AELE Monthly Law Journal

ISSN 1935-0007
Cite as: 2015 (6) AELE Mo. L. J. 301
Jail & Prisoner Law Section – June 2015

Prisoners, Parolees, Sex Offenders, Computers, and the Internet

Part 1 (Last Month)

- **Introduction**
- **Access to Computers**
- **Information from the Internet**
- **Federal Prison Electronic Messaging System**

Part 2 (This Month)

- **Supervised Internet Access**
- **Cell Phones and the Internet**
- **Parolees and the Internet**
- **Sex Offenders and the Internet**
- **Some Suggestions**
- **Resources and References**

This is a two-part article. To read Part 1, click here.

❖ Supervised Internet Access

Many states have statutory or administrative restrictions or bans on unrestricted Internet access by prisoners, which vary widely. Ohio's Administrative Rule 5120-9-51 (1-12-2010) is an example, and prohibits prisoner access unless "the prisoner is under direct supervision and is participating in an approved educational program that requires the use of the Internet for training or research purposes."

The rule spells out criteria for prisoners to be screened and approved (or denied) for participation in supervised access, which may be for "academic, vocational, release preparation, apprenticeship, advanced employment and training, and service learning programs."

A small number of states (including Ohio, Florida, Louisiana, Virginia, Michigan, North Dakota, Washington, and Georgia) and some localities have been experimenting with

programs that allow some prisoners to buy and use $49.99 mini-tablet computers to communicate with families via monitored e-mails as well as listen to music. The messages are monitored at the individual correctional facility. See "Some prisons let inmates connect with tablets," by Kimberly Railey, USA Today (August 2, 2013).

Similarly, a two year experimental pilot program at San Francisco's jail involving 100 prisoners, which is also now being carried out at a jail in Los Angeles, provides participating inmates with digital tablets that they have with them for most of the day, but which can only access four secure websites, including a law library and education program.

Jail authorities retain the ability to deactivate the tablets at any time, and their function is focused on education and training. Those promoting the program also argue that some prisoners' lack of familiarity with the Internet can be a major hurdle to finding both jobs and services upon reentering society.

Additionally, the states of Iowa, Oklahoma, and Minnesota currently make available to some prisoners a closed and monitored electronic messaging system operated by Corrlinks, the same private company which operates the monitored electronic messaging system available to federal prisoners.

In England, a report in 2013 by the private Prison Reform Trust and Prisoners Education Trust recommended giving some prisoners controlled and "fully supervised" and monitored access to the Internet, contending that this could help with rehabilitation**,** job training, maintaining family ties, and cutting down on recidivism.

❖ Cell Phones and the Internet

For years, there has been a plague of smuggling cell phones into prisons and jails, and they are among the mostly highly sought items of contraband. Today's cell phones are capable of far more than simply voice communication, as many are now smart phones able to send and receive text messages, e-mail, photographs, and even video, as well as to access the Internet generally. See "Outlawed, Cellphones Are Thriving in Prisons," by Kim Severson and Robbie Brown, New York Times, January 2, 2011.

Gang members have in some instances used them to continue to direct violence and drug trafficking from behind bars, and some prisoners run Facebook pages or Twitter accounts, and have been known to stalk and harass former victims, or to coordinate work stoppages with inmates at other prisons.

In California, even notorious murderer Charlie Manson was found in possession of a cell phone in his cell. This is despite their use being unlawful for prisoners in all state and

federal prisons in the U.S., subjecting prisoners to a variety of possible punishments, including loss of good time or even, in some instances, criminal charges.

The article reports that in the first four months of 2010 alone, federal prisons in the U.S. confiscated 1,188 cell phones. That same year, California correctional officers found almost 9,000 illegal cell phones in state facilities.

In some instances, correctional facilities have deployed technology to detect unauthorized cell phone calls and texts. In one Mississippi state facility, this resulted in the interception of 643,388 calls and texts in a six month period from a population of 3,000 prisoners.

The problem with jamming technology, however, according to the FCC, is that "cell phone jamming doesn't just block inmate calls – it can also interfere with mobile 9-1-1 calls and public safety communication. That raises serious concerns for national public safety organizations like the National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO)."

