Manohar Raju

Public Defender

City and County of San Francisco

Matt Gonzalez

Chief Attorney

Crystal R. Lamb, SBN 185810

Deputy Public Defender

555 Seventh Street

San Francisco, CA 94103

Direct: 415-553-4911

Fax: 415-553-9810  
Email: Crystal.Lamb@sfgov.org

Attorneys for DELBERT J ERVIN

**SUPERIOR COURT OF CALIFORNIA**

**SAN FRANCISCO COUNTY**

|  |  |
| --- | --- |
| People of the State of California,  Plaintiff,  vs.  DELBERT J ERVIN,  Defendant. | SCN:  Ltd. Juris. No.: 20010906  **MOTION TO MODIFY CONDITIONS OF RELEASE ON OWN RECOGNIZANCE**  Date: Date  Time: 9:00 AM  Dept: M11 |

COMES NOW THE DEFENDANT, DELBERT J. ERVIN, by and through his attorney of record, CRYSTAL LAMB of the San Francisco Public Defender’s Office, and presents this Motion to Modify Conditions of Release from Custody.

**Procedural History**

On October 16, 2020, Judge Richard C. Darwin of Department 11 of the above-entitled court, issued an order conditioning Mr. Ervin’s continued release on his own recognizance to a search and seizure condition, a prohibition against the use of encryption software on devices that connect to the internet and a mandate that he inform the police of his passwords to any electronic devices in his possession. Mr. Ervin had been released on his own recognizance prior to arraignment, and appeared in court on the date and time set for his arraignment at which time he was appointed counsel. Mr. Ervin had been released on his own recognizance prior to arraignment due to his complete lack of criminal history and prior failures to appear in court. He is a long time resident of San Francisco, a homeowner, and holds a professional job. He is 72 years old, Judge Darwin ordered the conditions on the mere request of ADA Katy Wells, who presented no specific facts regarding Mr. Ervin which would warrant the requested conditions. Rather, she asserted that other judges routinely impose these conditions (at her request) for anyone accused of the crimes for which Mr. Ervin stands accused (Mr. Ervin is accused of two counts of Penal Code Section 311.11). Defense counsel objected on Constitutional grounds: Fourth, Fifth, Sixth, and Fourteenth Amendments to the U.S. Constitution. At this time, counsel also objects on First and Eighth Amendment grounds. Judge Darwin granted the prosecution’s request and imposed the above conditions on Mr. Ervin, subject to defense counsel bringing a motion to modify conditions of release. In other words, Judge Darwin shifted the burden to the defendant to justify the removal of these conditions, rather than requiring the prosecution to provide specific facts regarding Mr. Ervin which would warrant their imposition.

This motion follows.

///

///

///

**Arguments and Authorities**

**1. The warrantless search condition violates Delbert’s 4th Amendment rights as applied to the State of California by and through the Due Process Clause of the 14th Amendment.**

The search and seizure condition herein sought to be modified states that a condition of release is “WARRANTLESS SEARCH OF PERSONAL PHONES, COMPUTER, TABLET, CLOUD STORAGE, HARD DRIVES.” See minute order attached hereto as Exhibit A.

The text of the 4th Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The 4th Amendment has been affirmatively held by the U.S. Supreme Court to apply to the states.[[1]](#footnote-1) Federal courts have consistently held that there is an expectation of privacy in personal electronic devices such as phones sufficient to invoke the protections of the 4th Amendment.[[2]](#footnote-2)

The seminal California case allowing courts to impose a waiver of defendants’ Fourth Amendment rights as a condition of pre-trial release is *In re York* (1995) 9 Cal. 4th 1133, 1149. However, in 2006 the Ninth Circuit held that conditions of pre-trial release requiring a defendant to waive 4th Amendment protections are an invalid condition of pretrial release.[[3]](#footnote-3) In footnote 1 of the *Scott* opinion the court stated,

