CRIMINAL INTELLIGENCE SYSTEMS:

A CALIFORNIA PERSPECTIVE

Bill Lockyer, Attorney General

California Department of Justice
Division of Law Enforcement

September, 2003

TABLE OF CONTENTS

I.

OVERVIEW

A criminal intelligence system engages in three general functions: (1) collection and analysis of information; (2) storage and maintenance of that portion of the information that qualifies as criminal intelligence and (3) limited dissemination and use of the intelligence information to enhance public safety. It is important to emphasize that there is a major responsibility which accompanies the operation of a criminal intelligence system, that is *the protection of the privacy of the persons or entities whose names are put into the system*:

> "Disclosure of public records . . . involves two fundamental yet competing interests: (1) prevention of secrecy in government; and (2) protection of individual privacy." (*City of San Jose v. Superior Court* (1999) 74 C.A. 4th 1008, 1017; see also *C.B.S. Inc. v. Block* (1986) 42 C.3d 646, 651 and *California State University, Fresno Assn. Inc., v. Superior Court* (2001) 90 C.A.4th 810, 823.)

Thus, the process of gathering information, some of which becomes part of an intelligence system, creates a tension between the needs of society and the expectations of members of society. Put another way, when law enforcement engages in intelligence operations it must necessarily intrude on the privacy of those persons about whom it gathers information, and then is obligated to protect the information to the extent legally permitted.

In the early part of the last century there was a societal bias in favor of a "paternalistic" view of law enforcement. This bias was premised on the general attitude that law enforcement acted with the public good as its goal and, therefore, the methods employed were necessary. Generally speaking, law enforcement was given considerable latitude regarding the methods that could be employed to do its job. In fact, because of the latitude given and the fact that criminal activity was generally viewed as "unorganized", there was little emphasis on intelligence. As a result, there were

virtually no statutes which governed intelligence gathering or any other aspect of the intelligence process.

The view that criminal activity was not organized also gave rise to the notion that criminal activity was essentially local in scope and impact. Consequently, law enforcement agencies tended to focus their efforts on local problems as opposed to engaging in cooperative, multi-jurisdictional efforts. A by-product of this focus was that any intelligence gathered was generally not shared among agencies.

California became concerned about organized crime as a separate and distinct activity in the late 1940's. On November 11, 1947, the Governor established a commission to study and report on organized crime as part of an overall effort against all types of criminal activity (see former Penal Code § 6028.3, enacted in 1947). The organized crime commission became known as the Standley Commission (after its chairperson).

The Standley Commission published four reports during the time of its existence (1947-1950). Its second report (March, 1949) concluded that California had an organized crime problem. The third report (March, 1950) attributed the success organized crime attained to its multi-jurisdictional structure and the lack of cooperation or coordination amongst law enforcement. In its final report (November, 1950), the Commission suggested that there be greater leadership by the Attorney General and recommended continued study of the problem.

Nineteen-fifty was the year in which the Kefauver hearings in the United States Senate introduced the Mafia to the American public. These hearings emphasized the need for law enforcement agencies to make intelligence gathering and dissemination a high priority.

Certain facts about intelligence became apparent. **First**, to be useful intelligence had to be shared. **Second**, it had to be accurate and current. **Third**, it had to be maintained and gathered in a uniform way. These facts later spurred legislative bodies to enact or amend laws to balance the intrusion necessary to successful intelligence functions and the individual rights of citizens. Not surprisingly the judicial system was the forum in which the meaning of these laws was often established.

California followed the final Standley Commission recommendation and created a second organized crime commission. This second commission operated from October 1951 to May 1953. After numerous hearings and reviews of the work of both the Standley Commission and the Kefauver Committee, this commission made several recommendations.

Two of the recommendations are particularly important in the criminal intelligence context. **First,** taking a page from the Kefauver Committee, the need to increase cooperation amongst law enforcement agencies was stressed. **Second,** it was recommended that there be a statewide intelligence system dealing with organized crime in the Attorney General's office.

While there was little, if any, legislative focus on criminal intelligence or organized crime in California from 1953 until 1957, one singularly important step was taken.

In 1956, twenty-six local and state law enforcement agencies formed the Law Enforcement Intelligence Unit (L.E.I.U.). The central coordinating agency was then and continues to be the California Department of Justice. Perhaps the most important aspect of L.E.I.U. was its development of guidelines dealing with criteria for gathering, analyzing, maintaining, and disseminating intelligence information (see Appendix 1, current L.E.I.U. guidelines). This effort to limit the information collected, maintained and disseminated by imposing the discipline of

analysis and the adoption of standards (see Appendix 1) was found by the courts to be within the statutory definition of intelligence information deemed to be conditionally exempt from public access (see *American Civil Liberties Union Foundation v. Deukemejian* (1982) 32 C.3d 440, 443). Indeed, the courts found that intelligence information that complied with such guidelines could be conditionally exempt even if disclosure to the public would not reveal the identity of a confidential source. (*American Civil Liberties Union Foundation, supra,*):

> "The term 'intelligence information', even if read narrowly so as to further the Act's [California Public Records Act] objective of expanded disclosure, should protect information furnished in confidence even if that information does not reveal the identity of a confidential source." (at 443.)

Thus, the threshold issue became not the protection of a source, rather the focus is on whether the information was furnished in confidence. In practical terms it meant that the concept of intelligence information was as broad as the concept of "official information" (Evidence Code §1040(a); see Appendix 2).[1]

On the federal level there were further hearings. The Federal Bureau of Investigation began to compile intelligence files on organized crime. However, there was no legislation by Congress.