The FCC takes the position that jamming or blocking mobile calls is illegal, but it has worked with state correctional officials, federal partners, and wireless carriers to try to find new technologies that can serve as solutions, such as inmate call capture that can reject unauthorized calls while preserving public safety communications, and allows and passes through all 9-1-1 and authorized calls. See FCC handout "Putting an end to illegal cell phone use in prisons." Technology to accomplish this, however, may be expensive. See also Mobile phones in prison, Wikipedia.

❖ Parolees and the Internet

Given both the overcrowded conditions of many correctional facilities and the interest in reintegrating ex-offenders into society and encouraging them to become productive members of the community, many convicted prisoners who have not served their entire sentence are granted parole.

In exchange, it is clear, authorities have a legal right to impose a wide variety of restrictions on their conduct, such as prohibiting fraternization with former criminal associates, compelling consent to home inspections, drug testing, etc.

In instances where an offender has in the past used a computer and the Internet as an integral part of a criminal scheme, or in which the nature of their past crimes, such as sexual offenses, raise special concerns about predatory conduct, parole authorities or courts allowing periods of supervised release have imposed restrictions on access to the Internet. Some courts have cautioned that such restrictions should be carefully tailored to prevent the feared harm, and not prevent legally protected conduct.

In *U.S. v. Crume*, #04-3181, 422 F.3d 728 (8th Cir. 2005), for instance, the court vacated a broad ban on computer and Internet access without prior approval when the defendant never "used his computer for anything beyond simply possessing child pornography." The court stated that it was "not convinced that a broad ban from such an important medium of communication, commerce, and information-gathering is necessary given the absence of evidence demonstrating more serious abuses of computers or the Internet."

The court suggested imposing a more narrowly tailored restriction on computer use through a prohibition on accessing certain categories of websites and Internet content and ensuring compliance with some combination of random searches and software that filters objectionable material.

In *U.S. v. Phillips*, #14-2118, 2015 U.S. App. Lexis 7399 (8th Cir.), a man who previously pled guilty to statutory rape was sentenced to 24 months' imprisonment and 10 years supervised release for failing to register as a sex offender. When he violated his release conditions through admitted unsupervised contact with minors, he was sentenced to 24 months imprisonment and lifetime supervision.

As a special release condition, he was told that he could not "possess or use . . . a computer . . . gaming equipment, cellular devices, or any other device with access to any 'on line computer services,' or subscribe to or use any Internet service . . . without the written approval of the probation office."

A federal appeals court vacated that special condition. The court below premised the broad ban on computer use and Internet access on the offender's possession of adult (not child) pornography, including pictures of his own penis, and his statutory rape conviction.

> "Because possessing child pornography may not necessarily justify a broad ban on Internet access, Crume, 422 F.3d at 733, a court exceeds its discretion under §3583(d) by banning Internet access for possessing adult pornography."

On remand, the court stated, lesser restrictions on his Internet access may be consistent with the federal sentencing statute 18 U.S.C. Sec. 3583(d), dealing with special conditions of supervised release. "When crafting a special condition of supervised release, the district court must make an individualized inquiry into the facts and circumstances underlying a case and make sufficient findings on the record so as to ensure that the special condition satisfies the statutory requirements."

In contrast with this case, see *U.S. v. Munjak*, #11-2058, 669 F.3d 906 (8th Cir. 2012) where a prior-approval Internet ban was acceptable because the defendant did more than possess child pornography—he used a computer to distribute it. In accord is *U.S. v. Stults*,

#08-3183, 575 F.3d 834 (8th Cir. 2009), upholding a prior approval Internet ban (with an exception for employment use) where the defendant distributed child pornography.

Courts have appeared far more willing to impose an Internet ban on offenders who used the Internet to perpetrate a fraud like a telemarketing scheme, investment fraud, or computer hacking. See, *U.S. v. Mitnick*, #97-50365, 145 F.3d 1342, 1998 U.S. App. Lexis 10836 (9th Cir. 1998), *U.S. v. Keller*, #08-3549, 366 Fed. Appx. 362 (Unpub. 3d Cir. 2010), and *U.S. v. Suggs*, #01-6080, 50 Fed. Appx. 208 (Unpub. 6th Cir. 2002).

❖ Sex Offenders and the Internet

The concern over the possibility of those who have committed sex offenses, especially although not exclusively those involving minors, have resulted in a wide variety of restrictions on persons subject to registration as sex offenders, restrictions that last long beyond serving sentences of incarceration or even beyond periods of parole.