The dissent points to only two states whose supreme courts have addressed this issue: Maine and California [ME citation omitted] (*In re York,* 9 Cal.4th 1133, 40 Cal.Rptr.2d 308, 892 P.2d 804 (1995). It is unclear whether those cases would come out the same way today, as both were decided before *United States v. Knights,* 534 U.S. 112, 122 S.Ct 587, 151 L.Ed.2d 1281, 149 L.Ed.2d 205 (2001)

California state courts are bound by United States Supreme Court decisions regarding constitution laws, but are not bound by lower federal court decisions, even on federal questions. “However, they are persuasive and entitled to great weight.”[[4]](#footnote-4)

///

///

///

1. The Ninth Circuit’s *Scott* Analysis:

Raymond Lee Scott was arrested in Nevada on state charges of drug possession. In order to qualify for release from custody, Mr. Scott was required to sign a form consenting to a standard list of pretrial release conditions, including random drug testing and a search of his home for drugs by any peace officer, at any time, with or without a warrant.[[5]](#footnote-5)

Based on an informant’s tip, state police officers went to Scott’s home and drug tested him. The test was positive for methamphetamine. Based on the positive test, Mr. Scott was arrested and his home was searched. An unregistered shotgun was found. Scott was subsequently indicted for unlawful possession of an unregistered shotgun. Mr. Scott brought a motion to suppress both the shotgun and his statements to police regarding the shotgun. Mr. Scott’s suppression motion was granted and the government appealed.[[6]](#footnote-6)

The *Scott* court first examined whether the drug test and search of Mr. Scott’s home were valid because Mr. Scott consented to them.[[7]](#footnote-7) In finding that they were not, the court pointed to the “unconstitutional conditions doctrine.”[[8]](#footnote-8) The court stated that the doctrine “limits the government’s ability to exact waivers of rights as a condition of benefits, even when those benefits are fully discretionary.”[[9]](#footnote-9) This is because the law does not give “the government free rein to grant conditional benefits by attaching strings strategically, striking lopsided deals and gradually eroding constitutional protections.”[[10]](#footnote-10) The court noted that the unconstitutional conditions doctrine was “especially important in the Fourth Amendment context.”[[11]](#footnote-11)

The court addressed the dissent’s argument that Fourth Amendment rights may be validly waived. The court stated, “[n]o one disputes that Fourth Amendment rights can be waived. [citations omitted] The question here is whether the government can *induce* Scott to waive his Fourth Amendment rights by conditioning pretrial release on such a waiver.”[[12]](#footnote-12) “While government may sometimes condition benefits on waiver of Fourth Amendment rights . . . its power to do so is not unlimited.”[[13]](#footnote-13) The court further noted,

[U]nder the Excessive Bail Clause . . . “the Government’s proposed conditions of release or detention [must] not be ‘excessive’ in light of the perceived evil.” [citations omitted] There may thus be cases where the risk of flight is so slight that any amount of bail is excessive; release on one’s own recognizance would then be constitutionally required, which could further limit the government’s discretion to fashion conditions of release.[[14]](#footnote-14)

The court then addressed the government’s “special needs” arguments. The “special needs” doctrine allows for searches on less than probable cause, even sometimes suspicionless seizures.[[15]](#footnote-15) However, under the special needs doctrine, the needs must be “beyond the normal need for law enforcement.”[[16]](#footnote-16)

The government’s proffered “special needs,” for the imposed conditions of pretrial release on Mr. Scott were (1) protecting the community from criminal defendants released pending trial and (2) ensuring that defendants show up at trial.”[[17]](#footnote-17)

The *Scott* court dismissed number one out of hand, noting, “[c]rime prevention is a quintessential general law enforcement purpose and therefore is the exact opposite of a special need.”[[18]](#footnote-18)

Having eliminated the first justification for the imposed conditions, the court then had to assume that the primary purpose of the imposed conditions was to ensure attendance in court.[[19]](#footnote-19)