In August, 1957, the California Assembly created the Subcommittee On Rackets. This body held hearings over a two-year period. The final report was filed in 1959. This report recommended various legislative initiatives to "attack" organized crime, among the initiatives was the suggestion of creating a statewide intelligence system. Little action was taken on the various recommendations.

No new initiatives were undertaken at either the state or federal level until the 1960's.

---

[1]This standard becomes important in terms of the distinction between intelligence information and investigatory information (*A.C.L.U., supra,* fn. 10 at 449). This distinction is fundamental to the argument that intelligence information does not have to be furnished as part of discovery in a criminal case (see Appendix 16).

Much of the legal and legislative development in the criminal intelligence area occurred in the 1960's when so-called "radical" political and social events were occurring. It was during this same time that concern about personal privacy loss vis-a-vis government information gathering became a more important issue. At least three factors during the 1960's interacted to create the environment that shaped the federal and state legislative action. These factors were: **First**, confrontations between government and persons or groups challenging the decisions made by government; **second**, the use of computers to store and disseminate information about persons and groups; and **third**, focus on the three underlying issues surrounding intelligence systems: personal privacy; information gathering and dissemination; and open government. One result of Congress' focus on these issues was the enactment in 1967 of the Freedom Of Information Act (Title 5 U.S.C. § 552; see Appendix 3; hereinafter this legislation will be abbreviated as F.O.I.A.) and the Right of Privacy Act (Title 5 U.S.C. § 552a; see Appendix 4).

Also in 1967, the President's Commission On Organized Crime made its report. This document endorsed the use of criminal intelligence by law enforcement. Another federal entity, the Law Enforcement Assistance Administration also released a study of organized crime which made recommendations regarding how to address the problem, it too supported use of intelligence.

During this same time period, as a result of hearings chaired by Senator McClellan, Congress began consideration of what has become known as the Omnibus Crime Control And Safe Streets Act Of 1968 (see Title 42 U.S.C. § 3711, et. seq.). This legislation addressed wiretap (see 18 U.S.C. § 2510, et. seq.) racketeering (see 18 U.S.C. § 1961, et. seq.) and regulation of intelligence operations (see Title 42 U.S.C. §§ 3782(a) and 3789g (c)–Appendices 5 and 6 which in turn gave rise to the regulations found in Code of Federal Regulations, Title 28, part 23, Appendix 7).

While California did not pass any legislation regarding intelligence at this time, then Attorney General Lynch proposed and the Legislature funded an Organized Crime Prosecution Unit (Budget Act of 1967-1968). In June, 1969, this Organized Crime Unit published a progress report. One of the objectives identified in that report was the creation of a comprehensive intelligence system. Such a system, focused on organized crime, was created by legislation enacted in 1971, and became operative on January 6, 1972 (see Appendix 8, Government Code section 15025 et seq.).

On the federal side of intelligence system structure, the Regional Information Sharing System (RISS) program was initiated in 1973. These six systems[2] combined to create a computerized national intelligence system.

As the federal and state operation of intelligence systems became more widespread, the tension between public access to government records and the need for an appropriate level of secrecy to permit certain government operations become the subject of litigation (see e.g., *Black Panther Party v. Kehoe* (1974) 42 C.A.3d 645; *State of California ex rel Division of Industrial Safety* (1974) 43 C.A. 3d 778; *Los Angeles Police Department v. Superior Court* (1977) 65 C.A.3d 661.) The issue which consistently emerged was the need to establish a proper balance of interests.

California addressed this balancing issue by focusing on the access side of the ledger. In other words, California has not enacted legislation which has created a framework like that imposed by Title 28 C.F.R., Part 23. Instead, it has adopted a comprehensive public records act which encourages access.

The various legislative bodies, including California's, which have enacted strong public access laws have also addressed the concern that public safety should not be jeopardized. These

---

[2] California is part of the Western States Information Network (WSIN).

bodies appreciated that much of the work law enforcement does depends on secrecy for success. Consequently the laws enacted generally provided exceptions that applied to many law enforcement records. *However, it is important to emphasize that these exceptions are not absolute, they are conditional.* (*C.B.S., Inc. v. Block* (1986) 42 C.3d 646, 652.) As will be discussed in greater detail, *infra,* this means that the custodian of intelligence materials as an interested party with standing[3] must assert an exemption and satisfy a court that disclosure is not required.

After the legislative frameworks were imposed and the social/political climate changed, criminal intelligence systems lost their "hot button" status for several years. Several recent trends have once again caused more attention to be focused on the need for intelligence systems. These trends are: (1) conspiratorial/criminal activities such as gangs; (2) the increase of terrorist activities in the United States; (3) the growth of "fringe" groups which express their beliefs in unlawful ways (i.e., so called "militia" groups); (4) activities of foreign crime groups in this country and (5) a need to track certain types of criminal offenders (such as sexual predators) who present major risks to especially vulnerable groups of citizens.

Not surprisingly, as the use of criminal intelligence systems grows, the level of scrutiny given to these systems will also increase.

