Memorandum 2016-15

Government Interruption of Communication Service (Discussion of Issues)

In 2013, the Legislature enacted Senate Concurrent Resolution 54 (Padilla), which directs the Commission[1] to study two related topics involving government action that affects private communications.

This study addresses the second topic that was assigned by SCR 54, "state and local agency action to interrupt communication service."[2]

Because the legal and policy issues presented by that topic vary with the circumstances in which the government acts, the analysis in this study has been organized around the different scenarios in which such action might arise.

Prior memoranda discussed three distinctly different scenarios where government might interrupt communications in order to protect public health, safety, and welfare:

- Interruption of a specific communication service that is being used to violate the law (e.g., a telephone being used for illegal gambling).[3]
- Interruption of area communications to protect the public from a destructive act (e.g., use of a cell phone to trigger a bomb).[4]
- Interruption of area communications to protect the public from a dangerous public assembly (e.g., cell phones being used to incite and coordinate a riot).[5]

This memorandum discusses the last of the four scenarios that the Commission planned on examining — the interruption of communications of

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

2. Minutes (June 2015), p. 3.
3. Memorandum 2015-18.
4. Memorandum 2015-32.
5. Memorandum 2016-5.

persons subject to government control (e.g., the suppression of cell phone service in a state prison).[6]

In addition, this memorandum discusses the following miscellaneous issues, which have come up over the course of the study:

- Interruption of communications for emergency broadcasting purposes.
- Blocking specific channels of Internet communication to protect against malware and other threats to network operation and security.
- Gang injunctions.

CORRECTIONAL FACILITIES

Government regulation of the speech of prisoners is significantly different from the scenarios discussed in prior memoranda. Government has very strong interests at stake when operating a prison, jail, or other correctional facility (e.g., the need to maintain security in a dangerous environment). Moreover, prisoners necessarily have restrictions on their freedoms as a consequence of incarceration. Consequently, courts have generally been deferential to correctional authorities when reviewing actions that restrict prisoner communications.

This part of the memorandum will first summarize the case law on prisoner free expression rights. The memorandum will then discuss existing law restricting wireless communications in prisons and the technology available to implement such restrictions. Finally, the staff will make recommendations on how the law should address the interruption of communication services in correctional facilities.

Free Expression Rights of Prisoners

In considering the constitutional free expression rights of prisoners, the Supreme Court has balanced two broad principles. First, the Court has held that the fact of imprisonment does not wholly extinguish prisoners' constitutional rights:

> Prison walls do not form a barrier separating prison inmates from the protections of the Constitution. Hence, for example, prisoners retain the constitutional right to petition the government for redress of grievances …; they are protected against invidious

6. See Memorandum 2015-18, pp. 5-6.

> racial discrimination …; and they enjoy the protections of due process….[7]

However, prison administration presents extremely difficult and important considerations, which often require restricting prisoner freedoms in ways that a court may be reluctant to second-guess:

> "[C]ourts are ill equipped to deal with the increasingly urgent problems of prison administration and reform." … As the *Martinez* Court acknowledged, "the problems of prisons in America are complex and intractable, and, more to the point, they are not readily susceptible of resolution by decree." … Running a prison is an inordinately difficult undertaking that requires expertise, planning, and the commitment of resources, all of which are peculiarly within the province of the legislative and executive branches of government. Prison administration is, moreover, a task that has been committed to the responsibility of those branches, and separation of powers concerns counsel a policy of judicial restraint.[8]

In light of those two competing considerations, the Court must "formulate a standard of review for prisoners' constitutional claims that is responsive both to the 'policy of judicial restraint regarding prisoner complaints and [to] the need to protect constitutional rights.'"[9]

Procunier v. Martinez

In striking a balance between the considerations discussed above, the court has adopted slightly different standards of review for different circumstances. In an early case, *Procunier v. Martinez*,[10] the court considered regulations authorizing the censorship of prisoners' outgoing mail. The Court adopted a fairly strict standard of review (commonly known as the *Martinez* standard):

> First, the regulation or practice in question must further an important or substantial governmental interest unrelated to the suppression of expression. Prison officials may not censor inmate correspondence simply to eliminate unflattering or unwelcome opinions or factually inaccurate statements. Rather, they must show that a regulation authorizing mail censorship furthers one or more of the substantial governmental interests of security, order, and rehabilitation. Second, the limitation of First Amendment freedoms must be no greater than is necessary or essential to the protection of

7. Turner v. Safley, 482 U.S. 78, 84 (1987) (citations omitted).
8. *Id.* at 84-85 (citations omitted).
9. *Id.* at 85.
10. 416 U.S. 396 (1974).

> the particular governmental interest involved. Thus a restriction on inmate correspondence that furthers an important or substantial interest of penal administration will nevertheless be invalid if its sweep is unnecessarily broad. This does not mean, of course, that prison administrators may be required to show with certainty that adverse consequences would flow from the failure to censor a particular letter. Some latitude in anticipating the probable consequences of allowing certain speech in a prison environment is essential to the proper discharge of an administrator's duty. But any regulation or practice that restricts inmate correspondence must be generally necessary to protect one or more of the legitimate governmental interests identified above.[11]

Turner v. Safley

Several years later, in *Turner v. Safley*,[12] the Court adopted a more deferential, reasonableness-based standard when reviewing censorship of letters between prisoners (commonly known as the *Turner* standard):

> [W]hen a prison regulation impinges on inmates' constitutional rights, the regulation is valid if it is reasonably related to legitimate penological interests. In our view, such a standard is necessary if "prison administrators…, and not the courts, [are] to make the difficult judgments concerning institutional operations." Subjecting the day-to-day judgments of prison officials to an inflexible strict scrutiny analysis would seriously hamper their ability to anticipate security problems and to adopt innovative solutions to the intractable problems of prison administration. The rule would also distort the decisionmaking process, for every administrative judgment would be subject to the possibility that some court somewhere would conclude that it had a less restrictive way of solving the problem at hand. Courts would become the primary arbiters of what constitutes the best solution to every administrative problem, thereby "unnecessarily perpetuat[ing] the involvement of the federal courts in affairs of prison administration"[13]

The Court went on to explain several factors that are involved in applying the new standard of review:

> First, there must be a "valid, rational connection" between the prison regulation and the legitimate governmental interest put forward to justify it. … Thus, a regulation cannot be sustained where the logical connection between the regulation and the asserted goal is so remote as to render the policy arbitrary or

11. *Id.* at 413-14.
12. 482 U.S. 78 (1987).
13. *Id.* at 89.