Because the Internet can and has been used to facilitate a variety of sexual crimes, it is hardly surprising that there have been legislative and administrative attempts to reign in registered sex offenders' use of the Internet. In a number of instances, however, federal courts have cautioned against going too far in this regard by enacting overly broad restrictions.

In *Doe v. Prosecutor, Marion County*, #12-2512, 705 F.3d 694 (7th Cir. 2013), the court found that an Indiana state statute that broadly prohibited most registered sex offenders from using instant messaging services, social media sites and chat programs that allowed users younger than 18 violated their First Amendment rights.

While the state justifiably wished to protect children from inappropriate sexual communication, and the law was content neutral, the law placed a burden on more speech than was necessary to achieve that purpose.

The court stated that a sex offender's use of social media was not dangerous as long as they did not engage in improper communication with minors. Such communication was a tiny subset of the "universe of social media." The state could have, without substantial difficulty, more precisely targeted the evil it wanted to prevent, the court believed.

Similarly, in *Doe v. State of Nebraska*, #8:09CV456, 898 F. Supp. 2d 1086 (D. Neb. 2012), a federal trial court has struck down a Nebraska state law barring registered sex offenders from using the Internet for most purposes, including social media. The court said that by severely limiting "even benign" uses of the Internet, the law raised First Amendment, due process, Fourth Amendment, and ex post facto issues. The law, the judge found, did not leave open ample alternative channels for communication of information.

A portion of the statute that applied to those registered as sex offenders but who were not on probation, parole, or court monitored supervision violated the Fourth Amendment. The court said the law wrongly bars offenders "from using an enormous portion of the Internet to engage in expressive activity," and "potentially restricts the targeted offenders from communicating with hundreds of millions and perhaps billions of adults and their companies despite the fact that the communication has nothing whatsoever to do with minors."

Further, the law "is not narrowly tailored to target those offenders who pose a factually based risk to children through the use or threatened use of the banned sites or services. The risk posited by the statute is far too speculative when judged against the First Amendment."

In *Doe v. Harris*, #13-15263, 772 F.3d 563 (9th Cir. 2014), a federal appeals court upheld a preliminary injunction granted to plaintiff registered sex offenders who asserted that the Californians Against Sexual Exploitation Act (CASE Act) infringed their freedom of speech in violation of the First Amendment. The law was found to impose a substantial burden on sex offenders' ability to engage in legitimate online speech, and to do so anonymously.

The law required the offenders, among other things, to provide "[a] list of any and all Internet identifiers established or used by the person" and "[a] list of any and all Internet service providers used by the person."

The appeals court agreed that registered sex offenders who have completed their terms of probation and parole enjoy the full protection of the First Amendment. The panel then held that because the Act imposes a substantial burden on sex offenders' ability to engage in legitimate online speech, and to do so anonymously, First Amendment scrutiny was warranted.

Applying intermediate scrutiny, the court found that the Act unnecessarily chilled protected speech in at least three ways:

(1) it did not make clear what sex offenders are required to report;

(2) it provided insufficient safeguards preventing the public release of the information sex offenders do report; and

(3) the requirement of reporting within 24-hour the adding or changing of an Internet identifier or an account with an Internet service provider was onerous and overbroad.

This brief article cannot address in depth all the various restrictions that courts and agencies have attempted to impose upon registered sex offenders' online activities.

Additionally, various social media sites have, in some instances, decided to impose their own restrictions via their terms of service agreements.

The point of this section of the article, however, is to make it clear that attempts to impose a broad blanket ban on all online activity by registered sex offenders, especially those no longer on parole, has increasingly resulted in scrutiny by the courts, a trend only likely to continue because of the extent to which use of computers and the Internet is now an integral part of so many aspects of daily life in the U.S.

❖ Some Suggestions

With the widespread integration of computers and the Internet into almost every area of modern life, including education, commerce, banking, job hunting, and personal communication, there are bound to be increasing pressures for prisons and jails to allow some forms of electronic communication and Internet access.

This is a complicated area in which there is much to learn from creative experimentation followed by the summing up of experience. The federal prisons' monitored electronic messaging system for prisoners is the most widespread and well thought out such attempt to date, but a number of experiments being conducted by state and local agencies also bear watching.