An investment in the intelligence process is not without risk to a law enforcement agency. This is because of the nature of the endeavor. It is important to remember that the process of gathering, analyzing and using intelligence is primarily a "covert" process. Success of an intelligence system depends on secrecy and, of course, secrecy grows out of the ability to gather

---

[3] An agency which has provided information and which has been given notice of a request might also have standing.

information about groups and individuals which does not have to be disclosed to those groups or individuals. Thus, the "intelligence culture" exists in an overall culture which values openness and full disclosure by government as well as associational freedom and individual privacy.

The successful operation of an intelligence system requires that law enforcement understand and respect the limits to which privacy can be set aside to meet intelligence needs. Law enforcement must also understand the need to protect the information it has gathered because of its private nature. And, law enforcement must be sensitive to the issue of how criminal intelligence operations and their products are perceived by four groups. These groups are: (1) the agency's governing body; (2) the various mediums of communication; (3) the courts, and (4) the public.

Governing bodies are, of course, the funding source and are also empowered to legislate. These bodies are sensitive to public opinion and typically do not like controversy. Because intelligence efforts are potentially controversial, the governing body must have confidence in these efforts. The governing body should be made aware in a general way of what the intelligence operation's contribution to the agency's effort to protect the public has been.

The various mediums of communication (newspapers, radio and television) view their mission as ensuring that the public's "right to know" is enforced. Enforcement of this "right to know" often leads to situations in which the communication mediums will seek to compel disclosure of information law enforcement believes should not be disclosed. While it is always useful to remember Mark Twain's admonition to "Never pick a fight with someone who buys ink by the barrel," it is law enforcement's obligation to endeavor to protect the privacy of the information about persons and organizations which is contained in the intelligence system.

The courts are the forums in which the disputes over access to intelligence system information will be resolved. If the courts conclude that intelligence operations have been conducted properly and the products generated have been used properly, operations will be supported and the information contained in the system will generally be protected. Judicial approval has been and will continue to be the best defense against unfavorable treatment by the various communication mediums, the best confidence builder for the governing body and an important assurance for the public and its representatives that law enforcement is using this important tool in a responsible manner.

The best assurance for public acceptance of intelligence operations are clear guidelines that focus intelligence efforts on illegal activities, and do not encourage surveillance of people or groups engaged in acts of protest or civil disobedience. We do not mean to suggest that law enforcement should not be aware of disruptive events taking place in a community that may affect public safety, but it is one thing to ensure that law enforcement officers are aware of the potential for disruption, and quite another to focus intelligence operations on those participating in or organizing such events in the absence of credible information that they intend to engage in or encourage criminal acts. When policies and intelligence efforts focus on criminal wrongdoing and recognize the rights of people to engage in protest as a means of political expression, the public can be assured that law enforcement agencies have struck the right balance between public protection, associational freedom and individual privacy. The California Supreme Court emphasized these principles in *White v. Davis* (1975) 13 Cal.3d 757.

A successful intelligence operation is the result of: (1) an understanding of the legal principles which apply; (2) organization of the agency so that it is committed to proper collection,

analysis, maintenance and use of intelligence information; and (3) cultivation of support for and understanding of the value of the intelligence operation in the community which will lead to acceptance and understanding of the scope of that operation. The balance of this document will examine these areas.

II.

APPLICABLE LAW: CONSTITUTIONAL PROVISIONS

Generally speaking, the two primary foundations of law applicable to the intelligence arena are privacy and freedom of association and/or expression. There are both federal and state laws (statutory and decisional) which relate to intelligence activities. The federal laws and the state laws are essentially complementary. The federal government has not "occupied the field" which means that state (and in some instances local) jurisdictions may pass laws in the area so long as these laws do not provide less privacy protection than the federal laws.

Because of the fact that the area is open to state regulation, it is necessary to consider both federal and state legal aspects. Also, it is important to remember that California state law has, in some instances, left the "field" open to local regulation. Thus, one should always ascertain whether there are local regulations which apply. This document will not attempt to catalog local regulations because of the number of jurisdictions involved.

A.

FREEDOM OF ASSOCIATION/EXPRESSION

1.

Federal Concepts

The First Amendment to the United States Constitution is the source of the right to associate with whomever one chooses and the right to speak freely. This means that mere membership in an organization, regardless how unpopular, cannot be criminal (see e.g., *Scales v. United States* (1961) 367 U.S. 203, 223; *People v. Green* (1991) 227 C.A.3d 692, 699-700 holding that mere membership in a gang is not a crime. However, also note *People v. Bailey* (2002) 101 C.A.4th 238 which held

that once a person was convicted of a gang-related crime, he/she could be required to register (at 244)) and that speech, regardless how offensive, is protected so long as it does not immediately incite or encourage the doing of an unlawful act (see e.g., *McCoy v. Stewart* (9th Cir., 2002) 282 F.3d 626, 631-632 holding that merely advocating gang membership and/or gang activity could not be criminally prosecuted).

If, however, one is associated with a criminal enterprise and acts in a way that carries out the criminal objective(s) of that enterprise, the association with the enterprise can be the predicate for prosecution. More important to this manual's discussion is the fact that criminal associations exist and, as will be discussed, this fact provides a legal basis for gathering and maintaining intelligence on those associations and their members. Thus, as the court in *People v. Castenada* (2000) 23 C.4th 743 held, membership and involvement that is more than ". . . nominal or passive." *will* support a criminal conviction (see discussion at 749-752); note also that the overall analysis in *Green, supra,* is significantly overruled by *Castenada*). It is the author's opinion that the activities described in both *Green* and *McCoy* would support entry into an intelligence file.[4]

2.