> irrational. Moreover, the governmental objective must be a legitimate and neutral one. We have found it important to inquire whether prison regulations restricting inmates' First Amendment rights operated in a neutral fashion, without regard to the content of the expression. …
>
> A second factor relevant in determining the reasonableness of a prison restriction … is whether there are alternative means of exercising the right that remain open to prison inmates. Where "other avenues" remain available for the exercise of the asserted right, … courts should be particularly conscious of the "measure of judicial deference owed to corrections officials . . . in gauging the validity of the regulation." …
>
> A third consideration is the impact accommodation of the asserted constitutional right will have on guards and other inmates, and on the allocation of prison resources generally. In the necessarily closed environment of the correctional institution, few changes will have no ramifications on the liberty of others or on the use of the prison's limited resources for preserving institutional order. When accommodation of an asserted right will have a significant "ripple effect" on fellow inmates or on prison staff, courts should be particularly deferential to the informed discretion of corrections officials. …
>
> Finally, the absence of ready alternatives is evidence of the reasonableness of a prison regulation. … By the same token, the existence of obvious, easy alternatives may be evidence that the regulation is not reasonable, but is an "exaggerated response" to prison concerns. This is not a "least restrictive alternative" test: prison officials do not have to set up and then shoot down every conceivable alternative method of accommodating the claimant's constitutional complaint. … But if an inmate claimant can point to an alternative that fully accommodates the prisoner's rights at *de minimis* cost to valid penological interests, a court may consider that as evidence that the regulation does not satisfy the reasonable relationship standard.[14]

In *Turner*, the Court explained the new standard of review by citing four prior cases in which the Court had not applied strict scrutiny when reviewing (and upholding) prison rules that limited prisoner expression and association rights:

- In *Pell v. Pecunier*,[15] the Court upheld a regulation prohibiting face-to-face media interviews with individual prisoners. In that case, the Court stated that judgments about prison security "are peculiarly within the province and professional expertise of corrections officials, and in the absence of substantial evidence in the record to indicate that the officials have exaggerated their

14. *Id.* at 89-91 (citations omitted).
15. 417 U.S. 817 (1974).

response to these considerations, courts should ordinarily defer to their expert judgment in such matters."[16] The Court also noted that there are other available means for prisoners to communicate with journalists.[17]

- In *Jones v. North Carolina Prisoners' Union*,[18] the Court upheld regulations that prohibited meetings of a prisoners union, solicitation of other prisoners to join the union, and incoming bulk mail discussing the union. The Court upheld the restriction on incoming mail as "reasonable" in the circumstances and explained that the "ban on inmate solicitation and group meetings … was rationally related to the reasonable, indeed to the central, objectives of prison administration."[19]
- In *Bell v. Wolfish*,[20] the Court upheld a rule restricting prisoner receipt of hardback books, because the rule was a "rational response" to a clear security problem.[21] Further, the Court found no evidence that the rule was an exaggerated response to the legitimate security concern.[22]
- Finally, in *Block v. Rutherford*,[23] the Court upheld a policy restricting "contact visits" with pre-trial detainees. Citing *Wolfish*, the Court stated that "[P]rison administrators [are to be] accorded wide-ranging deference in the adoption and execution of policies and practices that in their judgment are needed to preserve internal order and discipline and to maintain institutional security."[24]

In summary, the Court in *Turner* stated: "In none of these four 'prisoners' rights' cases did the Court apply a standard of heightened scrutiny, but instead inquired whether a prison regulation that burdens fundamental rights is 'reasonably related' to legitimate penological objectives, or whether it represents an 'exaggerated response' to those concerns."

Thornburgh v. Abbott

The application of the *Turner* standard of review was reaffirmed and clarified in *Thornburgh v. Abbott*.[25] In that case, the court considered a regulation authorizing prison officials to block prisoner receipt of publications based on

16. *Id.* at 827.
17. *Id.* at 824-25.
18. 433 U.S. 119 (1977).
19. *Id.* at 129-30.
20. 441 U.S. 520 (1979).
21. *Id.* at 550.
22. *Id.* at 551.
23. 468 U.S. 576 (1984).
24. *Id.* at 585 (citation omitted).
25. 490 U.S. 401 (1989).

their content. Under the rule, a publication could be excluded if the warden determined that its introduction would be "detrimental to the security, good order, or discipline of the institution or it might facilitate criminal activity."[26] The Court applied the *Turner* standard and upheld the constitutionality of the regulation.

The Court explained the rationale for the reasonableness-based standard articulated in *Turner*, as follows:

> The Court's decision to apply a reasonableness standard in these cases rather than *Martinez'* less deferential approach stemmed from its concern that language in *Martinez* might be too readily understood as establishing a standard of "strict" or "heightened" scrutiny, and that such a strict standard simply was not appropriate for consideration of regulations that are centrally concerned with the maintenance of order and security within prisons. … Specifically, the Court declined to apply the *Martinez* standard in "prisoners' rights" cases because, as was noted in *Turner, Martinez* could be (and had been) read to require a strict "least restrictive alternative" analysis, without sufficient sensitivity to the need for discretion in meeting legitimate prison needs.

The Court did not entirely overturn *Martinez,* but it did restrict its application to cases involving the regulation of *outgoing* prisoner mail, reasoning that "[t]he implications of outgoing correspondence for prison security are of a categorically lesser magnitude than the implications of incoming materials."[27]

The Court rejected a suggestion that the governing standard of review should depend on whether a prison regulation of prisoner speech also restricts the speech of non-prisoners (i.e., those outside the prison who wish to communicate with prisoners):

> We do not think it sufficient to focus, as respondents urge, on the identity of the individuals whose rights allegedly have been infringed. Although the Court took special note in *Procunier v. Martinez* … of the fact that the rights of nonprisoners were at issue, and stated a rule in *Turner v. Safley* … for circumstances in which "a prison regulation impinges on *inmates'* constitutional rights," … any attempt to forge separate standards for cases implicating the rights of outsiders is out of step with the intervening decisions in *Pell v. Procunier*…; *Jones v. North Carolina Prisoners' Labor Union*, Inc.…; and *Bell v. Wolfish*…. These three cases, on which the Court expressly relied in *Turner* when it announced the reasonableness

26. *Id.* at 404 (citations and footnote omitted).
27. *Id.* at 413.

> standard for "inmates' constitutional rights" cases, all involved regulations that affected rights of prisoners *and* outsiders.…[28]

The reasonableness-based *Turner* standard has since been applied by the Court to uphold restrictions on visitation[29] and a broad prohibition on the receipt of all newspapers and magazines by "a group of specially dangerous and recalcitrant inmates."[30]

Prisoner Telephone Use Generally

The staff has not found any United States Supreme Court case that considers the constitutionality of regulations that restrict prisoner use of telephones.[31] However, there are federal and state appellate decisions addressing that issue.

Those cases have considered several different types of restrictions on prisoner telephone use. These include limits on the frequency and duration of telephone calls, restrictions on the persons that a prisoner may call, a requirement that calls be monitored and recorded,[32] and the imposition of fees that may be prohibitive to some prisoners.

