HENRY MCMASTER
ATTORNEY GENERAL

December 15, 2010

Jon Ozmint, Director
SC Department of Corrections
PO Box 21787
Columbia, SC 29221

Dear Mr. Ozmint:

We received your letter requesting an opinion of this Office concerning the use of cell phones by inmates within the South Carolina Department of Corrections (SCDC) and SCDC's access to information about the phone calls illegally made by the inmates.

As provided in the request letter, "SCDC in conjunction with SHAWNTECH Communications, Inc. and Digital Receiver Technologies, (a Boeing subsidiary) has emplaced at Lieber Correctional Institution in Dorchester County a device which has been characterized by the wireless communications industry as 'Managed Access.' The equipment and hardware that comprise this device have been erected in cooperation with the cell phone providers that service Dorchester County. It has also been emplaced with the authorization of the Federal Communication Commission (FCC). The **managed access device acquires the signals of all illegal, unauthorized cell phone signals emanating from within Lieber CI.**"

The letter further explains that the "**data collected by the managed access equipment will include the electronic identifier of the cell phone, the network that provides service to that device and the telephone number that is being called by that device.** The managed access system does not capture the content of any intercepted call unless specifically programmed to do so. This capability will not be enabled."

Specifically, you asked this Office to opine on whether the operation of the above described system, as authorized by the FCC, would violate the definitions and requirements of the South Carolina Code of Laws, Title 17, Chapter 29.

Law/Analysis

Pen Register
Chapter 29 of Title 17 of the South Carolina Code of Laws governs Pen Registers and Traps and Trace Devices. S.C. Code § 17-29-10 defines the term "pen register" as follows:

> a device which records or decodes electronic or other impulses which **identify the numbers dialed** or otherwise transmitted on the telephone **line to which the device is attached**[1] . . .

S.C. Code § 17-29-10(1) (emphasis added). This Office is not a fact-finding entity; investigations and determinations of facts are beyond the scope of an opinion of this Office and are better resolved by a court. Ops. S.C. Atty. Gen., September 14, 2006; April 6, 2006. However, the request letter explained that the managed access equipment will **identify the cell phone being used**, the **network that provides service** to that device and the telephone **number that is being called** by that device. Also, SCDC informed this Office that the data is collected through a pen register. Hence, this opinion presumes that a pen register has been installed and is being used; therefore, S.C. Code § 17-29-10 et seq. is applicable.

Electronic or Wire Communication Service Provider
Generally, a pen register may not be installed or used without first obtaining a court order under S.C. Code § 17-29-40.[2] S.C. Code § 17-29-20(A).[3] However this prohibition does not apply if the pen register is used **by a provider of electronic or wire communication service** in one of the following circumstances:

> (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

---

[1] ". . . but this term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by the provider, or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business." S.C. Code § 17-29-10(1)

[2] S.C. Code § 17-29-40 governs the issuance of court orders authorizing installation of pen registers or trap and trace devices.

[3] Anyone who violates S.C. Code § 17-29-20(A) is guilty of a misdemeanor according to S.C. Code § 17-29-20©.

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service; or
(3) where the **consent of the user of that service** has been obtained.

S.C. Code § 17-29-20(B).

As stated above, this Office is not a fact-finding entity; however, the request letter explained that SCDC is working in conjunction with SHAWNTECH Communications, Inc. and Digital Receiver Technologies. This opinion presumes that SHAWNTECH and Digital Receiver Technologies would be considered "provider[s] of electronic or wire communication service[s]." Under this presumption, S.C. Code § 17-29-20(B) may apply, specifically S.C. Code § 17-29-20(B)(3).

"If a statute's language is plain, unambiguous, and conveys a clear meaning, then the rules of statutory interpretation are not needed and a court has no right to impose another meaning. The words must be given their plain and ordinary meaning without resorting to subtle or forced construction which limit or expand the statute's operation." Strickland v. Strickland, 375 S.C. 76, 88-89, 650 S.E.2d 465, 472 (2007); Op. S.C. Atty. Gen., June 13, 2008. S.C. Code § 17-29-20 is clear that a court order must be obtained before using or installing a pen register unless the pen register is being used by the provider of electronic or wire communication service, in this instance SHAWNTECH and Digital Receiver Technologies, and one of three exceptions apply. According to S.C. Code § 17-29-20(B)(3), a pen register may be used by the provider if consent of the user of the service has been obtained.

Consent By User

It is the opinion of this Office that a court would likely conclude that while no express consent is provided, an inmate implicitly consents to the electronic or wire communication service provider using a pen register to monitor telephone activity. An inmate gives implied consent when he or she is informed of agency policies and procedures, specifically the prohibition regarding the possession and use of cell phones.