The court noted that the connection between drug use and non-appearance at trial was tenuous.[[20]](#footnote-20) The court also noted that the government had produced no evidence to show that Mr. Scott was particularly likely to engage in future drug use that would decrease his likelihood of appearing at trial.[[21]](#footnote-21) It stated that the government may not rely on the special needs doctrine based only on “hypothetical” hazards that are unsupported by any concrete evidence, specific to the defendant:[[22]](#footnote-22)

The government in this case has relied on nothing more than a generalized need to protect the community and a blanket assertion that drug testing is needed to ensure Scott’s appearance at trial. Both are insufficient. We thus cannot validate Scott’s search under the special needs doctrine.[[23]](#footnote-23)

The *Scott* court stated that “pretrial releasees are ordinary people who have been accused of a crime but ***are presumed innocen*t**. . . People released pending trial . . . have suffered no judicial abridgment of their constitutional rights.”[[24]](#footnote-24)

The crux of this opinion bears repeating verbatim:

[T]he assumption that Scott was more likely to commit crimes than other members of the public, without an individualized determination to that effect, is contradicted by the presumption of innocence: That an individual is charged with a crime cannot, as a constitutional matter, give rise to any inference that he is more likely than any other citizen to commit a crime if he is released from custody. Defendant is, after all, constitutionally presumed to be innocent pending trial, and innocence can only raise an inference of innocence, not of guilt. . . [No] case authorizes detaining someone in jail while awaiting trial, or the imposition of special bail conditions based merely on the fact of arrest for a particular crime.[[25]](#footnote-25). . .The arrest alone did not establish defendant’s dangerousness . . .It follows that if a defendant is to be released subject to bail conditions that will help protect the community from the risk of crimes he might commit while on bail, the conditions must be justified by a showing that defendant poses a heightened risk of misbehaving while on bail. The government cannot, as it is trying to do in this case, short-circuit the process by claiming that the arrest itself is sufficient to establish that the conditions are required.[[26]](#footnote-26)

The court concluded that the search of Mr. Scott and his home did “not pass constitutional muster” based on either consent, special needs, or the totality of the circumstances.[[27]](#footnote-27)

The imposed conditions of release on Mr. Ervin, quite frankly, are exponentially more problematic than those in *Scott:* San Francisco County uses an algorithm to score the potential of an arrested individual to recidivate or fail to appear in court.[[28]](#footnote-28) Only those who score the lowest possible on each scale are released on their own recognizance, without conditions, prior to arraignment.

Further, in this case, Mr. Scott did NOT consent to the conditions of release. Mr. Ervin, through counsel, immediately objected to the imposition of the conditions on constitutional grounds. Mr. Scott did not sign a consent form, nor affirmatively agree to a waiver of his constitutional rights.

In addition, this court did not require the prosecutor to provide any specific facts regarding Mr. Ervin (and, as pointed out above, the charges themselves are NEVER a permissible, constitutionally valid reason to impose a waiver of constitutional rights pending trial) that would show, by clear and convincing evidence, that Mr. Ervin was likely to commit crimes while on release, posed a public safety risk, or was likely to abscond or fail to appear in court. This court, to its discredit, imposed the conditions based on the prosecution’s statement that 1. The crime is repugnant 2. Child porn victims are re-victimized every time a photo is viewed or disseminated and 3. Other judges routinely impose these conditions on anyone charged with PC 311.11.

When asked by defense counsel, Ms. Wells was unable to provide the name of any person victimized by Mr. Scott in this case. Nor was she able to provide specific evidence REGARDING MR. ERVIN, rather than folks in general charged with identical crimes, that would prove that Mr. Ervin posed a public safety risk or would fail to appear in court.

**2. The bail condition prohibiting the use of encryption software is an unconstitutional prior restraint of free speech.**

The order to be modified states that Mr. Ervin may not use encryption software on devices that connect to the internet. This issue goes to extremely fundamental legal questions but requires a sufficient grasp of technological issues, which necessitates a technical introduction.