In general, the courts have applied the *Turner* standard when reviewing regulations that limit prisoner telephone use for security reasons and have upheld such regulations.[33] According to one article that analyzed the case law in this area, "[t]he *Turner* standard almost certainly is the correct standard to apply when prison regulations limit prisoner telephone use due to security concerns."[34]

For example, in *Pope v. Hightower*,[35] the Eleventh Circuit Court of Appeals upheld regulations limiting the times during which calls could be made and prohibiting prisoners from calling anyone who is not on the prisoner's approved

---

28. *Id.* at 410, n.9 (emphasis in original) (citations omitted).
29. Overton v. Bazzetta, 539 U.S. 126, 132-37 (2003).
30. Beard v. Banks, 548 U.S. 521, 524-25 (2006).
31. A recent law review article similarly found that there is no Supreme Court decision directly on point. See P. Shults, *Calling the Supreme Court: Prisoners' Constitutional Right to Telephone Use*, 92 B.U. L. Rev. 369, 379 (2012) ("The Court never has decided a case in which prisoners challenged infringements on their right to use the telephone.").
32. Federal appellate courts have held that the recording of prisoner phone calls (to persons other than counsel) does not violate the Fourth Amendment of the United States Constitution. Prisoners do not have a reasonable expectation of privacy with respect to their telephone calls. The policy of taping is justified by institutional security concerns. Prisoners impliedly consent to recording by placing calls despite notices warning that calls will be recorded. See, e.g., United States v. Van Poyck, 77 F.3d 285 (9th Cir. 1996).
33. *Id.* at 392 ("Courts generally review prison policies that limit prisoners' telephone use under the *Turner* standard.")
34. *Id.* at 393.
35. See, e.g., Pope v. Hightower, 101 F.3d 1382 (11th Cir. 1996).

list of 10 persons. The court explained that reducing criminal activity and harassment qualifies as a legitimate governmental objective. According to the court, the "connection between that objective and the use of a ten-person calling list is valid and rational because it is not so remote as to render the prison telephone policy arbitrary or irrational."[36] The court also found that there were alternative means of communicating with those outside the prison (mail and visitation), that invalidating the prison's rules would have a significant negative effect on administration, and that the rules were not an "exaggerated response" to the prison's concerns.[37]

In California, Penal Code Section 2600 provides that a prisoner may, during their time of confinement, "be deprived of such rights, and only such rights, as is reasonably related to legitimate penological interests." This appears to be a rough approximation of the *Turner* standard, discussed above.

California regulations place a number of restrictions on prisoner telephone use (e.g., limits on frequency and duration; access based on prisoner privilege level; prohibitions on calls to inmates at other facilities, victims, and peace officers; monitoring and recording).[38] The staff has not found any case challenging the constitutionality of California's regulations on prisoner use of telephones.

Wireless Communications

In addition to the restriction of prisoner use of landline telephones, it is also very common for correctional systems to *prohibit* prisoner possession and use of wireless communication devices. This is the rule in California and in federal prisons and it appears to be very common if not universal in state prisons (the staff has not checked to confirm that all states impose such a prohibition).

Existing Restrictions

As noted above, prisoners in California are prohibited from possessing cell phones and other wireless communication devices. Such devices are classified as "dangerous" contraband.[39] Possession of an unauthorized wireless communication device in a local correctional facility is a misdemeanor.[40]

36. *Id.* at 1385.
37. *Id.*
38. 15 Cal. Code Regs. § 3282.
39. 15 Cal. Code Regs. § 3006.
40. Penal Code § 4575(a).

Possession of a wireless communication device with intent to deliver it to a prisoner is also a misdemeanor.[41]

In 2009, the Office of the Inspector General issued a report on the problems associated with prisoner cell phone use in California. The report was largely focused on the problem of keeping contraband cell phones out of the hands of prisoners, but it also offered an explanation of the kinds of problems posed by prisoner cell phone use:

> According to numerous Department [of Corrections] officials, the possession of cell phones and electronic communication devices by California's inmates is one of the most significant problems facing the Department today. Cell phones provide inmates with the ability to communicate amongst themselves and their criminal associates outside of prison to coordinate criminal activity. OIG and Department staff believe that if inmate cell phone usage continues to escalate, activities such as the intimidation of victims and witnesses, assaults, narcotics trafficking, and hostage taking could proliferate throughout the state. In addition, simultaneous disruptive activities, such as escapes and riots could occur. For example, Department staff often referred to a 2006 Sao Paolo, Brazil riot where an inmate with a cell phone orchestrated a multi-prison and city riot that resulted in a four-day crime spree. The rioting occurred simultaneously in ten different prisons and on the streets of various cities over a span of three different states. Approximately 39 law enforcement officials and 41 civilians were killed.
>
> …
>
> Today's wireless technology allows inmates to communicate clandestinely with one another, whether they are assigned to the same prison or in other facilities across the state. Inmates also use cell phones to effortlessly make tobacco, drug, and other contraband transactions, which create additional serious problems for the Department. A Department executive stated that inmates are communicating with one another in real time by calling or sending text messages providing information about correctional officers' movements and uploading pictures of secured areas within the prison. This type of information could be used to facilitate escapes, coordinate riots, and order assaults on staff and other inmates.
>
> For example, one inmate told correctional staff he regularly used a cell phone to conduct inquiries on inmates recently admitted to his housing unit. Subsequently, he targeted those individuals for assault if they were members of a rival gang or if they were members of his gang not in good standing.

41. Penal Code § 4576(a).

> On another occasion, inmates used cell phones to plan their escape from a southern California prison. The escaping inmates used a cell phone to arrange to be picked up off prison grounds. They also received a text message from a fellow inmate inside the prison advising them that correctional officers were conducting an emergency count because of their escape. The inmates were subsequently apprehended and returned to custody, where they informed the correctional staff that their cell phones played an integral role in coordinating their escape.
>
> …
>
> The Department is also concerned that inmates are uploading pictures of correctional staff and sharing them with outside criminal associates, jeopardizing the safety of correctional officers and their families.
>
> …
>
> Inmates with technologically advanced cell phones, such as iPhones and Blackberries, are constructing web pages and communicating with individuals on heavily trafficked web sites …. Inmates are posting pictures of themselves and their fellow gang members on their web pages created while incarcerated and are soliciting members of the general public to communicate with them. To an untrained person, it may not be immediately obvious that the individual depicted is a California prison inmate. Therefore, inmates may take advantage of minors and other vulnerable individuals by soliciting items such as photographs, money, or personal information.[42]

Similar concerns have been expressed by the United States Department of Justice:

> A widespread technology that allows people to connect with anyone, anywhere, has created concerns for corrections officials. The use of inexpensive, disposable cell phones has changed the age-old cat-and-mouse game of controlling whom inmates communicate with in the outside world and is creating serious problems for public safety officials.
>
> In the 1990s, cellular phones were larger and heavier and had audio capabilities only. Today they are lightweight, can be thinner than a matchbook, and can send both audio and data, including written messages and streaming video. Although these advances are welcome in society in general, they have had a negative impact on the law enforcement community, as criminals have taken advantage of cellular technology to conduct illegal activities.
>
> …
>
> The issue of cellular phone use by criminals, especially prison and jail inmates, gained national attention when a death row

42. Office of the Inspector General, State of California, *Inmate Cell Phone Use Endangers Prison Security and Public Safety* (2009).

