are there ways to protect against potential abuses? The industry has suggested safeguards to address some of the concerns raised, such as a "no match-no memory" system which would insure that images are not kept by the system unless matched to a person with a known criminal history. In addition, SB 169 also included provisions to help safeguard the security of data collected through the use of facial recognition technology, placing restrictions on when businesses may sell or share the information and requiring that the information be encrypted or otherwise secure from unauthorized access.

Conclusion

As the use of the possible analytical template demonstrated in the case studies above, careful and consistent analysis of anti-terrorism proposals by policymakers appears to be an important objective. In discussing Attorney General Ashcroft's plan for fighting terrorism recently, University of Southern California law Professor Erwin Chemerinsky pointed out the importance of carefully examining anti-terrorism proposals, stating:

> Great care must be taken to not repeat the mistakes of the past where significant freedoms were lost in times of crisis without any gain in security. During World War I, laws were enacted to punish critics of the war effort. Mild and ineffectual speech led to long prison sentences. During World War II, more than 100,000 Japanese Americans were uprooted and placed in what President Franklin D. Roosevelt called "concentration camps." Nothing was gained in security from this unconscionable loss of freedom. Not one Japanese American was charged or convicted of any crime against the war effort.
>
> In hindsight, these mistakes occurred because the public, Congress and even the courts were reluctant to challenge the executive proposals in a time of crisis. This mistake must not be repeated. Dissent is never disloyal. Patriotism means supporting the country but not any particular proposal.[24]

Thus the Committee hopes the possible analytical template discussed and exemplified above proves helpful in its deliberations over the important anti-terrorism proposals it anticipates evaluating in the coming year. To the extent others find this possible analytical tool useful, the Committee recommends its consideration and potential use as one of many possible methods for evaluating and comparing the potential strengths and weaknesses of upcoming anti-terrorism proposals.

---

[1] "Criminal defense lawyers object to eavesdropping rule," *The Washington Times*, November 10, 2001.
[2] California Constitution, Article I Section 1.
[3] American Academy of Pediatrics v. Lungren, (1997) 16 Cal. 4th 307, 329; Smith v. Fresno Irrigation District (1999) 72 Cal. App. 4th 147, 161.
[4] "Smart Cards: Digital IDs can help prevent terrorism," *Wall Street Journal*, October 8, 2001.
[5] "Identity Card May Fly as Lines Grow Longer," *Seattle Times*, November 20, 2001.
[6] "Driver's Licenses Could Serve as National IDs," CNSNews.com, November 20, 2001.
[7] "Congress Hears National ID opinions," Federal Computer Week, November 19, 2001.
[8] Terry v. Ohio (1968) 392 U.S. 1.
[9] Kolender v. Lawson (1982) 461 U.S. 352.
[10] 461 U.S. at 362.

[11] Hill v. NCAA (1994) 7 Cal.4th 1.
[12] Perkey v. DMV (1986) 42 Cal.3d 185
[13] Written Statement of Professor Jonathan Turley, George Washington University Law School, submitted for the Oversight Hearing on National Identification Cards of the House Committee on Government Reform's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, November 16, 2001.
[14] Testimony of Katie Corrigan, ACLU Legislative Counsel, submitted for the Oversight Hearing on National Identification Cards of the House Committee on Government Reform's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, November 16, 2001.
[15] "Terror ID system debuts in Fresno," *The Sacramento Bee*, November 24, 2001; "ACLU calls on Fresno airport to stop using face ID system," *The Los Angeles Times*, November 20, 2001.
[16] "Airport to get facial recognition technology," *The Los Angeles Times*, October 29, 2001.
[17] "Olympics to use facial recognition," *The Associated Press*, November 15, 2001.
[18] Katz v. U.S., (1967) 389 U.S. 347.
[19] Prop. 11 Ballot Argument, Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972).
[20] Hill, *supra* note 11 (1994).
[21] Id. at 35.
[22] Id. at 38.
[23] Federal Aviation Regulation, 14 CFR 107.101.
[24] "Giving up our rights for little gain," *The Los Angeles Times*, September 27, 2001.