The following are just a few suggestions to consider:

1. The more closely that electronic messaging systems and Internet access can be supervised and monitored, the better. Special proprietary systems have much to offer, because ordinary personal computers, even with selective filtering software, can all too easily be "hacked" by an increasing number of technologically sophisticated persons.
2. The use of monitored electronic messaging systems has the potential to cut down greatly on the burden of screening of physical mail, and cannot be used for the smuggling of contraband. For that reason, their use should be encouraged.
3. The presence of smuggled contraband cell phones, including smart phones, is a continuing serious threat to institutional security, and there is a need for further technological, legislative and regulatory efforts in this area.
4. Restrictions on the use of computers and the Internet by parolees and sex offenders must be carefully thought out and narrowly tailored to ensure that they serve their intended goal of deterring the use of technology to commit further crimes, while not being overly broad and thus limiting legitimate protected First Amendment activity.

5. The available case law seems to indicate that the courts are more willing to uphold broader restrictions on those offenders and ex-offenders for whom the use of technology and the Internet was an integral part of their crimes.

❖ Resources

The following are some useful resources related to the subject of this article.

- Computers, E-mail, & Internet Issues. AELE Case Summaries.
- Corrlinks. Wikipedia article.
- Internet in Prisons. Wikipedia article.
- Trust Fund Limited Inmate Computer System (TRULINCS) – Electronic Messaging, Federal Bureau of Prisons Program Statement P5265.13 (February 19, 2009).

❖ Prior Relevant Monthly Law Journal Articles

- Prisoner Mail Legal Issues, 2007 (6) AELE Mo. L.J. 301.
- Prisoners and Sexually Explicit Materials, 2010 (2) AELE Mo. L. J. 301.
- Legal Issues Pertaining to Inmate Telephone Use, 2008 (2) AELE Mo. L.J. 301.

❖ References: (*Chronological*)

1. The Case for Internet Access in Prisons, by Ben Branstetter, The Washington Post, (February 9, 2015).
2. With No Google, the Incarcerated Wait for the Mail, by Max Kutner, Newsweek (January 25, 2015).
3. Inside the prison system's illicit digital world, Part 1, Part 2, Part 3, by Kevin Roose and Pendarvis Harshaw, Fusion (February 3, 4, and 5, 2015).
4. How to Use CorrLinks to E-mail Federal Prisoners for Free, HubPages (September 27, 2014).
5. Wrong Number: Contraband Cellphones are Major Problem at Oklahoma Prisons, by Andrew Knittle and Nolan Clay, Oklahoman (September 22, 2013).
6. Through The Gateway: How Computers Can Transform Rehabilitation, by Nina Champion and Kimmett Edgar, Prison Reform Trust and Prisoners Education Trust, UK (2013).

7. Improved Evaluations and Increased Coordination Could Improve Cell Phone Detection, Federal Bureau of Prisons, U.S. Government Accountability Office (GAO) (September 6, 2011).
8. Note: MySpace, Yourspace, But Not Theirspace: The Constitutionality of Banning Sex Offenders From Social Networking Sites, by Jasmine S. Wynton, 60 Duke Law J. 1859 (May 2011).
9. Computer Use for/by Inmates, Corrections Compendium (June 22, 2009).
10. Protecting the Playgrounds of the Twenty-First Century: Analyzing Computer and Internet Restrictions for Internet Sex Offenders, by Krista L. Blaisdell, 43 (3) Valparaiso University Law Rev. 1155-1210 (Spring 2009).
11. Access Denied: Imposing Statutory Penalties on Sex Offenders Who Violate Restricted Internet Access as a Condition of Probation, by Jane Adele Regina, 4 Seton Hall Circuit Review 187 (2007).
12. An Introduction to the Supervision of the Cyber Offender, by Art Bowker and Michael Gray, 68 Federal Probation No. 3 (Dec. 2004).

AELE Monthly Law Journal

Bernard J. Farber
Jail & Prisoner Law Editor
P.O. Box 75401
Chicago, IL 60675-5401 USA
E-mail: bernfarber@aele.org
Tel. 1-800-763-2802

- The purpose of this publication is to provide short articles to acquaint the reader with selected case law on a topic. Articles are typically six to ten pages long. Because of the brevity, the discussion cannot cover every aspect of a subject.
- The law sometimes differs between federal circuits, between states, and sometimes between appellate districts in the same state. AELE Law Journal articles should not be considered as "legal advice." Lawyers often disagree as to the meaning of a case or its application to a set of facts.

AELE Home Page – Publications Menu – Seminar Information

This article appears in the IACP Net database.