McGeorge Law Review

Volume 34 | Issue 2 Article 9

1-1-2003

Crimes / Who's Listening - Changes in California's Wiretap Statute

Jeff R. Boone

Who's Listening? Changes in California's Wiretap Statute

Jeff R. Boone

Code Sections Affected

Penal Code §§ 629.53, 629.61 (new); 629.50, 629.51, 629.52, 629.54, 629.56, 629.58, 629.60, 629.62, 629.64, 629.68, 629.70, 629.72, 629.74, 629.76, 629.78, 629.80, 629.82, 629.86, 629.88, 629.89, 629.90, 629.94, 629.98 (amended).

AB 74 (Washington); 2002 STAT. Ch. 605.

I. INTRODUCTION

In June 2002, law enforcement agents arrested thirty-nine members of the Arellano Felix drug cartel as part of a two-year investigation called Operation Vise Grip.[1] The cartel is responsible for smuggling cocaine and heroin into the Los Angeles area and then distributing it throughout the United States.[2] In furtherance of its drug smuggling operation, law enforcement agencies estimate that the Arellano Felix cartel has paid out millions of dollars in bribes to public officials and is responsible for over one thousand killings.[3] With the use of four wiretaps, Operation Vise Grip seized almost $14 million in drugs and arrested over 230 suspects nationwide.[4]

Results like those achieved in Operation Vise Grip have convinced law enforcement agencies that electronic surveillance is an "essential tool" in the fight against crime.[5] Civil libertarians, on the other hand, believe that the value of the evidence gathered by electronic surveillance is insignificant when balanced against the intrusion on the right to privacy, not only of the suspect, but also the privacy of innocent third parties whose communications are intercepted.[6]

---

1. Marisa Taylor, et al., *Drug Cartel's State Network Disrupted 39 Arrested in Arellano Felix Crackdown*, SAN DIEGO UNION TRIB., June 14, 2002, at A1, *available at* 2002 WL 4608191.

2. *Id.*

3. *Id.*

4. *Id.*

5. Letter from John Lovell, Government Relations Manager, California Peace Officers' Association and California Police Chiefs' Association, to Carl Washington, Assemblymember (Jan. 11, 2002) [hereinafter Lovell Letter] (on file with the *McGeorge Law Review*).

6. *See* Telephone Interview with Francisco Lobaco, Legislative Director, ACLU (Sept. 11, 2002) [hereinafter Lobaco Interview] (notes on file with the *McGeorge Law Review*) (stating that the ACLU opposes the use of electronic surveillance because of its intrusion on an individual's right to privacy, the large number of communications of innocent bystanders that are inevitably intercepted, and the financial cost of conducting electronic surveillance).

Since September 11, 2001, laws and procedures relating to electronic surveillance have been reexamined in light of the increased terrorist threat.[7] The balance has tipped in favor of law enforcement.[8] There has been tremendous pressure to remove restrictions and streamline the procedures that law enforcement agencies follow when conducting electronic surveillance. In response to this pressure, the California Legislature enacted Chapter 605.[9] This statute extends the sunset provision on California's electronic surveillance statute, expands law enforcement's ability to use wiretaps to combat terrorism and other types of crime, and establishes stricter reporting requirements.[10]

II. LEGAL BACKGROUND

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) regulates the federal government's use of electronic surveillance.[11] Title III also provides the framework for states that wish to permit electronic surveillance.[12] Under Title III, a state is required to enact an enabling statute authorizing electronic surveillance.[13] California passed its enabling statute in 1988.[14] However, that statute contains a sunset provision that takes effect in January 2003.[15]

---

7. *See* Letter from Leroy D. Baca, Los Angeles County Sheriff, Chairman of the California Anti-Terrorism Information Center, to Carl Washington, Assemblymember (Nov. 6, 2001) [hereinafter Baca Letter] (on file with the *McGeorge Law Review*) (stating that Chapter 605 would provide law enforcement with a tool to protect citizens from criminals attempting to use agents such as Anthrax or other weapons of mass destruction); Letter from Scott Ciment, Legislative Advocate, California Attorneys for Criminal Justice, to Carl Washington, Assemblymember (Jan. 8, 2002) [hereinafter Ciment Letter] (on file with the *McGeorge Law Review*) (stating that California Attorneys for Criminal Justice appreciates the fact that the Assembly Committee on Public Safety is attempting "to balance civil liberties with law enforcement demands for increased wiretap authority" to combat potential terrorists threats).