1. Technical Introduction as to computer encryption

Although modern pop culture might suggest that encryption is some new discipline available only to the highest of computer coding gurus versed in pure mathematics, the truth is that encryption is a far older and a far more accessible practice than the modern legal issues arising from it.

Basic written encryption involves taking a message or note and scrambling the information it conveys by changing the characters to something else according to a prearranged set of rules and formulas called a cipher or key.[[29]](#footnote-29) The cipher is held by the sender and receiver or the note taker, and the message or note in its scrambled form can then be discovered by any third person not in possession of the cipher, and such third person will then be unable to determine the original contents, hence the origin of the English word, “decipher,” a synonym for “decrypt,” which is the act of using a cipher to unscramble an encrypted message or note into its meaningful state.

The introduction of the use of modern computers into the domain of encryption is not qualitatively different from the replacement of the abacus by the calculator in the field of accounting. It is a tool which opens up new horizons of speed and degree. It may lead to a dependency on the tool as people stop practicing the skill previously done with pencil and paper, but no one would deny that with sufficient time and discipline, the computer’s task could be performed with pencil and paper.

Encryption today is not used less than in the past. It is used far more, precisely because of the combination of the advent of the internet and the computer. Every judicial efiling system of any sophistication uses encryption, so a prohibition against using encryption software on a machine that connects to the internet is a closing of the courthouse doors in many instances. Particularly in the age of COVID-19, and particularly in San Francisco, the medical profession is rapidly moving online, and encryption is strictly essential to the management of such practice, so a prohibition against using encryption software on a machine that connects to the internet is a prohibition against seeking medical advice and attention from the isolation of one’s home in the middle of a pandemic. Modern lawyers who are bound to protect the confidences of their clients often use encrypted communication, and there is some discussion among the profession that a basic knowledge and regular use of encryption is a requirement of professional responsibility, so a prohibition of the use of encryption software on a device that connects to the internet is a denial of the effective right to counsel. ATMs and online banking use encryption and connect to the internet, so such a prohibition is an imposed vow of poverty. Mental health professionals, food delivery services and online libraries all require the use of encryption software on devices connected to the internet. In 2020, when lockdowns and cash businesses are regularly closed by the state due to disease and fire, the denial of the right to use encryption software on devices that connect to the internet is nothing less than an exclusion from civilization itself.

1. Established case law recognizes that restrictions on encryption are restrictions on freedom of speech

In 1997, The Northern Federal District Court of California heard the case of *Bernstein v. U.S. Dept. of State*,[[30]](#footnote-30) which concerned legal prohibitions placed on a Berkeley computer scientist who developed an encryption and decryption protocol. The U.S. Department of State, citing national security concerns that the protocol could be used as a weapon, sought to impose an executive order on the scientist, limiting its distribution.[[31]](#footnote-31) The scientist sued in federal court to have the executive order declared unconstitutional as a prior restraint of freedom of speech.[[32]](#footnote-32) That court’s opinion is deeply complex and concerns multiple counts and allegations concerning byzantine and rapidly adjusting attempts by the Clinton administration to craft regulation through the course of the litigation, but the basic holding of the court after many iterations was that encryption programs are themselves speech, and that even licensing limitations on them amount to prior restraint, and are thus unconstitutional.[[33]](#footnote-33) Furthermore, that court held that the regulations in question, since they concerned speech, were subject to the higher level of over breadth scrutiny reserved for such restrictions,[[34]](#footnote-34) and that court then found the federal government’s licensing restrictions overbroad as well as a prior restraint.[[35]](#footnote-35)

There is no reason to believe that the outcome of the *Bernstein* case would have been different if, rather than a scientist developing and distributing the protocol, Bernstein had been a private citizen using it. The First Amendment protects the reader as well as the writer, and the consumer of media as well as its producer.[[36]](#footnote-36) It is the software itself which is the subject of the *Bernstein* court’s findings, and these findings comport with common sense.