State Concepts

California's Constitution also provides protection for the rights of privacy, speech and association (California Constitution, Article I, §§ 1-3). As in the federal framework, it is not a crime to belong to non-mainstream groups or to say unpleasant things. Also like the federal framework, California law permits the prosecution of persons whose associations are connected with the criminal conduct of the groups with which there is association (see e.g., Penal Code § 186.20).

---

[4]However, merely because there is a gathering to express political views or to engage in religious practices will not, without more, justify inclusion of these events in an intelligence file.

Thus, certain associations, with gangs as an example, are properly the subject of intelligence operations by law enforcement.

3.

Summary

Neither the federal law nor California law allow mere uninvolved association or non-inciting speech to be the sole basis for allegations of criminal conduct. Unless the association is active and with a group which has a criminal goal or history of criminal conduct or the speech directly and immediately incites criminal acts, these protections mitigate against gathering intelligence merely because of association or speech. In fact, it is typically the case that allegations of abuse of the intelligence gathering function arise out of "targeting" of persons or groups whose exercise of the rights of freedom of speech or association cannot be demonstrated to relate to definable criminal activity. A classic example of the problems that arise when information gathering focuses on "unpopular" speech or "bad" associations which have no nexus to criminal conduct is found in *White v. Davis* (1975) 13 C.3d 757. Put bluntly, it is a mistake of constitutional dimension to gather information for a criminal intelligence file where there is no reasonable suspicion of the existence of a criminal predicate.

B.

PRIVACY

Legal concepts that are collected under the general heading of the "Right of Privacy" are always in issue in connection with intelligence operations. In general terms, this right is described as the right of citizens to be free from government intrusion into their lives. The process of intelligence gathering is, in the first instance, obtaining information about the lives of citizens. The process of intelligence sharing is also privacy driven in that the goal is to reveal the information gathered only to those who should receive it, not to the public generally. This puts those involved

in the intelligence process in the position of having to, first, justify an intrusion on a person's privacy and, second, after the intrusion has occurred, having the responsibility to protect the information gathered from all except those few who are legitimately entitled to access the information.

1.

Federal Concepts

The federal constitution, which included the Bill of Rights, was ratified and adopted in 1789. The Bill of Rights portion of the constitution, the first ten amendments,[5] established the balance of authority between the individual citizen and the government. However, the federal constitution does not include an express provision establishing a "right of privacy." (*American Academy of Pediatrics v. Lungren* (1997) 16 C.4th 307, 326.) Thus, for many years the concept of privacy did not appear in the jurisprudence of the United States Supreme Court.

Privacy began to matter, in the legal context, when Justice Brandeis wrote a dissent in the case of *Olmstead v. United States (1928) 277 U.S. 438.*[6] *Olmstead* involved the question whether it was legal to "wiretap" a telephone conversation without the consent of the parties. The majority of the United States Supreme Court upheld law enforcement use of non-consentual wiretap. Justice Brandeis advocated the opposite result on the theory that the parties to the telephone call had an expectation of privacy in their conversation.

Thirty-seven years later in *Griswold v. Connecticut (1965) 381 U.S. 479* the majority of the United States Supreme Court overturned a state law forbidding advice about the use of contraceptives because it found an implied constitutional right of privacy in the "penumbras" of

---

[5]One court has stated it in terms that the concept of privacy is "fundamental" to the rights articulated in the first, third, fourth, fifth, and ninth amendments (see *Ortiz v. Los Angeles Police Relief Association* (2002) 98 C.A.4th 1288, 1301; see also *Hill v. National Collegiate Athletic Assn.* (1994) 7 C.4th 1, 21).

[6]Brandeis first explored the concept of the "right to privacy" in an article he co-authored in 1890 (see 4 Harvard Law Review 1931).

several of the express constitutional rights contained in the first ten amendments. *Griswold* was followed by *Berger v. New York* (1967) 388 U.S. 41 and *Katz v. United States* (1967) 389 U.S. 347. *Berger* invalidated a state law which permitted court ordered "bugging" as overbroad and, therefore, in violation of federal constitutional safeguards.

Katz rejected the notion that privacy was a location based right and held that it was a personal right that attached to the individual and not to the place.

The time frame of these decisions was fortuitous for those who believed that the long held view of law enforcement as a benevolent, paternalistic institution should be set aside. The focus of legislatures and the courts became the correct balance between the needs of law enforcement and the now constitutionally based privacy rights of the individual. The impact of *Griswold, Berger,* and *Katz* in the states was to establish a constitutionally compelled minimum standard. That is, no state could enact, enforce or interpret laws in a manner which would provide less protection than these decisions required.

Thus, in the late 1960s, Congress was faced with the need to address the growing problems of organized criminal activity within the judicially established framework of privacy protection. The result was the enactment of three statutory schemes: (1) The Omnibus Crime and Safe Streets Act of 1968; (2) The Federal Freedom of Information Act (5 U.S.C. § 552); and (3) The Federal Right of Privacy Act (5 U.S.C. § 552a) which are discussed, *infra.*.

2.

State Concepts

As has been noted, California is subject to the rules protecting privacy established by *Griswold, Berger, Katz* and subsequent United States Supreme Court decisions. However, California has also developed a specific set of rules in this area.