8. *See* NAT'L CONF. OF ST. LEGISLATURES, PROTECTING DEMOCRACY AMERICA'S LEGISLATURES RESPOND: OVERVIEW OF STATE ACTIVITY IN RESPONSE TO SEPTEMBER 11, at 105 (Apr. 2002), *available at* http://www.ncsl.org (copy on file with the *McGeorge Law Review*) (stating that "[f]ollowing the tragedies of September 11, there is growing support to give law enforcement agencies more power to tap into private communications to thwart further acts of terrorism by monitoring private electronic communications.").

9. *See* SENATE RULES COMMITTEE, FLOOR ANALYSIS OF AB 74, at 6 (Aug. 22, 2002) (explaining that Chapter 605 is designed to allow law enforcement to meet the threat of possible terrorist acts).

10. *Id.* at 3-4, 6.

11. 18 U.S.C.A. § 2510 (West 2000 & Supp. 2002); *see* SENATE COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 7 (June 25, 2002) (discussing congressional authorization of wiretaps by Title III).

12. *See* ASSEMBLY COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 6 (Jan. 15, 2002) (stating that before wiretaps can be used by state law enforcement agencies, the state must enact an enabling statute that comports with the minimum protections established by Title III); *see also* 18 U.S.C.A. §2516(2) (West 2000) (establishing the procedures by which state law enforcement officers may request an intercept order).

13. *See* 18 U.S.C.A. § 2516(2) (discussing the requirement of a state enabling statute).

14. CAL. PENAL CODE § 629 (West 1999).

15. *Id.* § 629.98 (West 1999).

Existing California law authorizes "the Attorney General, Chief Deputy Attorney General, or Chief Assistant Attorney General, Criminal Law Division, or . . . a district attorney" to apply for an intercept order.[16] Authorities may intercept "wire, electronic digital pager, or electronic cellular telephone communications."[17] They must apply for an intercept order with the presiding superior court judge.[18] Intercept orders may only be authorized for specific enumerated crimes.[19] Presently, law enforcement agencies may request intercept orders only for specific violent crimes and felonies involving large amounts of certain illegal drugs.[20]

Existing law permits the issuing court to grant oral approval for an intercept order in emergency situations so long as a written application is submitted to the court within forty-eight hours.[21] Law enforcement agencies are also required to submit written reports every seventy-two hours to the issuing judge detailing the progress made toward achieving the objective of the intercept order.[22] Further, the California Attorney General is required to prepare an annual report containing specific data which is submitted to the Director of the Administrative Office of the United States Court, the Judicial Council, and the California Legislature.[23]

Prior to the enactment of Chapter 605, law enforcement agencies were required to provide defendants with transcripts of evidence resulting from an intercept order ten days prior to any court proceeding.[24] Also, standing to suppress evidence acquired by communication interception was quite broad. Anyone may move to suppress evidence on the basis that it was acquired contrary to the protection against unlawful search and seizure established by the Fourth Amendment of the United States Constitution.[25]

California law strictly regulates the use of information that law enforcement acquires through electronic surveillance. If investigators discover information about a crime that is not mentioned in the intercept order, several requirements must be met before that information can be used.[26] If the crime is one for which

16. *Id.* § 629.50 (West 1999).

17. *Id.* § 629.52 (West 1999 & Supp. 2002).

18. *Id.* § 629.50.

19. *Id.* § 629.52.

20. *See id.* (stating that an intercept order may be issued upon probable cause for various specified offenses).

21. *Id.* § 629.56 (West 1999).

22. *Id.* § 629.60 (West 1999).

23. *Id.* § 629.62 (West 1999).

24. *Id.* § 629.70 (West 1999).