The case at bar involves a much broader, much less well-defined regulation than the executive order in the *Bernstein* case. Whereas that case involved a complex and intricate regulatory framework, here again the order sought to be modified presents a single, all-caps sentence which could have any meaning at all. What is “encryption software?” Does that include only standalone applications for encrypting on-disk files like Veracrypt, or does it include the encryption and decryption protocols that must exist in every modern web browser? Does it include decryption software or encryption software used for decryption? Does it include email or instant messaging? Does this refer to all encryption, or just end-to-end encryption (the kind with no third party having the cipher)? Does it include file compression programs like WinRar which can be used to encrypt, but are also simply necessary for packaging files for easy transmission? What about ATMs or electronic voting machines? Can he sign for a package when a delivery driver from UPS asks him to sign an electronic pad? More importantly, how, without any existing case law, is Mr. Ervin or his lawyer meant to figure out the answers to these questions? It cannot be done. This prohibition would be among the most overbroad legal commands to ever escape a judge’s pen, (and doubtless the order was generated automatically on a computer which is doubtlessly connected to the internet using encryption protocols).

**3. The bail condition requiring Mr. Ervin to provide passwords violates his privilege against self-incrimination, his right to counsel and his right to privacy.**

Fifth Amendment jurisprudence includes not only self-incriminating testimony in court, but also testimonial evidence produced to law enforcement for the purpose of being used in court against the defendant.[[37]](#footnote-37) The scope of the privilege against self-incrimination is wide and deep and covers not only outright admissions of criminal culpability, but anything which could lead to evidence of a crime.[[38]](#footnote-38) The touchstone of the privilege against self-incrimination is a defendant should not be compelled to disclose the contents of his/her own mind.[[39]](#footnote-39) Criminal defendants are often doubly protected from such questioning once they have been appointed counsel because such requests violate the right to counsel as recognized in the *Massiah* line of cases.[[40]](#footnote-40) For such questioning to be compelled by a court order does not cure this defect in any way. Indeed, the core of the privilege against self-incrimination is precisely created to prevent a situation in which the defendant is ordered by a court to self-incriminate. That such an order would be enforceable by incarceration through revocation of bail rather than incarceration by a finding of contempt makes little practical difference.

Here, an order compelling the defendant to produce passwords to law enforcement, outside the presence of his appointed counsel, is obviously intended to aid law enforcement in their search for incriminating evidence against Mr. Ervin. If similar prosecutions are of any indication, they are not only hoping to find more contraband, but also metadata and anything that would help them to prove that Mr. Ervin accessed and made deliberate choices to acquire the contraband at issue in the two counts already pled, or that he had knowledge that the contraband was on his computer, or that the computer in question belonged to him. Assuming without admitting that the device at issue did in fact belong to Mr. Ervin, even giving a password to gain basic metadata would be incriminating, and therefore protected by the privilege against self-incrimination. Such information would also be protected by the right to counsel since Mr. Ervin has been appointed counsel.

1. The Password condition violates Mr. Ervin’s right to be free of unreasonable and unwarranted search

To compel Mr. Ervin to provide passwords to law enforcement would have the same 4th Amendment effect as the police forcing them open. It would require a warrant which complies with the requirements imposed by the 4th Amendment, already covered above under the search and seizure condition: probable cause, particularity in time, space and description, and a basis in sworn testimony. As with the search and seizure condition, none of these conditions are met even to the point that an officer could rely on them in good faith. Thus, this bail condition also violates Mr. Ervin’s 4th Amendment rights for the same reason that the search and seizure condition does.

