AELE Monthly Law Journal

ISSN 1935-0007
Cite as: 2015 (5) AELE Mo. L. J. 301
Jail & Prisoner Law Section – May 2015

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

Part 1 (This Month)

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

Part 2 (Next Month)

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

❖ Introduction

The issues of computer use, e-mail and electronic messaging, and information from and access to the Internet in jails and prisons are increasingly discussed. Since 2009, federal prisons throughout the country have developed their own text only electronic messaging system, the Trust Fund Limited Inmate Computer System (TRULINCS) for inmate and public use, and a number of state correctional systems and local correctional facilities have experimented with allowing prisoners limited supervised access to the Internet or portions of it for a variety of purposes, including education, vocational training, job search prior to release, legal research, or communication with family.

Mobile phones smuggled into correctional facilities may have access to the Internet, causing a host of problems. With the ubiquity of computers and the Internet in contemporary society, this is an arena that is almost certain to grow, raising a host of both legal and practical issues for correctional management, including First Amendment issues,

protection of the public and particularly crime victims from potential harassment, and institutional security.

As prisoners get released into the community through parole or probation, their opportunities to access all aspects of the Internet are obviously greatly expanded, raising a variety of concerns, including preventing computer crime, fraud, harassment, and misuse of social media. Courts have addressed, in a small but growing number of cases, attempts to limit these problems through restrictive parole or probation conditions.

Those who have committed sex crimes resulting in lifetime registration as sex offenders are of special concern in this regard, and courts have seen an increasing number of legal challenges to attempts to bar them from the Internet and electronic communication, including use of social media.

This two-part article takes a brief look at these issues and developments. In Part 2, some suggestions to consider are presented, along with a listing of useful and relevant resources and references.

❖ Access to Computers

Some prisoners have sought the possession and use of personal computers in correctional facilities. Some courts have upheld prison policies that have completely barred or severely restricted such possession and use of even computers lacking Internet access.

In *West Virginia, ex rel. Anstey v. Davis*, #25155, 509 S.E.2d 579 (W. Va. 1998), the West Virginia Supreme Court upheld a state policy barring prison inmates from possessing computers in their cells. It easily found that a prior practice of allowing such possession did not create any vested right to continue to possess them, and that deprivation of computer possession did not result in the denial of meaningful access to the courts.

In cases where prison officials have allowed possession and use of computers in connection with prisoner's legal needs, access to the courts issues can arise. In *Newell v. Sauser*, #94-35243, 79 F.3d 115 (9th Cir. 1996), for instance, a federal appeals court ruled that an Alaska state inmate and prison law librarian, who had been allowed a computer in his cell by prison officials, had a right to aid a mentally retarded inmate in preparing legal documents.

- Prison employees were not entitled to qualified immunity for seizing legal documents from the law librarian's cell and disciplining him for possessing them.

In *Bryant v. Muth*, #91-6672, 994 F.2d 1082 (4th Cir. 1993), *cert. denied*, #93-5842, 510 U.S. 996 (1993), on the other hand, the Fourth Circuit held that a federal prisoner's rights

were not violated by the confiscation of unauthorized computer disks on which he had placed legal materials pertaining to his appeal. In that instance, the prisoner was not allowed to possess the disks or use prison computers, so prison authorities properly confiscated the disks.

Prisoners allowed possession or use of computers or other electronic devices who abuse such privileges can quickly lose them. In *Williams v. Revlon Co.*, #93 Civ. 4837, 156 F.R.D. 39 (S.D.N.Y. 1994), a federal trial judge, hoping to make the "message" clear to prisoner who filed multiple frivolous lawsuits, confiscated any computer, word processor or typewriter the prisoner had, as well as imposing a $5,000 monetary sanction (to be collected by attachment of prisoner's commissary funds and future prison earnings), and ordered that the prisoner state, on the outside of each envelope of outgoing mail, that he has been "enjoined from asserting fraudulent personal injury claims."

Similarly, in *Jensen v. Powers*, #910079, 472 N.W.2d 223 (N.D. 1991), a court found that a warden's decision to deprive a prisoner of his television set and personal computer because of his refusal to sign an "individual performance plan" agreeing to keep himself and cell clean did not violate the prisoner's rights.

❖ Information from the Internet

In a number of instances, prisons have attempted to limit the access of prisoners to information whose source was the Internet, when received as printouts through regular prison mail. Some courts have struck these restrictions.

In *Clement v. California Department of Corrections*, #03-15006, 364 F.3d 1148 (9th Cir. 2004), a California prison ban on mail containing printed-out downloads from the Internet was held to violate the First Amendment. The policy, adopted in 2001, provided, "No Internet Mail. After reviewing staffing levels and security issues [I]nternet mail will not be allowed. To do so would jeopardize the safety and security of the institution."