25. *Id.* § 629.72 (West 1999).

26. CAL. PENAL CODE § 629.82 (West 1999); *see also* SENATE RULES COMMITTEE, FLOOR ANALYSIS OF AB 74, at 5 (Aug. 22, 2002) (explaining that if officers learn of information concerning a crime for which they lack an intercept order, the information cannot be used as evidence unless the officers can show that the information was "obtained through an independent source" or would have been discovered inevitably).

law enforcement could have requested an order,[27] the information may be used only upon a request to the court to use such information as soon as possible after the interception.[28] However, if investigators gather information concerning a crime for which an intercept order could not have been issued, the information cannot be used except to prevent a future criminal act.[29] The information may not be used as evidence in any proceeding unless investigators can show that either the information came from an independent source or that the officers would have discovered the information without electronic surveillance.[30]

III. REVISIONS MADE BY CHAPTER 605

A. Overview of Revisions

The California Legislature enacted Chapter 605 for several reasons. First, the enabling statute authorizing electronic surveillance in California contains a sunset provision that took effect on January 1, 2003, ending state and local law enforcement's authorization to conduct electronic surveillance.[31] Chapter 605 extends the term of the authorization to January 1, 2008.[32] Second, the Legislature is responding to the terrorist attacks of September 11th.[33] Specifically, the new law expands the list of enumerated crimes for which electronic surveillance is authorized to include crimes involving weapons of mass destruction.[34] Third, the act redefines certain key terms to clarify the law and close loopholes that existed in prior law.[35] Fourth, Chapter 605 expands the ways in which information gathered under an intercept order can be used.[36] Finally, the act streamlines both the procedures that law enforcement agencies must follow to obtain an intercept order and the surveillance reporting requirements.[37]

---

27. *See* CAL. PENAL CODE § 629.52 (West 1999 & Supp. 2002) (enumerating the crimes for which an intercept order may be authorized).

28. *Id.* § 629.82(a) (West 1999).

29. *Id.* § 629.82(b).

30. *Id.*

31. *See* CAL. PENAL CODE § 629.98 (West 1999) (stating that the law is in effect until January 1, 2003).

32. *Id.* § 629.98 (amended by Chapter 605).

33. *See* SENATE COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 6 (June 25, 2002) (stating that current laws need to be revamped because of the terrorist threat).

34. CAL. PENAL CODE § 629.52(a) (amended by Chapter 605).

35. *Id.* § 629.51 (amended by Chapter 605); *see also* SENATE COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 2-3 (June 25, 2002) (stating that Chapter 605 defines the terms wire communication, electronic pager communication, electronic cellular communication, and aural transfer, and adding that communications from "any electronic pager" may be intercepted).

36. CAL. PENAL CODE §§ 629.74, 629.76, 629.78, 629.82 (amended by Chapter 605); *see also infra* Part III.B (describing how Chapter 605 allows greater use of information gathered under an intercept order).

37. CAL. PENAL CODE §§ 629.56, 629.58, 629.62 (amended by Chapter 605); *id.* § 629.61 (enacted by Chapter 605); *see also infra* Part III.C (discussing the ways in which Chapter 605 streamlines existing procedures).

B. Expansion of California's Electronic Surveillance Law

Chapter 605 extends the sunset or termination date of the State's wiretap provisions until January 1, 2008.[38] The new law broadens the list of crimes for which intercept orders can be issued.[39] Under Chapter 605, law enforcement can request an intercept order for offenses involving the use of "weapons of mass destruction."[40]

Chapter 605 allows the appointment of an individual who can request intercept orders in the district attorney's absence.[41] Also, Chapter 605 allows judges, other than the presiding superior court judge, to issue intercept orders.[42] Judges on an established list may issue intercept orders if the presiding judge is unavailable.[43]

Chapter 605 expands the type of communications that may be intercepted to include tone and digital electronic pagers.[44] It also redefines "wire communication"[45] and "aural transfer."[46] The new definitions are closely aligned with the definitions contained in Title III.[47]

The new law allows officers to use information regarding any violent felony that is overheard.[48] Prior to Chapter 605, if an officer conducting electronic surveillance gathered information on a crime that was not specified in the intercept order, that information could be used only if the crime was listed in section 629.52 of the California Penal Code.[49] Chapter 605 continues to allow intercept orders for crimes listed in section 629.52, but expands the scope of the law by authorizing intercept orders for crimes listed in section 667.5(c),[50] which defines "violent felonies."[51]

---

38. CAL. PENAL CODE § 629.98 (amended by Chapter 605).

39. *See id.* § 629.52 (amended by Chapter 605) (enumerating the crimes for which a wiretap may be authorized).