> inmate used a cell phone to threaten a Texas senator. In Nevada, prison officials fired a dental assistant for helping an inmate get a cell phone to plan a successful escape. In New York, an inmate used a cell phone to orchestrate an attempted escape while on a medical transfer. In Tennessee, prison officials banned jars of peanut butter after learning that an inmate accused in the shooting death of a guard had used a jar to hide the cell phone he used to coordinate his escape. Prisoners have also used cell phones to harass and threaten their victims.[43]

The Federal Communications Commission has expressed similar concerns.[44]

In 2010, Congress passed the "Cell Phone Contraband Act of 2010," which prohibits prisoner cell phone possession in federal prisons.[45]

Constitutionality of Prohibition on Wireless Communication

The staff has not found any appellate case discussing whether prisoners have a constitutional right to possess and use wireless communication devicess. This is not surprising, as it seems very likely that such restrictions would survive scrutiny under the First Amendment.[46]

One justification for prohibiting prisoner user of wireless communications is that such restrictions are necessary in order to implement the existing restrictions on landline telephone use. If prisoners were permitted to possess wireless communication devices, they could easily circumvent the limitations on telephone use that are part of the system of privileges and penalties imposed to encourage good conduct. More importantly, access to wireless communications would enable prisoners to avoid the monitoring and recording of prisoner conversations, giving prisoners greater scope for misuse of telephones. For example, prisoners could make surreptitious calls to organize an escape attempt, intimidate witnesses, harass victims, arrange contraband smuggling, etc. A ban on wireless communications seems necessary in order to give prison officials control over such matters. Such control has been repeatedly held to be constitutional.

---

43. U.S. Dep't of Justice, Cell Phones Behind Bars (2009) *available at* <https://www.ncjrs.gov/pdffiles1/nij/227539.pdf>.

44. Federal Comm. Comm'n, *In re* Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, 28 FCC Rcd 6603, 6606-07 (2013).

45. See Pub. L. 111-225; 18 U.S.C. § 1791(d)(1)(F).

46. The staff did find one California case in which a court upheld a probation condition that prohibited possession and use of a cell phone. See *In re Victor L.*, 182 Cal. App. 4th 902, 921 (2010) ("A restriction on the mode of communication is viewed more tolerantly than a restriction on content. … [H]e remains free to exercise his constitutional right of expression but must simply employ less sophisticated means, such as a landline phone, the mail, or in-person contact.").

In addition to all of the legitimate concerns that justify the existing restrictions of landline telephone use, wireless devices create special problems of the types described by the Office of the Inspector General and the U.S. Department of Justice. Wireless communications can be used to monitor the movements of guards and other prisoners and share that information in real time; to research security devices and systems; and to procure, coordinate, or commit new crimes. That last point is a particular concern for prisoners who are part of a larger criminal organization or whose crimes involved electronic communications (e.g., electronic mail fraud or child pornography).

Under the *Turner* standard of review, these additional concerns would seem more than sufficient to justify a prohibition on the possession and use of wireless communication devices:

- Those concerns clearly represent legitimate penological interests. A prohibition on wireless communications seems reasonably related to those interests and does not appear to be an exaggerated response to the concerns.
- Other alternative means of communication remain open to prisoners. Most importantly, prisoners could continue to use landline telephones under regulated conditions.
- Allowing wireless communications would have significant "ripple effects," inviting all of the serious security problems discussed above and imposing significant costs and risks on prison staff, other prisoners, and the public outside the prison's walls.
- There is no obvious practicable alternative to prohibition.

Interrupting Wireless Communication Service

A simple prohibition on the possession and use of wireless communication devices within correctional facilities does not fall within the scope of this study, because it does not involve a third party service provider. Recall that the resolution assigning this study directed the Commission to do the following:

> Clarify the process communications service providers are required to follow in response to requests from state and local agencies … to take action that would affect a customer's service, with a specific description of whether a subpoena, warrant, court order, or other process or documentation is required…[47]

47. 2013 Cal. Stat. res. ch. 115.

However, this study would encompass action by correctional officers to block cell phone service within the area of a correctional facility, *if a communication service provider is involved.*

It is easy to imagine a situation in which officials might request that a service provider block wireless communications in a correctional facility, in response to an emergency. For example, if prisoners are using wireless communications to coordinate rioting, interruption of communications would seem to be a reasonable response. Under the analysis discussed in Memorandum 2016-5, a short-term action of that type would likely be constitutional (if properly limited and authorized).

However, as discussed above, correctional officers may need to do more than temporarily interrupt communications during an emergency. Officials may wish to *permanently* block wireless communication services within the confines of a correctional facility. Such action would likely be the best way to implement a ban on wireless communications, given the serious problems that prisons are having keeping cell phones from being smuggled into prisons.[48]

Officials are actively investigating technological means by which wireless communication services could be blocked in prisons. Those technological alternatives are discussed below.

Radio Signal Jamming

For several years, policy makers have been debating whether prisons should be permitted to use "radio signal jamming" technology to shut down wireless communications within prisons. "A radio signal jamming device transmits on the same radio frequencies as wireless devices and base stations, disrupting the communication link between the device and the network base station, and rendering any wireless device operating on those frequencies unusable."[49] The chief disadvantage of jamming is that it is indiscriminate. In addition to blocking use of contraband communication devices, jamming also blocks the authorized use of wireless communications by correctional officers and others.[50] This could create an additional threat to security and public safety, by impeding communications between law enforcement personnel and emergency

48. The Office of the Inspector General reported that the number of contraband cell phones seized in California prisons increased from 261 in 2006 to 2,811 in 2008. See Office of the Inspector General, *supra* note 42, at 1.

49. Federal Comm. Comm'n, *supra* note 44, at 6614.

50. *Id.*

responders. Furthermore, the area affected by jamming may reach beyond the confines of the correctional facility, suppressing the legitimate wireless communications of those who live or do business nearby.

Moreover, jamming is currently prohibited by federal law.[51] Efforts have been made in Congress to create a waiver system for jamming in prisons, but those efforts have not yet been successful. That lack of success is probably the result of concern about the negative consequences of jamming, discussed above, combined with the promising possibility that other methods could be used to block prisoner wireless communications without the same bad side-effects.

Those less disruptive alternatives were discussed in a 2010 report issued by the National Telecommunications and Information Administration.[52] More recently, and closer to home, the California Council on Science and Technology (CCST) released a report on technological methods of controlling wireless communications in California correctional facilities.[53] The CCST report was prepared pursuant to a formal request from Senators Elaine Alquist, Loni Hancock, Christine Kehoe, and Alex Padilla. That request posed a number of detailed questions, but it largely boiled down to "how best to prevent calls from being completed without impairing the ability of prison authorities to make and receive official business cell phone calls?"[54] The alternative methods identified in those reports are discussed below.

Cell Phone Detection

One option is to use a radio signal detection device to identify an active wireless communication signal, use triangulation to roughly identify the source of the signal, and then physically search that area to locate and seize the communication device.[55] This is a passive approach that would not interfere with authorized communications.

Because this approach would not involve the interruption of communications, it is not within the scope of this study. It is mentioned here only to give a complete sense of the available alternatives.

---

51. 47 U.S.C. §§ 302a, 333.
52. Nat'l Telecomm. & Info. Admin., *Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions* (2010) (hereafter "NTIA Report").
53. Cal. Council on Sci. & Tech., *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons* (2012) (hereafter "CCST Report").
54. *Id.* at 3.
55. See discussion in NTIA Report at 27-31.