The policy prohibited only mail containing material that has been downloaded from the Internet but was not violated if the information from the Internet was retyped or copied into a document generated in a word processor program. Further, the policy prohibited photocopies of downloaded Internet materials, but not of non-Internet publications. The prison at Pelican Bay allegedly received at most 500 pieces of mail containing Internet materials, the court stated, out of 300,000 total letters per month.

The appellate panel agreed with the trial court that prison officials had failed to show a rational or logical connection between the policy and its legitimate security interests. The prison officials had argued that permitting the receipt of materials downloaded from the

Internet would drastically increase the volume of mail that the prison had to process and that it would be easier to insert coded messages into Internet material than into photocopied or handwritten material and that Internet communications are harder to trace than other, permitted communications.

> "Prohibiting all Internet-generated mail is an arbitrary way to achieve a reduction in mail volume. [...] CDC did not support its assertion that coded messages are more likely to be inserted into Internet-generated materials than word-processed documents."

The appellate panel noted that while the injunction prohibited banning Internet materials simply because their source is the Internet, "it does not prohibit restrictions for any legitimate penological or security reason," such as imposing page limitations, "or a ban on recipes for pipe-bombs."

On the other hand, a state appellate court in an earlier case, *In re Collins*, #A090799, 86 Cal. App. 4th 1176, 104 Cal. Rptr. 2d 108 (2001), had held that a California prison rule prohibiting the receipt, through the U.S. mail, of Internet generated material, including e-mail, was rationally related to a prison's legitimate security concerns. The appeals court overturned an order allowing the prisoner to receive printouts of e-mails sent to his own Internet web page, created via an arrangement with an outside company.

The private company in the case, *Inmate Classified,* was in the business of publishing personal web pages on the Internet for prison inmates who subscribed to its service. Each inmate's page included an individual electronic (e-mail) address, and *Inmate Classified* periodically downloaded and printed any e-mail messages received by the inmate subscriber and sends them to the inmate by regular United States mail.

The case involved solely personal messages sent by members of the public to a specific inmate. One concern was the difficulty of identifying the identity of those sending the messages, given the ease in which anonymous or disguised identities can be used to transmit e-mail.

Similarly, in *Canadian Coalition Against the Death Penalty v. Ryan*, #02-1344, 269 F. Supp. 2d 1199 (D. Ariz. 2003), a federal court struck down as unconstitutional an Arizona statute prohibiting prisoners from communicating with Internet websites through the mail or otherwise or receiving mail from them.

The court found that the prohibition was not reasonably related to a legitimate penological purpose, and that other statutes and policies already prohibit communication involving fraud, harassment of victims, communication with minors, and other purported purposes of the ban on communication with Internet service providers.

Although prison authorities are permitted to establish regulations in anticipation of potential problems, "they must at a minimum supply some evidence that such potential problems are real, not imagined."

❖ Federal Prison Electronic Messaging System

It is obvious why prisoners cannot be granted unsupervised access to general Internet e-mail. While e-mail and other electronic messaging is probably now the most widely used form of public communication, long ago surpassing what is derisively called "snail mail" (letters sent through the postal system) for both personal and business communication, the problems accompanying prisoner access include the potential for financial fraud, harassment of crime victims, communication with criminal associates in the outside world, the hatching of escape plans, sexual messages directed at minors or at unwilling adults, and institutional security concerns.

The Federal Bureau of Prisons created its own electronic messaging system for inmate and public use, the Trust Fund Limited Inmate Computer System (TRULINCS), in 2009, which is governed by Program Statement 5265.013, and is based on the Bureau's authority in 18 U.S. Code § 402 to provide for the care of prisoners. It is now available at all federally run prison facilities, although not at contract facilities.

It does not involve access to the Internet. Examining this program in some detail is worthwhile as it appears to be well thought-out and planned, and may be instructive for other correctional systems considering the development of similar electronic message systems.

The objectives include providing prisoners with an alternative means of written communication with the public, as well as providing prison personnel a "more efficient, cost-effective, and secure method of managing and monitoring inmate communication services." It is also intended to reduce the opportunities for illegal drugs or contraband to be introduced into facilities through inmate mail. An inmate's participation is a privilege, and can be denied or limited by a warden if it is determined to "jeopardize the safety, security, or orderly operation of the correctional facility, or the protection of the public and staff."

Some prisoners may be excluded from participation as part of classification procedures, such as those with a personal history of, or prior offense conduct or conviction for, soliciting minors for sexual activity, or possession/distribution of child pornography through the Internet or other means, and those in a Special Housing Unit (SHU).

“Likewise, an inmate with a personal history or special skills or knowledge of using computers/email/Internet or other communication methods as a conduit for committing illegal activities will be excluded.” While sex offenders are not automatically excluded from participation, an individual assessment can exclude them.