40. *Id.* § 629.52(a)(4) (amended by Chapter 605).

41. *Id.* § 629.50 (amended by Chapter 605).

42. *Id.*

43. *Id.*

44. *See id.* § 629.51 (amended by Chapter 605) (defining "electronic pager communication" as "any tone or digital display or tone and voice pager communication").

45. *See id.* (defining "wire communication" as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of a like connection in a switching station), furnished or operated by any person engaged in providing or operating these facilities for the transmission of communications, and the term includes any electronic storage of these communications).

46. *See id.* (defining "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception").

47. *See* 18 U.S.C.A. § 2510 (West Supp. 2002) (defining "wire communication").

48. CAL. PENAL CODE § 629.82 (amended by Chapter 605).

49. *Id.* § 629.82 (West 1999).

50. *See id.* § 667.5(c) (West Supp. 2002) (denoting "violent felonies" as murder, voluntary manslaughter, mayhem, rape, sodomy by force, oral copulation by force, lewd acts on a child, any state felony punishable by a life sentence or death, any felony that inflicts great bodily injury, any felony where the defendant uses a firearm,

C. Streamlining the Procedures for Electronic Surveillance

Chapter 605 allows an order to be modified if "there is probable cause to believe that the person identified in the original order . . . changed the facility or device that is subject to the original order."[52] The modified order is restricted in duration to the time period authorized in the original order.[53] Also, the modified order must meet all requirements established under existing law and Chapter 605.[54]

The new law modifies the reporting requirements of an intercept order.[55] Rather than the seventy-two-hour requirement, a written report must be submitted every six days to the judge that authorized the order.[56] The report must detail the progress made towards meeting the objective of the wiretap, and it must contain the number of communications intercepted pursuant to the order.[57]

Chapter 605 modifies the information that must be included in the Attorney General's annual report to the Legislature on interceptions conducted under the wiretap provisions.[58] Chapter 605 requires that in addition to the data required under existing law, the following data must be included in the report: "[t]he number of wire, electronic pager, and electronic cellular telephone devices that are the subject to each order granted";[59] "the number of orders . . . applied for";[60] whether the subject of the order was notified;[61] and the number of other individuals notified.[62]

Chapter 605 also expands notification requirements.[63] It states that all defendants must be notified that they were "identified" as the result of an interception.[64] Chapter 605 also requires that notification be given before the defendants enter a plea of nolo contendere or guilty, or at least ten days before

---

robbery, arson, any offense accomplished against the victim by force or threat of force, attempted murder, kidnapping, certain categories of assault, continuous sexual abuse of a child, carjacking, extortion, certain categories of threats against witnesses and victims, and first-degree burglary).

51. *Id.* § 629.82 (amended by Chapter 605).

52. SENATE RULES COMMITTEE, FLOOR ANALYSIS OF AB 74, at 2 (Aug. 22, 2002); CAL. PENAL CODE § 629.50 (amended by Chapter 605)

53. *Id.*

54. *Id.*

55. *Id.* § 629.60 (amended by Chapter 605).

56. *Id.*

57. *Id.*

58. *Id.* § 629.62(a) (amended by Chapter 605).

59. *Id.* § 629.62(b)(4) (amended by Chapter 605).

60. *Id.* § 629.62(b)(1) (amended by Chapter 605).

61. *Id.* § 629.62(b)(15) (amended by Chapter 605).

62. *Id.*

63. *Id.* § 629.70 (amended by Chapter 605).