Managed Access Systems

A managed access system ("MAS") uses existing wireless communication technology to establish a small, geographically-limited communication system. It would operate in essentially the same way as any other cell network system, but with a very small area of effect. Any wireless communication device that places a call within the area covered by the MAS would be connected to the MAS. The device's identity would be checked against a database of approved devices. If the device is on the approved list, the MAS would allow the device to connect to a carrier's network and the call would continue unimpeded. If the device is *not* on the approved list, the MAS would prevent connection with any outside carrier network. The call would be dropped.[56]

In effect, the MAS device stands between the mobile communication device and service provider networks, acting as a gatekeeper. Only preauthorized devices are allowed to connect to an outside service provider.

At the time of the CCST report (2012), the use of MAS to block unauthorized wireless communications in correctional facilities was an emerging technology. There had been pilot tests, but the technology was not yet in routine use.[57] The report identifies a number of potential practical problems associated with use of MAS in prisons:

- As new communication protocols are introduced, MAS systems would need to be updated to properly coordinate with carriers that use the new protocols.
- It could be difficult to limit the area affected by an MAS to the boundaries of a correctional facility. If the MAS were to reach beyond the confines of a facility, it could capture and block wireless communications of non-prisoners in adjacent areas. This is less of a concern for prisons in remote rural locations. But many jails are in built-up urban areas.
- MAS systems must broadcast on frequencies that have been allocated for the exclusive use of commercial carriers. Correctional institutions would need to secure the carriers' permission to use those frequencies.
- Some kinds of wireless communication (e.g., texting) occur so quickly that the MAS screening might not be effective in trapping and blocking the communication.

56. See CCST Report at 15-17.
57. *Id.* at 17-18.

It is not clear whether the use of MAS to intercept and block prisoner wireless communications would fall within the scope of this study. The MAS equipment might be wholly owned and operated by the correctional facility, in which case the only involvement of service providers would be granting permission to use their radio frequencies. However, it is also possible that communication service providers would go into the business of installing and operating MAS systems in correctional facilities. That degree of involvement in the interruption of communications would probably be within the scope of this study.

Service Provider Deactivation of Contraband Device

Another possibility would be for correctional institutions to partner with service providers to set up a system to detect and deactivate specific contraband wireless communication devices, as they're used.

Correctional officers could provide service providers with a list of approved communication devices. The service provider would then monitor all communications that begin or end within the vicinity of the correctional facility. This could be done using triangulation between existing nearby cell towers or perhaps by installing a local tower that only provides service to the correctional facility (this would be very similar to how an MAS operates, as described above). When the service provider identifies an unauthorized device, it would discontinue service to that device.

This approach was recommended in the CCST Report:

> The CCST Project Team recommends that … cell phone carriers be engaged to explore options of denying connections for 'unregistered' cell phones within prison locations using the carriers' technology. In this latter case, identity of illegal cellular phones could be obtained via a benchmarking technology and the carrier could then deny cellular connection to the specific unregistered devices. Engaging the carriers would likely require either a legal requirement to participate or an income incentive via fee for participation.[58]

This option, which might be the easiest and least problematic to implement, would seem to fall squarely within the scope of this study. It would involve a state or local government requesting that a service provider interrupt certain communication services.

58. CCST Report at 14.

Analysis and Recommendation

As discussed below, government interruption of the wireless communications of prisoners is materially different from the other scenarios examined in prior memoranda.

Due Process

In the scenarios discussed earlier in this study, the taking of property without due process was a central concern. When government seeks to terminate a communication service that it alleges is being used as part of a criminal activity, it must afford the affected person an opportunity to dispute the government's allegations. Otherwise, a valuable asset could be seized erroneously and without recourse.

That was the crux of the problem in *Sokol v. Public Utilities Commission*[59] and *Goldin v. Public Utilities Commission*.[60] In those cases, it was held that government can summarily terminate communication service to a person who is using the service to conduct a criminal enterprise, *but only with the prior approval of a magistrate*. The magistrate must find that summary termination of the service is "'directly necessary' to the furtherance of an important public interest" and that there was a "demonstrable need for prompt and immediate action."[61] There must also be a prompt opportunity for post-termination judicial review.[62]

The magistrate approval requirement announced in those cases was codified in Public Utilities Code Section 7908. Among other things, that section requires a judicial officer to find:

> (A) That probable cause exists that the service is being or will be used for an unlawful purpose or to assist in a violation of the law.
>
> (B) That absent immediate and summary action to interrupt communications service, serious, direct, and immediate danger to public safety, health, or welfare will result.[63]

The magistrate approval requirement described above seems unnecessary when government seeks to interrupt wireless communications in a correctional facility, for four reasons:

---

59. 65 Cal. 2d 247 (1966).
60. 23 Cal. 3d 638 (1979).
61. *Id.* at 663.
62. *Id.* at 665.
63. Pub. Util. Code § 7908(b)(1)(A)-(B).

(1) *Prisoners have significantly restricted rights to possess personal property*. There are many types of property that are lawfully banned for security reasons, including wireless communication devices. It is a crime for a prisoner to possess such a device in California. For that reason, terminating wireless communication services would not seem to affect any legitimate property interest. Prisoners have no reasonable expectation that they will receive wireless service in prison.

(2) *Pre-deprivation hearings are generally not required when seizing prisoner property*. Post-deprivation hearings are adequate for due process purposes.[64]

(3) *Wireless communication by prisoners is categorically unlawful*. In *Sokol* and *Goldin*, pre-authorization by a magistrate was necessary in order to establish probable cause that law enforcement's allegations were correct — that the communication service at issue was indeed being used to further a criminal enterprise. Unauthorized wireless communications in prison are always illegal. The content of the communication is irrelevant. *It is the medium that is proscribed.* If government acts to block unauthorized wireless communications in prison it is *necessarily* blocking unlawful communications. The staff sees little point in requiring a magistrate to find probable cause, on a case-by-case basis, that this is true.

(4) *Proscribing wireless communications in prison is a matter of routine prison security.* For that reason, it might be problematic to require that a magistrate find an "immediate" need to block wireless communications to prevent a "serious, direct, and immediate danger to public safety, health, or welfare" (as required by Public Utilities Code Section 7908. That level of exigency might be hard to find when correctional officers take routine steps to implement general security rules.

Free Expression

As discussed at length above, it seems very unlikely that action to block unauthorized wireless communications in prison would violate prisoners' constitutional free expression rights. Consequently, the staff sees no First Amendment rationale for requiring magistrate approval before taking such action.

Recommendation

The staff takes no position on the general policy question of whether to restrict prisoner use of telephones, and to what extent. That issue is beyond the

64. See, e.g., Hudson v. Palmer, 468 U.S. 517 (1984).

scope of this study. For the purposes of this study, it is sufficient to understand that California does restrict telephone use, that a prohibition on the possession and use of wireless communication devices is an element of that regulatory scheme, and that such restrictions appear to be lawful. With those policy decisions already having been made by the Legislature, the Governor, and correctional officials, the only question presented in this study is the extent to which state and local officials may lawfully require that service providers interrupt communications to effectuate the established prohibition on cell phones in prisons. As discussed above, such action would appear to be constitutional under the existing case law.

