U.S. Department of Justice
Executive Office for United States Attorneys
United States Attorneys' USA Bulletin
March 2001 Vol. 49, No.2

Supervised Release and Probation Restrictions in Hacker Cases

Christopher M.E. Painter

USA Bulletin

(March 2001)

Christopher M.E. Painter
Deputy Chief, Computer Crime
and Intellectual Property Section

An often overlooked aspect of sentencing in computer crime cases are conditions that the court can impose as part of a sentence of probation or supervised release. These conditions can be tailored to restrict, among other things, a defendant's employment, associations, and other activities, once he is released from any term of imprisonment the court imposes to protect the public and aid in a defendant's rehabilitation. Such conditions are routinely imposed in non-computer crime cases. For example, in bank fraud cases or insurance fraud cases, courts often impose conditions restricting a defendant's employment in those industries. In investment fraud cases, defendants are prohibited from handling other people's money and in telemarketing cases, courts have prohibited defendants from soliciting investors, using names other than their own and have even restricted their access to telephones.

Appropriate restrictive supervised release conditions are even more important in hacker cases. In many hacker cases, the defendants have engaged in illegal conduct over a protracted period, are recidivists, or have otherwise demonstrated that they are unlikely to refrain from illegal hacking even after a conviction or imprisonment. In these cases, restrictive conditions that proscribe certain kinds of otherwise lawful conduct, such as use of aliases, association with other hackers, or, in extreme cases, access to computers and computer networks, serve to protect the public. This is particularly true when the sentence of imprisonment is either relatively short or where probation is imposed, despite the destructiveness of a defendant's conduct, or because the full extent of a defendant's activities is not determined. In other cases, particularly where the defendant is young, there is a good chance of rehabilitation. In these cases, supervised release or probation conditions can aid a defendant's rehabilitation by controlling or monitoring his access to those things that have tempted him in the past. In either case, appropriately tailored conditions can aid the probation office and the court in monitoring a defendant's conduct for the period of supervised release or probation to ensure he does not engage in further illegal conduct. If a defendant violates those conditions, the probation officer can seek revocation or modification of supervised release or probation and the court can impose additional imprisonment or refine the

restrictions on the defendant's conduct.

In general, in addition to certain mandatory conditions of supervised release, the court may order "any other condition it considers to be appropriate" so long as the conditions are "reasonably related" to the factors set forth in 18U.S.C. §§3553(a)(a), (1)(2)(B), (a)(2)(C), and (a)(2)(D). 18U.S.C. §3583(d). Specifically, conditions of the release must be reasonably related to the following factors:

• the nature and circumstances of the offense and the history and characteristics of the defendant; and
• the need for the sentence imposed – (B) ... to afford adequate deterrence to criminal conduct; (C)to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other corrective, treatment in the most effective manner. 18U.S.C. §3553.

See also United States Sentencing Guidelines ("U.S.S.G") §5D1.3(b). The probation statute, 18U.S.C. §3563, also allows the imposition of discretionary conditions that are related to "the need for the sentence imposed ... to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense," 18U.S.C. §3553(a)(2)(A), whereas the supervised release statute does not. *United States v. Eyer*, 67F.3d 1386, 1392 n.8 (9th Cir. 1995).

These conditions are not prerequisites, and a court may properly impose a condition of supervised release that is reasonably related to only some of these factors. *United States v. Johnson*, 998F.2d 696, 697-98 (9th Cir. 1993). The conditions must also involve no greater deprivation of liberty than is reasonably necessary for the purposes set forth above. 18U.S.C. §3583(d). Furthermore, the conditions must be consistent with pertinent policy statements issued by the Sentencing Commission. *Id.* In setting conditions, including those "restricting fundamental rights," the sentencing court has broad discretion. *United States v. Bolinger*, 940F.2d 478, 480-81 (9th Cir. 1991).

U.S.S.G. §5F1.5 allows a court to impose a condition of supervised release restricting employment in a specified occupation, business, or profession if it determines that:

• a reasonably direct relationship existed between the defendant's occupation, business, or profession and the conduct relevant to the offense of conviction; and
• imposition of such a restriction is reasonably necessary to protect the public because there is reason to believe that, absent such restriction, the defendant will continue to engage in unlawful conduct similar to that for which the defendant was convicted.