64. *Id.*; *see also* Ruffin Prevost, *The "Handoff": Wiretaps? The LAPD Don't Need No Stinking Warrant!*, *at* http://www.parascope.com/mx/articles/handoff.htm (last visited Sept. 30, 2002) (copy on file with the *McGeorge Law Review*) (describing the abuse of, among other things, notification procedures by the Los Angeles Police Department).

arraignment.[65] Finally, the new law specifies that the defendant must be given a copy of all of the interceptions, including a copy of the authorizing court order and monitoring logs.[66]

IV. ANALYSIS OF CHAPTER 605

A. *In Support of Chapter 605*

Electronic surveillance has been called an "essential tool" for law enforcement.[67] When traditional enforcement techniques are either ineffective or too dangerous, electronic surveillance permits officers to gather the information and evidence they need to solve crimes.[68] By broadening the type of crimes for which electronic surveillance is authorized,[69] permitting greater use of evidence gathered by electronic surveillance,[70] and streamlining the procedures[71] and reporting requirements that law enforcement must follow to conduct electronic surveillance,[72] Chapter 605 increases the utility of an already effective tool.

While the new law generally increases the ability of law enforcement agencies to conduct electronic surveillance in California, it also increases the protection afforded to third parties and defendants.[73] For example, Chapter 605 requires not only that a third party or defendant be notified that he is the subject of electronic surveillance, but also that a record of the notification be included in the Attorney General's annual report.[74] Chapter 605 further requires that the Attorney General's annual report include the actual number of devices[75] subject to each interception order.[76] These two changes, along with changes made in

---

65. *Compare* CAL. PENAL CODE § 629.70(a) (amended by Chapter 605), *with* CAL. PENAL CODE § 629.70 (West 1999) (lacking the requirement that the defendant be informed that he was identified as a result of a wiretap, and also lacking the requirement that notification occur before the defendant plead guilty or nolo contendere).

66. *Compare* CAL. PENAL CODE § 629.70 (amended by Chapter 605), *with* CAL. PENAL CODE § 629.70 (requiring that transcripts, not a copy of the recording, be provided to the defendant).

67. Lovell Letter, *supra* note 5.

68. *See* CAL. PENAL CODE §629.50(d) (West 1999) (explaining that before an intercept order will be authorized investigators must state "that conventional investigative techniques had been tried and were unsuccessful, or why they reasonably appear to be unlikely to succeed or to be too dangerous").

69. *Id.* § 629.52 (amended by Chapter 605).

70. *See id.* § 629.82 (amended by Chapter 605) (defining the circumstances under which information concerning a violent felony that is overheard during electronic surveillance may be used as evidence).

71. *See id.* §§ 629.56, 629.58, 629.61, 629.62 (amended by Chapter 605).

72. *See id.* § 629.60 (amended by Chapter 605) (explaining the changes to the reporting requirements).

73. *See* SENATE RULES COMMITTEE, FLOOR ANALYSIS OF AB 74, at 6 (Aug. 22, 2002) (stating that the author of AB 74 does not intend "to weaken the protections in California law by making our wiretapping law the same as federal law.").

74. CAL. PENAL CODE §§ 629.62(b), 629.68 (amended by Chapter 605).

75. *See id.* § 629.62(b)(4) (amended by Chapter 605) (requiring the number of devices to be listed to include wire, electronic pager, and electronic cellular telephone devices).

76. *Id.*

disclosure requirements, are significant. Civil libertarians and the defense bar advocated strongly for these revisions to help prevent abuses like the "Handoff" Scandal in Los Angeles.[77]

The "Handoff" is a technique that was used by the Los Angeles Police Department (LAPD) to share information gathered by electronic surveillance with others in the department.[78] For example, if the LAPD had authorization to conduct a wiretap on a defendant and while conducting surveillance the investigators gained information concerning a crime involving a third party, that information would be "handed off" to other officers to investigate.[79] The officers investigating the third party would use the information given to them as proof of probable cause.[80] After establishing probable cause, the investigators would request authorization for an intercept order for the third party without informing the judge how they had obtained the information.[81] If the crime is one for which an intercept order is not authorized, the officers could place the third party under surveillance under conventional techniques.[82]