In many respects California's seminal case dealing with the intelligence process is *White v. Davis* (1975) 13 Cal.3d 757.[7]

The factual situation in *White* was that the Los Angeles Police Department became convinced that certain subject matter being presented in particular college classes should be monitored for intelligence purposes. When this activity was discovered a taxpayer's suit was filed to terminate the activity. In its defense the police department argued that the monitoring was, under the circumstances, an appropriate intelligence gathering activity. The California Supreme Court disagreed:

> "Although the police unquestionably pursue a legitimate interest in gathering information to forestall future criminal acts, the identification of that legitimate interest is just the beginning point of analysis in this case, not, as defendant [L.A.P.D] suggests, the conclusion. The inherent legitimacy of the police 'intelligence gathering' function does not grant the police the unbridled power to pursue that function by any and all means. In this realm, as in all others, the permissible limits of governmental action are circumscribed by the federal Bill of Rights and the comparable protections of our state Constitution." (*White, supra*, at p. 766.)[8]

The court in *White* then analyzed the police conduct in the context of its impact on the rights to the exercise of free speech and association. One factor that the court singled out for comment was that the complaint alleged "that the information gathered by the undercover police officers pertains to no illegal activity or acts." (*White, supra,* at p. 773 .)[9] Thus, the lesson of *White* is that *absent*

---

[7]Indeed, in its discussion of California's constitutional privacy amendment, the state supreme court stated: "Our privacy initiative jurisprudence emanates from *White v. Davis* . . ." (*Hill v. National Collegiate Athletic Association* (1994) 7 Cal.4th 1, 32).

[8]In this regard the state constitutional right of privacy is a self-executing right that created a separate privilege from any legislatively created privileges. (See *Davis v. Superior Court* (1992) 7 Cal.App. 4th 1008, 1014; *Cutter v. Brownbridge* (1986) 183 Cal.App.3d 836, 842).

[9]This case arose as the result of the trial court granting a demurrer without leave to amend (essentially the same as a dismissal). Therefore the defendant police department had not stated what specific reasons, if any, justified the activity. The matter was remanded to the trial court to give the police the opportunity to demonstrate a compelling state interest which would justify the alleged infringement on these first Amendment rights and the right of privacy. The police were

an articulable criminal predicate for the gathering of information it will not be possible to justify it under the general heading of intelligence activity. Specifically, *White* teaches that there must be some connection between the information gathered and unlawful activity. Put another way, *White* is a warning to law enforcement in California that it cannot operate from the premise that it can gather intelligence on citizens' activities regardless of any articulable connection to unlawful action.

One result of the *White* case was legislation in the form of an initiative submitted to and approved by the voters which enacted an express state constitutional right of privacy.[10] A subsequent case before the California Supreme Court, *Hill, supra*, involved this privacy provision. *Hill* was a civil case which arose as a challenge to drug testing policies applicable to college athletes. The theory of the case was that the drug testing policy violated the state constitutional right of privacy. *Hill* is important because it, once again, gave notice of the sort of activity the court believed was improper:

> "The principle focus of the Privacy Initiative is readily discernable. The Ballot Argument warns of unnecessary information gathering, use and dissemination by public and private entities - images of 'government snooping' computer stored and generated 'dossiers' and 'cradle-to-grave' profiles on every American' dominate the framers' appeal to the voters. . . . The evil addressed is government and business conduct in 'collecting and stockpiling unnecessary information . . . . and misusing information gathered for one purpose in order to serve other purposes or to embarrass . . . . "' The [Privacy Initiative's] primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."' (*Id.* at p. 21.)

The critical threshold for an intelligence operation to meet to justify gathering information becomes clear from the *White* and *Hill* cases. Information collected should be necessary to a public purpose such as protecting the public's safety. This is another way of saying that where there is no

---

also required to establish that their purposes could not be achieved by less restrictive means. Thus, the California Supreme Court did not specifically rule on the validity of any particular police practice, but rather held that these covert activities in the university setting presented a sufficient threat to the constitutional rights that the government must justify them.

[10]The full text of this constitutional amendment is found in Appendix 9.

indication that the information relates to acts which impact the safety of the public or individual members of the public it should not be collected.

Hill went on to point out that there were two broad, general categories of privacy.[11] (*Id.*, at p.30.) These two categories were described as "informational privacy" and "autonomy privacy." (*Hill, supra*, at p. 35.)

Informational privacy is the individual's interest "in precluding the dissemination or misuse of sensitive and confidential information . . . ." Autonomy privacy is the individual's interest in making intimate personal decisions or conducting personal activities without observation, intrusion or interference . . . ." (*Hill, supra*, at p. 35.) Although it is generally the case that an intelligence operation will be in the realm of informational privacy, many of the sources of intelligence information (electronic surveillance as an example) will be in the realm of autonomy privacy.

The *Hill* case made two additional observations worth repeating. **First**, as is the case with all constitutional rights, the right of privacy is not absolute. (*Hill, supra*, at p. 35). **Second**, each situation will be fact driven and unique: ". . . privacy interests are best assessed separately and in context. Just as the right to privacy is not absolute, privacy interests do not encompass all conceivable assertions of individual rights." (*Hill, supra,* at p. 35; see also *Ortiz, supra,* 1304-1305 and 1307-1308).