Courts have addressed these issues by holding that probation conditions requiring supplying passwords is in violation of the 4th Amendment as being overbroad.[[41]](#footnote-41) The basic argument is that since devices tend to hold so much information about a person from so many different sources, the act of providing a password is in effect a statement of incredible breadth and depth across a wide variety of issues. The *Valdivia* court referred the words of Justice Learned Hand that there is a difference between searching a man’s pockets and ransacking his house, and then pointed out that in the age of smartphones, the contents of a pocket can be much broader than the contents of a house.[[42]](#footnote-42)

1. The password condition is unworkable.

Part of the reason that the privilege against self-incrimination is so deeply enshrined in the American system is that it is so naturally enforced. If a person simply chooses not to speak, there is little that can be humanely done to force them to. Similarly, if a person’s should claim a failure of memory, how would anyone prove whether it were genuine?

This court’s password condition in the order to be modified is not only illegal; it is entirely unworkable. Who, in modern society has never forgotten a password? If Mr. Ervin should claim that he does not remember a password, or that he never had one because the device law enforcement presents him with was not his, how will the court know whether he is telling the truth? If law enforcement wants Mr. Ervin to go back to jail, all they have to do is present Mr. Ervin with a locked device found somewhere near his belongings that he never owned, and then insist that Mr. Ervin is lying when he says he does not have the password. The court would never know the difference. Alternately, if Mr. Ervin were to simply claim that he had forgotten all of his passwords at the same time, the court could never figure out which he had genuinely forgotten and which he had not so as to determine with particularity how he had violated the court’s order. Thus, this condition is not merely unconstitutional for a wide variety of reasons; it would be completely unenforceable even if Mr. Ervin had no constitutional rights.

**Conclusion**

The search and seizure condition under the court’s bail condition plainly violate Mr. Ervin’s 4th and 8th Amendment rights. The encryption condition plainly violates Mr. Ervin’s 1st and 4th Amendment rights. The password condition plainly violates Mr. Ervin’s 1st, 4th, 5th and 6th Amendment rights, and all three violate his right to privacy under the 14th Amendment. These blanket conditions, unsupported by sworn testimony or evidence are directly opposed to the traditions and values of American law. This court should strike these conditions immediately.

DATED: October 29, 2020 By:

|  |
| --- |
| Crystal R. Lamb  Deputy Public Defender  Attorney for Delbert Ervin |