The "Handoff" allowed the LAPD to use information gathered by electronic surveillance to circumvent protections contained in California's wiretap law and investigate third parties or crimes for which electronic surveillance was not and could not be authorized.[83] The revisions made by Chapter 605 help ensure that individuals are informed when they have been subjected to electronic surveillance; this is accomplished by mandating stricter notification requirements[84] and increasing the Attorney General's oversight of notification.[85]

Supporters of Chapter 605 argue that given the threat posed by terrorism, it is reasonable to expand law enforcement's ability to conduct electronic surveillance.[86] By increasing the scope of California's electronic surveillance law to include crimes involving weapons of mass destruction, law enforcement is able to provide increased protection.[87]

---

77. Prevost, *supra* note 64; Lobaco Interview, *supra* note 6.

78. Prevost, *supra* note 64.

79. *Id.*

80. *Id.*; Lobaco Interview, *supra* note 6.

81. Prevost, *supra* note 64.

82. *See* Lobaco Interview, *supra* note 6 (giving an example of the use of the "Handoff").

83. *See* CAL. PENAL CODE § 629.82 (West 1999) (explaining when officers may use information gathered on third parties).

84. *See id.* § 629.70 (amended by Chapter 605) (describing the stricter notification requirements).

85. *See id.* § 629.62 (amended by Chapter 605) (requiring that the Attorney General's annual report specify whether the subject of the intercept had been notified).

86. *See* Baca Letter, *supra* note 7 (stating that the recent terrorist attacks and the bio-terrorist attacks demonstrated that the nation is vulnerable).

87. *See id.* (explaining that AB 74 will help reduce the vulnerability by providing law enforcement with "the necessary means in the area of electronic surveillance").

Although Chapter 605 expands the scope of electronic surveillance, it was carefully constructed so as not to violate the rights of Californians.[88] California's electronic surveillance statutes continue to place greater restrictions on law enforcement agencies than the federal statutes place on federal law enforcement.[89]

Chapter 605 allows for the modification of an existing order.[90] If the target of an intercept order is taking actions to avoid electronic surveillance, by changing phones or making calls from different locations, investigators may modify the existing order to counter the targeted individual's evasive actions.[91] The American Civil Liberties Union (ACLU) disputes whether the modification of an existing order is allowed under federal law.[92] However, the modified order is subject to the same requirements and restrictions of the initial order.[93] Thus, if the original order did not violate an individual's Constitutional rights, the modification should not violate the individual's Constitutional rights.

B. Opposition to Chapter 605

Opponents of Chapter 605 dispute law enforcement's claim that expanded authority to conduct electronic surveillance is needed to protect society from terrorist threats.[94] Detractors contend that federal law enforcement agencies already have the authority to conduct the type of electronic surveillance authorized in Chapter 605, and it is the federal agencies that are likely to investigate crimes involving terrorist threats.[95]

The ACLU opposes wiretaps on the ground that wiretaps violate the right to privacy, specifically the Fourth Amendment's requirement that warrants particularly describe "the place to be searched and the persons or things to be seized."[96] Wiretaps permit the interception of communications of not only the defendant but also of innocent third parties.[97] According to the ACLU, this is the type of

88. *See* SENATE COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 9 (June 25, 2002) (stating that despite the ACLU's opinion to the contrary the author of AB 74 believes that the bill does not violate the federal law because the requirements for modification of an intercept order are the same as the requirements for an original order).

89. *See* SENATE RULES COMMITTEE, FLOOR ANALYSIS OF AB 74, at 6 (Aug. 22, 2002) (explaining that California law grants greater protection to privacy rights than federal law).

90. *Id.* at 2.

91. *See id.* (stating that an order may be modified if the targeted individual "changed the facility or device that is subject to the order").

92. SENATE COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 9 (June 25, 2002).

93. *See id.* (stating that both the sponsor and the author believe that allowing modifications of orders is constitutional because the modified order must meet the same requirements as the original order).