In this connection, it is important to remember that so long as the state law does not provide less protection than federal law mandates it may differ from federal law. As the court in *Planned Parenthood Golden Gate v. Superior Court* (2000) 83 C.A.4th 347 observed in connection with California's constitutional right of privacy:

---

[11]Privacy is also mentioned in California's Constitution at Article I, section 24 (part of Proposition 115). This provision, applicable only to criminal cases, sought to make it the law that privacy concepts based only on the United States Constitution were controlling. However, this aspect of the law was later ruled to be unconstitutional by the California Supreme Court. (See *Raven v. Deukmejian* (1990) 52 Cal.3d 336.)

". . .[it is] broader and more protective of privacy than the (implied) federal constitutional right of privacy. . ." (at 357)

3.

Summary

The fact that there are two separate constitutional layers means that any question whether an intelligence gathering activity meets constitutional standards must consider both federal and state law. Further, as will become more clear in the discussion of the specific statutory provisions and their application which follows, the success of an intelligence effort depends on the ability to demonstrate that it was undertaken ". . . to forestall future criminal acts . . ." (*White v. Davis, supra,* at 766). If a connection between the information gathered and the prevention (or solution) of a criminal act can be shown then, the author submits, there will be no constitutional (federal or state) flaw.

III.

APPLICABLE LAW: STATUTORY PROVISIONS

A.

Laws Governing Gathering/Maintaining/Disseminating

1.

Federal Laws

a.

THE OMNIBUS CRIME AND SAFE STREETS ACT OF 1968

This broad legislation enacted provisions regarding electronic surveillance (18 U.S.C. § 2510 et. seq.) and authorized the development of guidelines governing the collection, maintenance and use of intelligence. The authorization to develop guidelines regarding intelligence resulted in the promulgation of the regulations contained in Title 28 Code of Federal Regulations, Part 23.

The Senate report regarding the 1968 Omnibus Crime And Safe Streets Act (see 1968 U.S. Code Congressional and Administrative News 2112, Senate Report No. 1097) favorably noted the need for cooperative intelligence efforts directed at organized crime. The report referred to the Commission On Organized Crime recommendation that every major city have an intelligence unit in its police department (see page 2120). In the context of the wiretap/eavesdropping proposal, the Senate Report stated:

> "The proposed provision (18 U.S.C. § 2517) envisions close Federal, State, and local cooperation in the administration of justice. *The utilization of an information-sharing system within the law-enforcement community circumscribed by suitable safeguards for privacy is within the intent of the proposed legislation.* Examples of existing systems include the law enforcement intelligence unit established in California in 1956, the New England State Police compact . . . the New York State identification and intelligence system and the National Information Center." (At page 2188; emphasis added.)

Because the Congress found that the Omnibus Crime And Safe Street Act was legislation necessary to carry out the constitutional requirements articulated in *Berger, supra,* and *Katz, supra,* 28 C.F.R. 23 should be viewed as constitutionally compelled. The Congressional reference to L.E.I.U. suggests

that the guidelines developed by L.E.I.U. can serve as one standard by which to measure the constitutionality of system provisions.

b.

Code Of Federal Regulations, Title 28, Part 23

The coincidence of the legal and legislative concern about privacy which has been briefly reviewed, *supra*, occurred in an environment of significant civil unrest. As a consequence, as has been noted, while there was a desire to encourage law enforcement to gather and use intelligence, there was also a desire to ensure that this activity did not improperly impinge on individual rights of speech, association or privacy.

One other factor affecting the environment at the time was the development of new sophisticated computers that enabled law enforcement to "pool" knowledge in a central data bank and disseminate it to participating agencies. Because of the reach and power of this type of system the federal government promulgated the regulations found at 28 Code of Federal Regulations, Part 23 (hereinafter 28 C.F.R. 23; see Appendix 7 for the full text).

> "The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for federally funded projects are required." (28 C.F.R. 23 § 23.2.)

As the language clearly states, 28 C.F.R. 23 exempts from its coverage those systems which are not federally funded. However, it also makes it clear that federally funded projects such as the R.I.S.S. projects cannot share information with systems which do not have criteria as stringent as 28 C.F.R. 23 in place (see 28 C.F.R. 23, § 23.20 (f)(1)). Thus, in the author's opinion, a complete and responsible intelligence operation should comply with 28 C.F.R. 23.

Therefore, information can be maintained only when it is based on a *reasonable suspicion* of *involvement in criminal activity or conduct* which information has been *validated* within a

reasonable period of time. Interestingly enough, information about political, religious and social views, associations or activities *is not* off limits when it relates directly to criminal conduct or activity which is the predicate and there is reasonable suspicion that the subject is involved in that criminal activity:

> "(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is *reasonable suspicion that the individual is involved in criminal conduct or activity.*
>
> (b) A project *shall not collect or maintain criminal intelligence information about the political, religious, or social views, associations or activities* of any individual . . . group, association, corporation, business, partnership, or other organization *unless such information directly relates to criminal conduct or activity and there is a reasonable suspicion that the subject of the information is or may be involved in the conduct or activity."* (28 C.F.R. 23 §§ 23.20(a) and (b); emphasis added.

Ortiz, supra, although not an intelligence system case, is a possible example of a circumstance where an associational interest could be intelligence data. In *Ortiz*, the court upheld a job termination based on a public employee's intention to marry a prison inmate. The court found that there was a significant enough likelihood of substantial danger to overcome any privacy interest. One could argue that *Ortiz* illustrates an association that meets the direct relationship requirement.