EXHIBIT A

1. *Elkins v. U.S.*, 364 U.S. 206, 213 (1960) *citing*: *Wolf v. Colorado*, 338 U.S. 25, 27-28 (1949); *also citing: Stefaneli v. Minard*, 342 U.S. 117, 119 (1951); *also citing* *Irvine v. California*, 347 UI [↑](#footnote-ref-1)
2. *See Riley v. California*, 573 U.S. 373 (finding a reasonable expectation of privacy in call log data contained on a phone) ;*see also U.S. v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (holding that there is a legitimate, objectively reasonable expectation of privacy in a personal computer); *citing U.S. v. Buckner*, 473 F.3d 551, 554n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in password-protected computer files) [↑](#footnote-ref-2)
3. *U.S. v. Scott*, 450 F.3d 863, 868, 875 (9th Cir., 2006) (holding that one who has been released on pre-trial bail does not lose his or her Fourth Amendment protections); *See also* *U.S. v. Gardner*, 523 F. Supp. 2d 1025, 1034 (Cal. N. Dist., 2007) (holding that defendants on pretrial release do not have reduced expectations of privacy like probationers). [↑](#footnote-ref-3)
4. *People v. Bradley* (1969) 1 Cal.3d 80, 86. [↑](#footnote-ref-4)
5. *U.S. v. Scott* at 865. [↑](#footnote-ref-5)
6. *Id.,* at 865. [↑](#footnote-ref-6)
7. *Id.* [↑](#footnote-ref-7)
8. *Id.,* at 866. [↑](#footnote-ref-8)
9. *Id.* [↑](#footnote-ref-9)
10. *Id.* [↑](#footnote-ref-10)
11. *Id.,* at 867. [↑](#footnote-ref-11)
12. *Id,* at footnote 4. [↑](#footnote-ref-12)
13. *Id.,* at 867-868. [↑](#footnote-ref-13)
14. *Id.,* at footnote 5. [↑](#footnote-ref-14)
15. *Id.,* at 868. [↑](#footnote-ref-15)
16. *Id..* [↑](#footnote-ref-16)
17. *Id.,* at 869 [↑](#footnote-ref-17)
18. *Id.,* at 870. [↑](#footnote-ref-18)
19. *Id.* [↑](#footnote-ref-19)
20. *Id.* [↑](#footnote-ref-20)
21. Id. [↑](#footnote-ref-21)
22. *Id.* [↑](#footnote-ref-22)
23. *Id.,* at 872. [↑](#footnote-ref-23)
24. *Id.,* at 871. Emphasis added. [↑](#footnote-ref-24)
25. *Id.,* at 874. [↑](#footnote-ref-25)
26. *Id.*  [↑](#footnote-ref-26)
27. *Id.* [↑](#footnote-ref-27)
28. The defendant does not concede to the appropriateness of such methods, in so far as they, to, do not provide actual evidence or specifics (other than prior convictions and failures to appear) regarding an indicidual defendant. [↑](#footnote-ref-28)
29. *See Bernstein v. U.S. Dep’t of State*, 974 F. Supp. 1288, 1292 (Cal. N. Dist. Ct. 1997). *See also* <https://en.wikipedia.org/wiki/Encryption> (accessed October 26, 2020). [↑](#footnote-ref-29)
30. 974 F. Supp. 1288 (affirmed by 9th Cir, then affirmation withdrawn, no new opinion issued due to statutory changes by the government, plaintiff then amended petition and returned to the N. Dist. CA attacking the new statutory scheme, which was denied for procedural reasons of timeliness and standing in *Bernstein v. DOC*, 2004 U.S. Dist. LEXIS 6672. The court’s earlier First Amendment analysis was undisturbed through the turbulent, subsequent appellate history). [↑](#footnote-ref-30)
31. *Id.* at 1293. [↑](#footnote-ref-31)
32. *Id.* at 1291. [↑](#footnote-ref-32)
33. *Id.* at 1310. [↑](#footnote-ref-33)
34. *Id.* 1293 [↑](#footnote-ref-34)
35. *Id.* [↑](#footnote-ref-35)
36. *Richmond Newspapers v. VA*, 448 U.S. 555, 599 n.2 (1980) *citing Kleindienst v. Mandel*, 408 U.S. 753 (1980) (affirming that the right to speak implies a freedom to listen). [↑](#footnote-ref-36)
37. *See Miranda v. Arizona*, 384 U.S. 436, 476 (1966) and *Rhode Island v. Innis*, 446 U.S. 291 (1980) (holding that the privilege against self-incrimination protects an accused from being compelled to incriminate himself in any manner, and does not distinguish degrees of incrimination). [↑](#footnote-ref-37)
38. *Kastigar v. U.S.*, 406 U.S. 441 (1972) (holding that The Fifth Amendment privilege against self-incrimination protects against any disclosures which the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used.) [↑](#footnote-ref-38)
39. *Doe v. U.S.*, 487 U.S. 201, 210-211 (1988) (stating that It is the "extortion of information from the accused," the attempt to force him "to disclose the contents of his own mind," that implicates the Self-Incrimination Clause). [↑](#footnote-ref-39)
40. 377 U.S. 201 (1964). [↑](#footnote-ref-40)
41. *People v. Gregor* (unpublished), 2018 Cal. App. Unpub. LEXIS 3306 *citing* *People v. Valdivia*, 16 Cal. App. 5th 1130, 1142 (2017) (finding a password surrender probation condition overbroad); *also citing* *People v. Appleton*, 245 Cal. App. 4th 717, 724 (2016) (same). [↑](#footnote-ref-41)
42. *People v. Valdivia*, 16 Cal. App. 5th 1130, 1144 (3rd Dist., 2017). [↑](#footnote-ref-42)