94. *See* Dan Morain, *Davis to Ask for Broader Wiretaps*, L.A. TIMES, Jan. 8, 2002 (stating that while the expanded wiretap authority "is pegged to the threat of terrorism," it could be used in "any criminal investigation").

95. *Id.*

96. *See* U.S. CONST. amend. IV (prohibiting general searches).

97. Letter from Francisco Lobaco, Legislative Director, American Civil Liberties Union, to Carl Washington, Assemblymember (Jan. 9, 2002) [hereinafter Lobaco Letter] (on file with the *McGeorge Law Review*).

general search prohibited by the Fourth Amendment.[98] The ACLU opposes wiretaps in general, and it also opposes legislation that allows law enforcement to take shortcuts in the application for intercept orders because such shortcuts increase the likelihood that privacy protections could be circumvented.[99] Thus, the ACLU opposes the modification provision in Chapter 605.[100]

Finally, civil liberties organizations oppose wiretaps because of the extensive degree of invasiveness.[101] A wiretap not only records conversations concerning the criminal activity of the defendant but also those concerning the activity of a large number of innocent third parties.[102] In fact, it is estimated that of all the calls intercepted by federal wiretaps, only about twenty percent are actually related to criminal activity.[103]

V. CONCLUSION

Not surprisingly, state law enforcement agencies welcome the changes made by Chapter 605[104] and civil libertarians oppose them.[105] Law enforcement views electronic surveillance as a valuable tool in its fight against crime and terrorism.[106] In light of the recent terrorist attacks, many people inside and outside the law enforcement community are questioning whether too many restrictions have been placed on the very agencies that are charged with protecting our society from terrorism.[107]

The ACLU disagrees. Even before September 11th, the ACLU believed that advances in technology and law enforcement's expanded authorization to conduct electronic surveillance posed a serious threat to an individual's right to privacy.[108] The ACLU is concerned that in a rush to make America safe from terrorism, legislators have gone too far by sacrificing personal freedoms unnecessarily.[109]

---

98. *See id.* (stating that because a wiretap "picks up both sides of all conversations of all calls" it "by definition constitutes a general search").

99. *See* Lobaco Interview, *supra* note 6 (explaining that the ACLU is opposed to any expansion of wiretap authority).

100. SENATE COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 74, at 8-9 (June 25, 2002).

101. *See* Lobaco Letter, *supra* note 97 (stating that in the year 2000, in California, law enforcement agencies intercepted in excess of 100,000 innocent conversations).

102. *Id.*

103. Prevost, *supra* note 64.

104. *See supra* Part IV.A (explaining law enforcement's support of Chapter 605).

105. *See supra* Part IV.B (discussing the reasons civil libertarians oppose Chapter 605).

106. Lovell Letter, *supra* note 5.

107. *See* Jessica Reaves, *Antiterrorism Bill Becomes Law*, TIME, Oct. 26, 2001, *available at* http://www.time.com/time/nation/article/0,8599,181437,00.html (copy on file with the *McGeorge Law Review*) (describing the swift and nearly unanimous passage of the "anti-terrorism bill" which grants law enforcement agencies "broad new powers" in the fight against terrorism).

108. *See* American Civil Liberties Union, *Privacy*, *at* http://www.aclu.org/Privacy/Privacylist.cfm (last visited Oct. 30, 2002) (copy on file with the *McGeorge Law Review*) (containing past ACLU articles expressing opposition to government surveillance).

109. *Id.*

Any bill relating to electronic surveillance is likely to be contentious because of the tension that exists between the individual's right to privacy and society's need to control crime. Although Chapter 605 extends the scope of California's wiretap statute,[110] it also provides important protections to third parties and defendants.[111] Also, it should be noted that even though the new law extends the scope of the wiretap statute, California's wiretap law is still more restrictive than federal law.[112]

110. *Supra* Part III.

111. *Id.*

112. *See* SENATE RULES COMMITTEE, FLOOR ANALYSIS OF AB 74, at 6 (Aug. 22, 2002) (explaining that California law grants greater protection to privacy rights than federal law).