Use of the system by inmates pending either investigation or disciplinary action for possible abuse or misuse of the system may also face partial or total restriction on their use of the messaging system. Criminal prosecution for misuse is also possible.

Inmates can only send and receive electronic messages from individuals on their approved contact list. An inmate must request to exchange electronic messages with a person in the community. They place that person on their contact list, which must be approved by prison staff.

After the prospective contact is approved, an automated message is sent to that person asking if they accept future electronic communication with that inmate or if they want to block it. If the prospective contact accepts messaging, the inmate will then be able to send electronic messages to that individual.

All messages on the system, including those to and from inmates, members of the public, and prison staff members, are subject to monitoring by trained staff, with the contents retained. Individual messages to and from inmates can be rejected by personnel monitoring the system.

Inmates are only allowed to exchange electronic messages with persons in the community who have accepted a request to communicate and have consented to monitoring. Inmates may place attorneys, “special mail” recipients, or other legal representatives on their electronic message contact list, with the acknowledgment that electronic messages exchanged with such individuals will not be treated as privileged communications and will be subject to monitoring. An attachment sent with an electronic message is removed from the message and is not delivered.

The bases on which an incoming or outgoing message can be rejected includes that it:

- Depicts, describes, or encourages activities that may lead to the use of physical violence or group disruption.
- Depicts or describes procedures for the construction or use of weapons, ammunition, bombs, or incendiary devices.
- Depicts, encourages, or describes methods of escape from Bureau facilities, diagrams, drawings, or similar descriptions of prisons.
- Encourages, instructs, or may facilitate criminal activity.

- Constitutes unauthorized direction of an inmate's business (see 28 CFR Part 541, subpart B, regarding Inmate Discipline).
- Contains threats, extortion, or obscenity.
- Is written in, or otherwise contains, a code.
- Constitutes sexually explicit material that, by its nature or content, poses a threat to the safety, security, and orderly operation of Bureau facilities, or protection of the public and staff.
- Depicts or describes procedures for the manufacture of alcoholic beverages or drugs.

While the Program Statement explicitly addresses the rejection of messages written in code, it does not address the possibility of electronic messages written in a language other than English, which has been the subject of some litigation when it comes to inmate postal mail.

The sender of a rejected message is notified of the rejection and the reason for the rejection, although the intended recipient is not notified. Either inmates or members of the public who try to send rejected messages or who forward inmate electronic messages to an unauthorized address may be removed from participation in the program.

Monitoring of electronic messages may be easier for prison staff than the handling of written postal mail which must be opened, inspected for possible contraband, and often involves the need to try to decipher an individual's handwriting.

There does not yet appear to be any reported court decisions challenging various restrictions on the use of the system, but many of the same legal principles that apply to postal mail to and from prisoners may apply, modified by the voluntary consent required of all users of the system to complete monitoring.

- See Prisoner Mail Legal Issues, 2007 (6) AELE Mo. L.J. 301 and Prisoners and Sexually Explicit Materials, 2010 (2) AELE Mo. L. J. 301. The discussion in Legal Issues Pertaining to Inmate Telephone Use, 2008 (2) AELE Mo. L.J. 301 may also be helpful in this regard.

Inmates can send electronic messages to inmates in another federal facility only if the other inmate is a member of their immediate family or a party or witness in a legal action in which both prisoners are involved. Other restrictions and procedures for approval are listed in the BOP Program Statement.

Inmates are currently charged five cents a minute for the costs of their use of the system, whether reading or writing a message, while members of the public are not. Prisoners can also print out received messages at a cost of fifteen cents a page. The system is operated by Corrlinks, a private company, which also provides similar services in a number of state prisons, such as Iowa, Oklahoma, and Minnesota, where sending an electronic message to prisoners currently costs $0.25, $0.30, and $0.30 per message respectively.

Messages are limited to 13,000 characters. No taxpayer funding was provided for the establishment and operation of the federal system, with funding provided entirely by the Inmate Trust Fund, maintained by the profits from inmate purchases of commissary products, telephone services, and inmate fees for using the system.

Messages sent or received on the TRULINC system can be disclosed for law enforcement purposes without subpoenas, a difference as compared to recorded inmate telephone conversations. "Upon receipt of a properly submitted written request from a law enforcement agency, BOP staff are authorized to release both transactional data (e.g., date, time, electronic message address, electronic message recipient and sender, and length of the message) and copies of the electronic messages."

The system is also now used for inmates to generate required TRULINCS outgoing mail labels to place on outgoing physical U.S. mail. Inmates in SHU or with other security concerns limiting access to TRULINCS can be exempted from this requirement.

- Part 2 of this two-part article includes a discussion of both legal restrictions on and attempts to provide access to electronic messaging in state and local correctional facilities (in the section on Supervised Internet Access).

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