The staff recommends that an express exception be added to Public Utilities Code Section 7908 for action by correctional officials to interrupt communication services within a correctional facility. This would not immunize such action from being challenged on constitutional, statutory, or other grounds. It would simply make clear that the magistrate pre-approval requirement would not apply.

PUBLIC SCHOOLS

Public schools are another setting in which government has special interests that may justify regulating the free expression of those in its charge. The discussion below first summarizes the relevant Supreme Court cases discussing public school regulation of student speech. It then considers whether there is any likelihood that a public school would ever have reason to interrupt communication services.

Student Free Expression

While public school students do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gates,"[65] those rights are "not automatically coextensive with the rights of adults in other settings."[66]

In considering whether public school regulations that restrict student speech violate student First Amendment rights, the Supreme Court has established different standards for differing circumstances.

65. Tinker v. Des Moines Independent Communicty School Dist., 393 U.S. 503, 506 (1969).
66. Bethel v. Fraser, 478 U.S. 675, 682 (1986).

In *Tinker v. Des Moines Independent Community School District*,[67] the Court considered a public school rule that prohibited students wearing black armbands to school, to protest against the military conflict in Vietnam. The Court held that wearing armbands for that purpose was pure political speech, that the prohibition was based on the content of the speech, and that the armbands would not materially and substantially interfere with schoolwork or discipline. For those reasons, the prohibition was not constitutionally permissible. Although the Court did not find constitutional justification for the school's prohibition on armbands, it did recognize that there are circumstances where student speech may be limited without violating students' First Amendment rights:

> [C]onduct by the student, in class or out of it, which for any reason — whether it stems from time, place, or type of behavior — materially disrupts classwork or involves substantial disorder or invasion of the rights of others is, of course, not immunized by the constitutional guarantee of freedom of speech.[68]

Bethel School District v. Fraser[69] discussed another circumstance where a public school may regulate student speech without violating the Constitution. In that case, a public high school student gave a student election endorsement speech that was filled with sexual innuendo. The student was suspended and removed from a list of eligible speakers for future school events. In finding that the school's actions did not offend the First Amendment, the Court held that public schools may prohibit modes of expression that are inconsistent with the "fundamental values necessary to the maintenance of a democratic political system,"[70] which schools properly seek to inculcate in their students:

> Nothing in the Constitution prohibits the states from insisting that certain modes of expression are inappropriate and subject to sanctions. The inculcation of these values is truly the "work of the schools." … The determination of what manner of speech in the classroom or in school assembly is inappropriate properly rests with the school board.[71]

The next year, in *Hazelwood School District v. Kuhlmeier*,[72] the Court held that schools may regulate student expression in the context of school-sponsored

67. 393 U.S. 503 (1969).
68. *Id.* at 513.
69. 478 U.S. 675 (1986).
70. *Id.* at 683.
71. *Id.*
72. 484 U.S. 260 (1987).

expressive activities (e.g., a school newspaper or play). In that case, public school officials had censored a student newspaper by deleting student-authored articles about students' experiences with pregnancy and parental divorce. The Court explained that schools must have the ability to control the content of sponsored expressive activities in order to control course content and ensure that inappropriate expression is not attributed to the school itself. For those reasons, the Court said:

> Accordingly, we conclude that the standard articulated in *Tinker* for determining when a school may punish student expression need not also be the standard for determining when a school may refuse to lend its name and resources to the dissemination of student expression. Instead, we hold that educators do not offend the First Amendment by exercising editorial control over the style and content of student speech in school-sponsored expressive activities so long as their actions are reasonably related to legitimate pedagogical concerns.[73]

Finally, in *Morse v. Frederick*,[74] the Court added one further wrinkle. That case involved a public high school's decision to punish a student for displaying a banner, at a school-sanctioned off-campus event, which read "BONG HiTS 4 JESUS." The Court held that "schools may take steps to safeguard those entrusted to their care from speech that can reasonably be regarded as encouraging illegal drug use. We conclude that the school officials in this case did not violate the First Amendment by confiscating the pro-drug banner and suspending the student responsible for it."[75]

Interruption of Communications by Public Schools

As discussed above, there are situations in which public schools may limit student expression without violating the First Amendment. The constitutionality of such action would depend on the circumstances and nature of the speech and its effect on the school and other students. This means that any analysis of the extent to which public schools can lawfully interrupt communications would need to be grounded in the specific factual scenarios in which such action might be taken.

In considering what those scenarios might be, the staff has largely drawn a blank. It is relatively easy to imagine a situation in which a school administrator

73. *Id.* at 272-73 (footnotes omitted).
74. 551 U.S. 393 (2007).
75. *Id.* at 397.

might want to restrict student use of cell phones — to enforce a general prohibition on phone use during instructional hours, to prevent cheating during standardized testing, to manage student gang activity or other crimes on campus, etc. But it is difficult to imagine an administrator concluding that the best way to address those issues would be to contact service providers and request a general interruption of all cell phone service in the area of the school.

Such action would have severe negative side effects. School sites are often embedded within residential neighborhoods. Any blanket interruption of communications at a school site would undoubtedly also disrupt communications of non-students in the neighborhood (including law enforcement and emergency responders), teachers, and school staff. Moreover, parents would probably be extremely resistant to any action that would make it impossible to contact their children in an emergency, or vice versa. Nor does it seem likely that a blanket interruption of communications would be necessary. To the extent that schools need to prohibit students from using cell phones during the school day, they can do so the old-fashioned way, having teachers or proctors watch for violations of school rules and then take action to enforce them.

The staff does see one scenario in which schools might want to take action to block some student speech, as a response to "cyber-bullying."[76] If a student posts content on a social media site that is clearly intended to harass or humiliate another student, the school might reach out to the social media service provider and request that the offensive content be deleted. That is among the responses recommended by the California School Boards Association.[77]

Such a response would probably not require any exercise of state power to compel that the offensive material be removed. Many social media providers already have policies in place that forbid content that is intended to bully or harass. For example, Facebook's community standards authorize the removal of "content that appears to purposefully target private individuals with the intention of degrading or shaming them."[78] If a school were to report a student

76. See Educ. Code § 48900(r) (defining bullying, including bullying by "electronic act").

77. Cal. School Boards Ass'n, Cyberbullying: Policy Considerations for Boards 5 ("Depending on the seriousness of the harassment, responses might include … filing a complaint with the Internet service provider or social networking site to have the content removed and/or the student's user privileges revoked…."), *available at* < https://www.csba.org/Services/Services/PolicyServices/~/media/Files/Services/PolicyServices/SamplePolicies/Cyberbullying.ashx>.

78. See < https://www.facebook.com/communitystandards#>.

for posting bullying content to a social media site, causing the service provider to *voluntarily* remove the offensive content by way of enforcing its own rules, it would not be the school that is interrupting the communication. The school would simply be raising a concern, as any citizen might, about content that violates the provider's own community standards. The provider would then decide whether and how to proceed.

So long as the school does not purport to compel action by a service provider, this kind of action would not seem to implicate constitutional concerns (or be within the scope of this study).