The *Ortiz* court noted that associational freedom was part of or closely related to the right of privacy (at 1302-1303). As is true of privacy, this right has two parts: (1) a right to intimate association and (2) a right to expressive association (at 1302-1303). After pointing out that associational freedom, like privacy, is not an absolute (at 1307-1308) the court weighed the interests involved. It concluded that the premium placed on confidentiality of peace office personnel files outweighed the "intimate association" right. Most important is the fact that no breach of confidentiality had been shown. It was the gravity of the potential breach which persuaded the court (at 1313).

A major concern is that no intelligence system may include information which has been obtained in violation of federal, state or local law. The resolution of this problem requires that the involved agencies agree upon guidelines that meet the 28 C.F.R. 23 standard.

Last, but of great importance, 28 C.F.R 23 mandates that all systems subject to its requirements have in place procedures which ensure that information retained ". . . has relevancy and importance." (28 C.F.R. 23, § 23.20 (h).) Or, to use the other statement of the requirement, the system must delete ". . . any information which is misleading, obsolete or otherwise unreliable. . . ." § 23.30 (h).) No retention period may exceed five years without review. The validation criterion is that the retained information continues to comply with the initial entry criteria.

It is the author's view that all systems ought to comply with the 28 C.F.R. 23 standards because these standards have proven that when properly applied they achieve the appropriate balance between law enforcement intelligence needs and individual privacy needs.[12] Intelligence efforts at any jurisdictional level which employs *criminal intelligence systems* supported by federal funds are subject to the 28 C.F.R. 23 guidelines (see 28 C.F.R. 23, § 23.33 (a)). However, to repeat, even if an agency maintains a system not supported by federal funds it is best to adopt the standards of 28 C.F.R. 23.

The term *criminal intelligence system* is defined in § 23.3 (b)(1) very broadly. The practical impact is that, in the author's opinion, nearly all intelligence systems are covered (see also §§ 23.3 (b)(2); (b)(4) and (b)(5)). It is important to note that the key factor which triggers the concerns to which the 28 C.F. R. 23 provisions are directed is the "pooling" or "interjurisdictional" sharing of the information. The propriety of interjurisdictional systems which do not comply with 28 C.F.R. 23 is often raised. Subject to state or local laws and assuming no use of federal funding to support the system, 28 C.F.R. 23 does not apply. But, as suggested (supra, fn. 12) there are potential pitfalls

---

[12]The author is aware that many agencies maintain "in house" intelligence systems that are not subject to the 28 C.F.R. 23 requirements. However, these systems ought to comply for at least three reasons. *First*, 28 C.F.R. 23 is a proven system that protects privacy and supports legitimate law enforcement interests. *Second*, there is always going to be a temptation to disseminate information from an "in house" system when that information would assist another agency. For this reason an "in house" system should comply with 28 C.F.R. 23 so that dissemination can properly occur. *Third*, if the "in house" system does not comply with 28 C.F.R. 23 requirements there will be a temptation to simply move information that should be purged to the "in house" system rather than purge it.

in failing to use the 28 C.F.R. 23 guidelines.

Perhaps the most important aspect of 28 C.F.R. 23 is that it defines what constitutes "criminal intelligence information" and sets parameters which relate to the "validation" of such information. The definition of "criminal intelligence information" is set out in 28 C.F.R. 23, § 23.3(b)(3):

> "*Criminal Intelligence Information* means data which has been evaluated to determine that, it:
>
> (i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and
> (ii) Meets criminal intelligence system submission criteria; . . ."

The submission criteria which apply are set out in 28 C.F.R. 23, § 23.20 (a), (b), (c), and (d). In summary, these criteria require that:

> (1) there is a *reasonable suspicion* an individual or organization is involved in criminal activity (§ 23.20 (a));
> (2) the information to be entered is relevant to the criminal activity (§ 23.20(a));
> (3) the information does not include information about political, religious or social views, associations, or activities except where such information relates directly to the *criminal predicate* which is the basis for focusing on the individual or group (28 C.F.R. 23, § 23.20 (b));
> (4) the information has not been obtained in violation of any "federal, state, or local law or ordinance." (28 C.F.R. 23, § 23.20 (d).);[13] and
> (5) the information establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator or employee *a basis to believe that an individual or organization is involved in a definable criminal activity or enterprise.* (28 C.F.R. 23, § 23.20 (c), emphasis added.)

To summarize, to put information into the system, there must be a *criminal predicate* to which the information relates. This criminal predicate must be based on a *reasonable suspicion.* A recent United States Supreme Court case, *United States v. Arvizu*, (2002) 534 U.S. 266, addressed the issue of what constitutes a reasonable suspicion. While the factual situation in *Arvizu* had to do with the

---

[13]It is important to note that it is the duty of an agency which is part of an interjurisdictional intelligence system (see 28 C.F.R. 23, § 23.3(b)) to screen the material it receives to determine whether it was properly obtained (28 C.F.R. 23, § 23.20(d.)).

propriety of a vehicle detention, the ruling should be applied to intelligence systems. In its ruling, the United States Supreme Court made several cogent findings:

First: it opined that the concept of what constituted "reasonable suspicion" was abstract and, therefore, depended on the facts of the particular situations rather than any rigid formulation; (at 274)

Second: the issue whether "reasonable suspicion" exists will depend on the totality of the circumstances of the particular situation, this means that each factor making up the basis for the action taken shall be considered in conjunction with all the other factors not in isolation; (at 273-274)

Third: the person making the assessment whether there is a reasonable suspicion may use his/her experience, specialized knowledge and training in making the assessment; (at 273-274) and

Fourth: "A determination that reasonable suspicion exists . . . need not rule out the possibility of innocent conduct." (at 277)

A related matter is the length of time such information may be considered valid and, therefore, may remain in the system (see 28 C.F.R. 23, § 23.3 (b)(6)). This matter is governed by the guidelines set out in 28 C.F.R. 23, § 23.20 (h) which provide that information must be evaluated for its "relevance and importance" and continuing compliance with the submission criteria. Such reviews must occur at least every five years and material which is not in compliance must be destroyed. Obviously, if information is found not to meet these criteria before the five-year period, it should be destroyed at once.