That section also states that "[i]f the court decides to impose a condition of probation or supervised release restricting a defendant's engagement in a specified occupation, business, or profession, the court shall impose the condition for the minimum time and to the minimum extent necessary to protect the public." *Id.*

The range of permissible discretionary conditions a court can impose is exceptionally broad and permits a wide range of restrictions depending on the facts of an individual case and the history

and prospects of the defendant. In a first-time hacker case, the restrictions could be as simple as a prohibition against unauthorized use of computer systems, a prohibition against association with others who have engaged in illegal hacking activities, and a directive that defendant use his own name when communicating online. On the other side of the spectrum, much broader conditions may be warranted.

For example, in the prosecution of the prolific and notorious computer hacker Kevin Mitnick, the court imposed the following conditions as part of his sentence:

Without the prior express written approval of the probation officer:

• The defendant shall not possess or use, for any purpose, the following:

• Any computer hardware equipment;
• Any computer software programs;
• Modems;
• Any computer related peripheral or support equipment;
• Portable laptop computers, "personal information assistants," and derivatives;
• Cellular telephones;
• Televisions or other instruments of communication equipped with on-line, Internet, world-wide web, or other computer network access;
• Any other electronic equipment, presently available or new technology that becomes available, that can be converted to or has as its function the ability to act as a computer system or to access a computer system, computer network or telecommunications network (except defendant may possess a "land line" telephone);

• The defendant shall not be employed in or perform services for any entity engaged in the computer, computer software, or telecommunications business and shall not be in any capacity wherein he has access to computers or computer-related equipment or software;
• The defendant shall not access computers, computer networks, or other forms of wireless communications himself or through third parties;
• The defendant shall not act as a consultant or advisor to individuals or groups engaged in any computer-related activity;
• The defendant shall not acquire or possess any computer codes (including computer passwords), cellular phone access codes, or other access devices that enable the defendant to use, acquire, exchange, or alter information in a computer or telecommunications database system;
• The defendant shall not use or possess any data encryption device, program or technique for computers;
• The defendant shall not alter or possess any altered telephone, telephone equipment, or any other communications-related equipment;
• The defendant shall only use his true name and not use any alias or other false identity.

These conditions that both restrict defendant’s access to computers, computer networks, and cellular phones and restrict his employment in the computer or telecommunications industries, were justified and necessitated by defendant’s habitual hacking activities and long history of failing to obey court-ordered restrictions on his conduct. Mitnick engaged in criminal hacking

and telecommunications fraud from the time he was a juvenile. In 1988, after several state convictions and revocations of probation for computer fraud, defendant was charged and pled guilty in federal court for hacking into Digital Equipment Corporation computers, stealing proprietary software, and using unauthorized access devices. He was sentenced to twelve months in prison followed by a three year period of supervised release. The judge imposed straightforward conditions of supervised release prohibiting Mitnick from engaging in further illegal access into computer or telecommunications networks and prohibiting him from associating with others known to have engaged in such conduct. Nevertheless, near the end of his supervised release term, Mitnick hacked into Pacific Bell voice mail computers and associated in this endeavor with another individual (and later co-conspirator) who had previously been convicted of computer fraud.

A warrant was issued for Mitnick's arrest and he fled, becoming a fugitive for the next two and one half years. During this time, Mitnick engaged in a virtual "hacking spree" gaining unauthorized access to dozens of computer networks using cloned cellular phones to hide his location and, among other things, stealing valuable proprietary software from some of the country's largest cellular telephone and computer companies. Mitnick also intercepted and stole computer passwords, altered computer networks, and broke into and read private e-mail. Mitnick was apprehended in February 1995 in North Carolina. When arrested he was found with cloned cellular phones, over one hundred clone cellular phone codes, and multiple pieces of false identification.

In imposing the extensive conditions of supervised release, the judge held a number of hearings and based her ruling on defendant's long history of hacking, defendant's inability to comply with less onerous restrictions and, most importantly, the need to protect the public. The court's focus on the "tools" Mitnick has habitually used to commit past criminal conduct, computer and cellular phones, was wholly appropriate given defendant's seeming inability to use these tools in a law-abiding manner. Given his past extensive and repeated criminal conduct, and the prospect that, unsupervised, he would be tempted to engage in the conduct again, the court expressly stated that the conditions were designed to protect the community. The court's occupational restrictions prohibiting his employment in the computer and telecommunications industries were similarly designed primarily to protect the public from future illegal conduct by removing both the tools Mitnick could use to commit this conduct and the tools that might tempt him to further transgressions.