Recommendation

Because there seems to be little realistic likelihood that public schools would ever contact providers and require that communication services be interrupted, there is probably no need for any special legislative language addressing such action by schools. **This conclusion should be explained in the Commission's report, but the staff recommends against revising existing law to address schools in any special way.**

EMERGENCY ALERTS

There are a number of ways in which government might interrupt communications in order to push emergency information out to the public. Before the widespread availability of cell phones and other modern mobile communications devices, this was done by means of the federal Emergency Broadcast System (now the Emergency Alert System[79]). The Emergency Alert System has the capacity to interrupt broadcast media in order to provide information about imminent emergencies (e.g., a tornado warning):

> The Emergency Alert System (EAS) is a national public warning system that requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service (SDARS) providers, and direct broadcast satellite (DBS) providers to provide the communications capability to the President to address the American public during a national emergency. The system also may be used by state and local authorities to deliver important emergency information, such as AMBER alerts and weather information targeted to specific areas.[80]

79. See 47 C.F.R. § 11.1 *et seq*.
80. See < https://www.fcc.gov/general/emergency-alert-system-eas>.

As indicated, states may use the EAS to broadcast "AMBER Alerts."

> The AMBER Alert™ Program is a voluntary partnership between law-enforcement agencies, broadcasters, transportation agencies, and the wireless industry, to activate an urgent bulletin in the most serious child-abduction cases. The goal of an AMBER Alert is to instantly galvanize the entire community to assist in the search for and the safe recovery of the child.[81]

In addition to disseminating emergency alerts and AMBER Alerts through broadcast media, government can now send such alerts to wireless communication devices, using the Wireless Emergency Alerts system ("WEA").[82]

> WEA is a public safety system that allows customers who own certain wireless phones and other enabled mobile devices to receive geographically-targeted, text-like messages alerting them of imminent threats to safety in their area. The technology ensures that emergency alerts will not get stuck in highly congested areas, which can happen with standard mobile voice and texting services. WEA (formerly known as the Commercial Mobile Alert System (CMAS) or Personal Localized Alerting Network (PLAN)) was established pursuant to the Warning, Alert and Response Network (WARN) Act.
>
> WEA enables government officials to target emergency alerts to specific geographic areas – lower Manhattan, for example – through cell towers that broadcast the emergency alerts for reception by WEA-enabled mobile devices.
>
> Wireless companies volunteer to participate in WEA, which is the result of a unique public/private partnership between the FCC, FEMA and the wireless industry to enhance public safety.[83]

The receipt of WEA messages by individual device owners is mostly optional. A device owner can block all WEA messages except emergency notices from the president.[84]

The EAS and WEA are relevant to this study because they involve government action that temporarily interrupts regular communication service in order to send the government's own message over the affected media. This action requires the involvement of communication service providers.

The staff has not found any case holding that government's use of the Emergency Alert System or the Wireless Emergency Alerts system is

---

81. See <http://www.amberalert.gov/index.htm>.
82. Pub. L. 109-347, § 601 *et seq*. (''Warning, Alert, and Response Network Act''); 47 C.F.R. § 10.1 *et seq*.
83. 47 C.F.R. § 10.280.
84. Pub. L. 109-347, § 602(b)(1)(E).

unconstitutional. There is one possible argument against the constitutionality of these messaging systems — that the First Amendment does not permit government to require a "captive audience" to listen to government messages.

That was one of the issues considered in *Public Utilities Commission v. Pollack*,[85] a case that involved a public transit system's decision to broadcast radio programming for passengers on its streetcars. That practice was challenged on multiple grounds, including an assertion that it violated the First Amendment rights of the passengers.

The Court found no violation of the First Amendment, explaining:

> Pollak and Martin contend that the radio programs interfere with their freedom of conversation and that of other passengers by making it necessary for them to compete against the programs in order to be heard. The Commission, however, did not find, and the testimony does not compel a finding, that the programs interfered substantially with the conversation of passengers or with rights of communication constitutionally protected in public places. It is suggested also that the First Amendment guarantees a freedom to listen only to such points of view as the listener wishes to hear. There is no substantial claim that the programs have been used for objectionable propaganda. There is no issue of that kind before us. … The inclusion in the programs of a few announcements explanatory and commendatory of Capital Transit's own services does not sustain such an objection.[86]

In a concurring opinion, Justice Black made clear that the First Amendment would be offended if government were to require a captive audience to listen to propaganda:

> I also agree that Capital Transit's musical programs have not violated the First Amendment. I am of the opinion, however, that subjecting Capital Transit's passengers to the broadcasting of news, public speeches, views, or propaganda of any kind and by any means would violate the First Amendment. To the extent, if any, that the Court holds the contrary, I dissent.[87]

Justice Douglas dissented, arguing that a system of government broadcasting to a captive audience presents a potential for abuse of privacy that should not be tolerated. His argument focused mostly on the claim that the streetcar radio broadcasts violated a right of privacy protected by the Fifth Amendment:

---

85. 343 U.S. 451 (1952).
86. *Id.* at 463 (footnote omitted).
87. *Id.* at 466 (Black, J. concurring).

> The government may use the radio (or television) on public vehicles for many purposes. Today it may use it for a cultural end. Tomorrow it may use it for political purposes. So far as the right of privacy is concerned the purpose makes no difference. The music selected by one bureaucrat may be as offensive to some as it is soothing to others. The news commentator chosen to report on the events of the day may give overtones to the news that please the bureau head but which rile the streetcar captive audience. The political philosophy which one radio speaker exudes may be thought by the official who makes up the streetcar programs to be best for the welfare of the people. But the man who listens to it on his way to work in the morning and on his way home at night may think it marks the destruction of the Republic.
>
> One who tunes in on an offensive program at home can turn it off or tune in another station, as he wishes. One who hears disquieting or unpleasant programs in public places, such as restaurants, can get up and leave. But the man on the streetcar has no choice but to sit and listen, or perhaps to sit and to try *not* to listen.
>
> When we force people to listen to another's ideas, we give the propagandist a powerful weapon. Today it is a business enterprise working out a radio program under the auspices of government. Tomorrow it may be a dominant political or religious group. Today the purpose is benign; there is no invidious cast to the programs. But the vice is inherent in the system. Once privacy is invaded, privacy is gone. Once a man is forced to submit to one type of radio program, he can be forced to submit to another. It may be but a short step from a cultural program to a political program.
>
> If liberty is to flourish, government should never be allowed to force people to listen to any radio program. The right of privacy should include the right to pick and choose from competing entertainments, competing propaganda, competing political philosophies. If people are let alone in those choices, the right of privacy will pay dividends in character and integrity. The strength of our system is in the dignity, the resourcefulness, and the independence of our people. Our confidence is in their ability as individuals to make the wisest choice. That system cannot flourish if regimentation takes hold. The right of privacy, today violated, is a powerful deterrent to any one who would control men's minds.[88]

Although *Pollack* upheld the constitutionality of the streetcar radio system, it suggests that government broadcasting to a captive audience could, in some situations, violate the listeners' constitutional rights. If the EAS and the WEA were used to broadcast propagandistic messages, there would be reason for

88. *Id.* at 468-69 (Douglas, J, dissenting).

concern. But the infrequent use of such systems to send emergency alerts seems unobjectionable.