A question often arises regarding how to treat information which does not yet rise to the level of reasonable suspicion. In other words, can information be maintained and developed. Although 28 C.F.R. 23 does not specifically address this issue, there is general agreement that such information may be kept for up to one year for development. (See L.E.I.U. Guidelines, IV B and D.O.J. Guidelines pages 3-4.) It is important to emphasize that such information *should not be incorporated into the intelligence system.* It is also important to point out that such "developmental

information" obviously is not "intelligence information" which enjoys some of the exemption benefits which was discussed *infra.*

A question arises as to an individual who is the subject of an intelligence file and who is incarcerated for more than five years. Title 28 C.F.R. 23 does not address this issue. The position taken by those in the federal government who are responsible for interpreting 28 C.F.R. 23 (Office of Justice Planning) is that incarceration *does not* "toll" the five-year validation criteria. While this position is being reconsidered, the current rule is that validation must occur or the intelligence file must be destroyed.

The C.F.R. guidelines spell out the necessary safeguards which must be in place (see 28 C.F.R. 23, § 23.20 (g)-(n). Of some interest are the specific assurances required by 28 C.F.R. 23 §§ 23.20 (k) and (l). Subsection (k) requires that all surveillance of electronic communications must conform to the federal or state laws governing such surveillance. Subsection (l) requires that the activities related to the intelligence function neither harass nor interfere with "any lawful political activities."

Collection and dissemination are specifically addressed by 28 C.F.R. 23, §§ 23.20 (e-f) and 23.30.)

With respect to collection of information section 23.30 (b) provides:

> "The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:
>
> (1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and
>
> (2) Are not limited to one jurisdiction."

Also of considerable interest are the provisions (§§ 23.39 (c)-(d)) which reflect the policy that accountability for the intelligence system be at the very highest level of a participating agency.

Dissemination is only permitted when there is a need to know and a right to know (28 C.F.R. 23, § 23.20 (e)) and when the recipients of the information are ". . .law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and

dissemination which are consistent with these principles." (§ 23.20 (f)(1).)[14] The only exception to this policy would be a situation where dissemination is necessary to avoid imminent danger to life or property. (§23.20 (f)(2)).

Finally, the guidelines suggest that intelligence systems to which it is applied should be designed to support state and local law enforcement/prosecution efforts including task force efforts which include a federal agency. (see §§ 23.30(a) and (e).)

c.

The P.A.T.R.I.O.T Act

This legislation (House Resolution 3162) was passed following the September 11, 2001 attack. It did not address the gathering or maintenance of intelligence information, It did, however, address the dissemination of such information and, indirectly the collection (most changes were in the area of electronic surveillance).

Almost all of this act's provisions initially impact federal agency inter-relationships. There was very little of substance that immediately impacts state and local intelligence systems.

2.

California Laws

California does not have any provisions similar to 28 C.F.R. 23. As was stated in *Los Angeles Police Department v. Superior court, supra*:

> "[The California Public Records) Act itself does not undertake to prescribe what type of information a public agency may gather, nor to designate the type of records an agency may keep, nor to provide a method of correcting such records. Its sole purpose is to provide for disclosure." (at 668.)

---

[14] This is another, persuasive argument for the proposition that an agency's system comply with 28 C.F.R. 23.

However, it seems clear given the *White v. Davis, supra,* admonition that intelligence gathering must be tempered by federal and state constitutional restrictions that the 28 C.F.R. 23, § 23.2 balance between privacy and intelligence activities applies in California. Further, it seems clear that *White v. Davis,* imposed the "criminal predicate" requirement of 28 C.F.R. 23, § 23.20 (c) on California intelligence systems. Finally, most California law enforcement agencies have had their intelligence operations funded (at least in part) by federal grants or receive information from intelligence systems that must comply with 28 C.F.R. 23.

3.

Summary

All systems which contemplate participation in interjurisdictional intelligence sharing should comply with 28 C.F.R. 23.

B.

LAWS GOVERNING ACCESS TO INTELLIGENCE INFORMATION

1.

Federal Laws

a.

Freedom Of Information Act

This federal law (for text see Appendix 3) applies only to federal agencies. (See 5 U.S.C. 552(f)(1)[15] also defining agency, and 5 U.S.C. 552(a) imposing the public record duty on agencies).

---

[15]This F.O.I.A. definition cross refers to the definition of agency set out in 5 U.S.C. § 551(1) which provides: (1) "agency" means each authority of the Government of the United States, whether or not it is within or subject to review by another agency, but does not include–

(A) the Congress;

(B) the courts of the United States;

(C) the governments of the territories or possessions of the United States;

(D) the government of the District of Columbia;

(E) agencies composed of representatives of the parties or of representatives of organizations of the parties to the disputes determined by them;