Of course, conditions as broad as the ones imposed in the *Mitnick* case must be justified by the facts of the case at issue. If such conditions are justified by a defendant's history and the nature of the offense, and if the judge makes an adequate record to support his or her findings, they should survive any challenge raised on appeal. Common challenges to conditions of supervised release restricting a defendant's association and activities are that such restrictions impermissibly restrict otherwise legal activities, that they violate the defendant's First Amendment rights, or are impermissibly vague or ambiguous. Mitnick challenged the conditions imposed by the court on each of these grounds but was flatly rejected by the Ninth Circuit Court of Appeals. *United States v. Kevin Mitnick*, No. 97-50365, 1998 WL255343 (9th Cir. May 20, 1998).

The argument that broad supervised release conditions restrict otherwise lawful activity misses

the point. Courts have frequently curtailed activities that, though otherwise legitimate, nevertheless might tempt a defendant to engage in further illegal conduct. *See United States v. Lowe*, 654F.2d 562, 566 (9th Cir. 1981) (court could properly restrict access within 250 feet of military base, thereby effectively precluding legitimate leafleting activity, to remove temptation of separate criminal conduct – trespassing on base); *United States v. Bolinger*, 940F.2d 478, 480 (9th Cir. 1991) ("Probation conditions may seek to prevent reversion into former crime-inducing lifestyle by barring contact with old haunts and associates, even though the activities may be legal"); *United States v. Peete*, 919F.2d 1168, 1181 (6th Cir. 1990) (proper to prohibit defendant convicted of violating Hobbs Act from running for public office to insulate him from temptation of same environment and protect the public); *United States v. Turner*, 44F.3d 900, 903 (10th Cir. 1995), (court properly ordered defendant not to picket abortion clinics because "it is not too fantastic to speculate that if she were permitted to protest at an abortion clinic she might not be able to restrict her activities within lawful parameter"); *United States v. Choate*, 101 F.3d 562, 566 (8th Cir. 1996) (defendant properly prohibited from self-employment because of risk that prior "excesses of salesmanship" could again lead to illegal conduct if not supervised).

In *Malone v. United States*, 502F.2d 554 (9th Cir. 1974), defendant was convicted of unlawful exportation of firearms to Ireland and, as part of his sentence, was ordered not to associate with, or belong to, any Irish organization, group, or movement, not to be employed in any capacity that directly or indirectly associated him with such groups and not to visit any Irish pubs. *Id.* at 555. In upholding these restrictions, the court recognized that the incidental chance of temptation warranted these conditions despite their usually lawful character:

The conditions here involved are not intended to infer that each member of a group or organization with which the appellant is forbidden to associate will necessarily lead him into criminal activities or be a bad influence. It is the incidental association with one or more who might lead him to future criminality that the court seeks to prevent. If the trial judge could only prohibit active association with a group having an illegal purpose, then the court would be, in effect, restricted to the standard condition that the probationer obey the law. It does not appear such limitation was intended. Here the crime stemmed from high emotional involvement with Irish Republic sympathizers.

Id at 556.

Challenges based on an impermissible restriction of a defendant's rights of expression or association should be similarly unavailing. Despite the growing importance of the Internet as a means of communication, restrictions on access to that technology are proper if related to and reasonably necessary to promote the goals of sentencing. It is axiomatic that those convicted of criminal conduct are "properly subject to limitations from which ordinary citizens are free[.]" *United States v. Consuelo-Gonzalez*, 521F.2d 259, 265 (9th Cir. 1975). Accordingly, the district court retains its broad discretion in setting conditions of supervised release and probation, even where fundamental rights are involved. *Bolinger*, 940F.2d at 480. Although conditions restricting fundamental rights are reviewed carefully, *Lowe*, 654F.2d at 567, there is no "presumption, however weak, that such limitations are impermissible". *Consuelo-Gonzalez*, 521F.2d at 265. As the Ninth Circuit stated in *Consuelo-Gonzalez*:

Merely because a convicted individual's fundamental rights are involved should not make a probation condition which limits those rights automatically suspect. The development of a sensible probationary system necessarily requires that the trial court be vested with broad discretionary powers. It also requires that any condition which is imposed following conviction, whether or not it touches upon "preferred" rights, must be viewed in the context of the goals underlying the Act. Thus, the crucial determination in testing probationary conditions is not the degree of "preference" which may be accorded those rights limited by the condition, but rather whether the limitations are primarily designed to affect the rehabilitation of the probationer or insure the protection of the public.