The staff recommends that Public Utilities Code Section 7908 be amended to make clear that it has no application to the interruption of communications by means of the Emergency Alert System or Wireless Emergency Alert system (or any similar emergency alert broadcasting system that might be developed in the future).

INTERNET SECURITY

There are a number of ways in which government might suspend specific channels of Internet communication, in order to protect against malware or other electronic threats to network operation and security. For example:

- If a computer has been taken over by malware and is being used for unauthorized purposes, the government might block the compromised computer's connection to the Internet.
- If a computer has been identified as the source of attempts to break a password on a secured system, government might block the offending computer's access to its target.
- If a "distributed denial of service" attack has been launched, by means of continuous mass connections to a targeted system, government might temporarily block all access to the target.
- If a destructive virus is propagating across the Internet, government might temporarily block all incoming email that contains suspect attachments.

The kinds of misconduct described above would almost certainly be criminal (though some threats could arise from simple malfunctions). Penal Code Section 502 imposes criminal sanctions on a person who misuses computers in wide variety of specified ways, including all the following:

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network.[89]

89. Penal Code § 502(c).

In many cases, government action to protect the security of computing systems will be taken on the government's own equipment. For example, California's public universities all operate extensive communications and computing systems, to provide Internet connectivity and services for employees and students. If campus IT staff discover a threat to the security of those systems, it can take immediate steps on its own equipment to neutralize the threat. That sort of routine system maintenance is not within the scope of this study, because it would not involve action by third-party communication service providers.

In some situations, government might reach out to communication service providers and request their assistance in blocking criminal misuse of computing resources or curing a software or hardware malfunction. In that situation, it seems almost certain that communication service providers would cooperate voluntarily. Service providers have a strong interest in protecting their systems from criminal misuse. It also seems nearly certain that the service agreements between providers and their customers will reserve the provider's right to terminate service to a customer who is criminally misusing the service. For example, Comcast's customer agreement reserves the right to immediately terminate or suspend a customer's service and delete any stored content, without notice, if it determines that the customer's use of the service violated the service agreement or any law.[90]

As discussed in a prior memorandum,[91] the First Amendment does not protect speech in service of criminal activity. For that reason, the staff is confident that any "expressive" aspects of computer hacking would not be constitutionally protected.

That prior memorandum also discussed how summary "seizure" of property does not offend constitutional due process so long as (1) immediate action is required to avoid harm to the public and (2) some form of post-seizure judicial review is available.[92] It seems likely that there will be many instances where immediate action needs to be taken to limit the harm from misuse of computing resources. It may not be practicable or useful to require a magistrate's approval before such action can be taken.

---

90. See Suspension and Termination by Comcast, *available at* <http://www.xfinity.com/Corporate/Customers/Policies/SubscriberAgreement.html>.

91. See Memorandum 2015-18, p. 12.

92. *Id*. at 9-12.

For example, suppose that an IT security employee at the University of California Davis notices that a specific computer in Los Angeles is attempting to break passwords on numerous student email accounts. In order to protect the privacy and integrity of the student accounts, the employee immediately imposes a block on the unidentified computer's Internet address, preventing it from accessing any university account. The employee then contacts the service provider for the offending computer and reports the attack. The service provider checks its own logs, confirms that its acceptable use policy has been violated, and terminates the account.

In that scenario, the staff sees little point in requiring the university employee to obtain a magistrate's approval before taking action. And the cost and delay of doing so could result in significant harm to the university's students and equipment.

The staff is inclined toward drafting a narrowly-drawn exception to the magistrate approval requirement of Public Utilities Code Section 7908, for any action that blocks a specific Internet service in order to address unlawful misuse or a malfunction. However, the staff concedes that its knowledge of computer security and networking concerns is thin. It is possible that some significant issue has been overlooked in the discussion above. Even if it is appropriate to draft an exception of the type proposed, the staff would benefit from technical advice on its wording.

For those reasons, the staff requests public comment on the merits of the proposed exception and how it should be framed.

GANG INJUNCTION

Memorandum 2016-5 discussed the constitutionality of government interruption of area communications, for the purpose of protecting the public from a dangerous public assembly. When discussing that memorandum, the Commission suggested that the staff also research case law on the constitutionality of gang injunctions.[93]

A "gang injunction" is a civil injunction crafted to abate a specific type of public nuisance — the range of harms caused by a criminal gang when it takes over a particular area as its base of operations (e.g., drug trafficking, violence, harassment, noise, public indecency, drug use, property damage). A gang

93. See Minutes (Feb. 2016), p. 4.

injunction seeks to abate that nuisance by restraining gang members from engaging in specified activities within the affected area. In California, a gang injunction may be issued under general nuisance law or provisions of the Street Terrorism Enforcement and Prevention Act.[94] For our purposes, the most relevant feature of a gang injunction is that it enjoins *association* by gang members in the specified area.

In *People ex rel. Gallo v. Acuna*,[95] a majority of the California Supreme Court held that a gang injunction did not violate the First Amendment rights of those enjoined. In that case, defendants were enjoined from, among other things, "[s]tanding, sitting, walking, driving, gathering or appearing anywhere in public view with any other defendant … or with any other known [member of specified gangs]" within a specified four square block area.[96] Defendants challenged that element of the injunction as violating their First Amendment right of free association.

The court explained that two types of association have been held to be entitled to First Amendment protection, those with "intrinsic" or "intimate" value, and association for religious or political purposes.[97] The first category involves deep attachment, selectivity, and seclusion, and includes the kinds of associations involved in the creation of families, the raising of children, and cohabitation with intimates.[98] The second involves groups that join together for "a wide variety of political, social, economic, educational, religious, and cultural ends."[99]

Association between members of a criminal street gang, within a limited geographical area, does not fall within either protected category. Freedom of association, in the sense protected by the First Amendment, "does not extend to joining with others for the purpose of depriving third parties of their lawful rights."[100]

That holding does not change the overall conclusion reached in Memorandum 2016-5 — that interruption of communications to suppress a dangerous public assembly would likely be constitutional if approved in

94. See Penal Code § 186.22a.
95. 14. Cal. 4th 1090 (1997).
96. *Id.* at 1110.
97. *Id.*
98. *Id.*
99. *Id.* at 1110-11.
100. *Id.* at 1112, *quoting* Madsen v. Women's Health Center, Inc., 512 U.S. 753 (1994).

advance by a magistrate under Public Utilities Code Section 7908. If anything, the holding in *Acuna* adds further support for that conclusion, by making clear that association for unlawful purposes can be restrained by a court without violating the First Amendment.

Unless the Commission directs otherwise, the staff will include a brief discussion of that point in the narrative "preliminary part" of a draft tentative recommendation.

NEXT STEPS

This memorandum concludes the discussion of issues presented in this study. After the Commission makes decisions on the topics presented in this memorandum, the staff will prepare a draft tentative recommendation that incorporates all of the decisions that the Commission has made in the course of this study.

Respectfully submitted,

Brian Hebert
Executive Director