Consuelo-Gonzalez, 521F.2d at 265 n.14. The restriction of even "preferred rights" is valid so long as they are: "(1)primarily designed to meet the ends of rehabilitation and protection of the public and (2)reasonably related to those ends." *Bolinger*, 940F.2d at 480. Like any other special condition of supervised release, such conditions also must involve no greater deprivation of liberty than is reasonably necessary. 18U.S.C. §3583(d).

Courts have routinely deferred to the sentencing court's broad discretion in setting conditions notwithstanding the implication of fundamental rights. *See, e.g., Malone*, 502F.2d at 556 (upholding restrictions limiting association with all Irish groups against First Amendment claim); *Lowe*, 654F.2d at 566-67 (upholding conditions that effectively precluded defendants from distributing literature to employees of military base or attend certain weekly meetings against free speech and association claim); *Peete*, 919F.2d at 1118 (prohibition on holding public office upheld); *United States v. Bird*, 124F.3d 667, 684 (5th Cir. 1997) (rejecting First Amendment challenge to condition that defendant stay 1,000 feet away from abortion clinics where he had previously been convicted for trespassing at abortion clinics); *United States v. Showalter*, 933 F.2d 573, 575 (7th Cir. 1991) (conditions upheld requiring the defendant convicted of possession of unregistered firearm to avoid associating with other skinheads and neo-Nazis).

As long as restrictions are reasonably related to the offense and defendant's history, are primarily designed to protect the public and promote rehabilitation by preventing recidivism, are expressly related to those ends, and particularly in light of defendant's past conduct, involve no greater deprivation of liberty than is reasonably necessary to achieving those ends, they should survive a First Amendment challenge.

A final likely claim is that broad conditions restricting access to computers are fatally vague and overbroad. Mitnick, for example, argued that because almost everything from automobiles to ATMs and toasters include computer chips, he would be forced to live as a hermit or commit unintentional violations of supervised release. Both the District Court and Court of Appeals rejected this argument stating that conditions restricting computer access should be read in a common sense manner. Although due process requires a defendant to be given fair warning before he forfeits his liberty, *see United States v. Grant*, 816F.2d 440, 442 (9th Cir. 1987).

[f]air warning is not to be confused with the fullest or most pertinacious, warning imaginable. Conditions of probation do not have to be cast in letters six feet high, or to describe every possible permutation, or spell out every last self-evident detail [they] may afford fair warning

even if not precise to the point of pedantry. In short, conditions of probation can be written – and must be read in a common sense way.

United States v. Gallo, 20F.3d 7, 11 (1st Cir. 1994). (internal citations omitted)

The scope and detail of supervised release restrictions in hacker cases will be highly dependent on the facts of the particular case and the history of the defendant. Nevertheless, prosecutors should be aware these conditions can be used as a powerful tool to protect the public and aid in rehabilitation. Accordingly, prosecutors should consider appropriate conditions when negotiating a plea agreement or in arguments presented during sentencing proceedings.

ABOUT THE AUTHOR

Christopher M.E. Painter is a Deputy Chief of the Computer Crime and Intellectual Property Section at the Department of Justice. From 1991 to March 2000, Mr. Painter was a criminal prosecutor in the U.S. Attorney's Office for the Central District of California (Los Angeles). Since taking that post, Mr. Painter specialized in the investigation and prosecution of high-tech, intellectual property and computer crimes and served as a Computer Crime and Internet Fraud Coordinator for his office.
Mr. Painter has investigated and prosecuted some of the most significant and high profile high-tech cases in the country, including the prosecution of notorious computer hacker Kevin Mitnick, the prosecution of the first Internet stock manipulation case involving the posting of a bogus Bloomberg News page falsely reporting the sale of a company called PairGain that caused its stock to soar, prosecution of another internet stock manipulation case, involving former and present UCLA students who hyped stocks on Yahoo by posting false spam messages, and the prosecution of one of the first Internet auction fraud cases. Mr. Painter co-chairs an ABA subcommittee concerning high-tech crimes and serves on several Department of Justice and interagency working groups relating to computer and Internet hackers, Internet fraud investigations and prosecutions, electronic evidence, intellectual property crimes, and thefts of trade secrets. He has frequently lectured to private groups and at the National Advocacy Center, appeared on 60 Minutes, CNN, CBS Morning News, the BBC, and has testified before Congress concerning computer crime issues.

###