For example, the United States District Court for the Southern District of New York explained that the inmate "gave implied consent to such interception by continuing to use the phones after he was put on notice . . . that the calls were being recorded and reviewed." U.S. v. Rittweger, 258 F.Supp. 2d 345, 354 (2003). The court cites other cases that reached similar conclusions. See, U.S. v. Amen, 831 F.2d 373, 379 (2d Cir. 1987) (prisoners had notice of prison telephone interception system and thus their use of the telephones constituted implied consent to monitoring); *accord* U.S. v. Workman, 80 F.3d 688, 693 (2d Cir. 1996) (finding consent even though appellant, having been warned of monitoring, was not specifically told that use of prison telephones constituted consent or that monitoring could include recording); United States v. Willoughby, 860 F.2d 15, 19-20 (2d Cir. 1988) (implied consent given to monitoring and taping when prison gave ample notice that phones

were taped and monitored and prisoner used phones; express consent also found based on prisoner execution of consent form). U.S. v. Rittweger, 258 F.Supp. 2d 345, 354 (2003).

In U.S. v. Lindsey, 2010 WL 4822939, the United States District Court for the District of Minnesota explained that "Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511, prohibits warrantless interception of oral or wire communications and prevents admission of such recordings into evidence unless a specific exception in the Act applies." The court further explains that "[i]t is not unlawful, however, for law enforcement officials to 'intercept a wire, oral, or electronic communication, where ... one of the parties to the communication has given prior consent.'" Lindsey, 2010 WL 4822939; 18 U.S.C. § 2511(2)©. In this case, the prisoner was made aware of the prison's policy to record or monitor all prisoner phone calls. Therefore, the court concluded that the prisoner implicitly consented to such monitoring by making the phone call. Lindsey, 2010 WL 4822939. See also, United States v. Horr, 963 F.2d 1124, 1127 (D.Minn.1992); United States v. Morin, 437 F.3d 777, 780 (8th Cir.2006) (holding that a prisoner handbook and signs informing defendant of call monitoring policy supported a finding of implied consent); Friedman v. United States, 300 F.3d 111, 122-23 (2d Cir.2002) (holding that a sign stating that calls from jail cells would be recorded constituted sufficient notice to support a finding of implied consent).

Similar to the Lindsey case, the prisoners at Lieber Correctional Institution are made aware of the facility's prohibition against the possession and use of cell phones by inmates. Therefore a court could, and most likely would, logically conclude that the inmates have consented to such monitoring.[4]

Authority to Define and Regulate Contraband

S.C. Code § 24-3-950 provides that the Director of SCDC may establish definitions as to what material is considered contraband. Criminal penalties are established for inmates found in possession of contraband and for those who furnished or attempted to furnish the contraband. S.C. Code § 24-3-950 reads as follows:

> It shall be unlawful for any person to furnish or attempt to furnish any prisoner under the jurisdiction of the Department of Corrections with any matter declared by the director to be contraband. It shall also be unlawful for any prisoner under the jurisdiction of the Department of Corrections to possess any matter declared to be contraband. Matters

[4] This Office is unaware of the exact wording used when warning inmates at Lieber CI about the prohibition against the possession and use of cell phones. To closely follow the reasoning in the Lindsey case, it would be best for Lieber CI to specifically warn that phone calls made from the correctional institute may be monitored and identified by a pen register as part of the managed access system.

> considered contraband within the meaning of this section shall be those which are determined to be such by the director and published by him in a conspicuous place available to visitors and inmates at each correctional institution. Any person violating the provisions of this section shall be deemed guilty of a felony and, upon conviction, shall be punished by a fine of not less than one thousand dollars nor more than ten thousand dollars or imprisonment for not less than one year nor more than ten years, or both.

S.C. Code § 24-3-950.

SCDC Policy defines contraband as "any item which was not issued to the inmate officially; Any item which cannot be purchased in the institutional canteen; Any item which has not been authorized by the Warden and/or Agency policy." SCDC Policy OP-22.35, Contraband Control. Section 1.13 of this policy specifically mentions cell phones and other electronic components as contraband.

If an inmate violates the set standards, certain sanctions are imposed. Disciplinary charge 898 specifically addresses the possession of any cell phone or other type of communication device. The charge explains that possessing, receiving, using, concealing, disposing of, storing, buying or selling a cell phone or other communication equipment such as an MP3 player, i-Pod, or other like devices is a prohibited act. See, SCDC Policy OP-22.14. As seen below, we deem such a policy to be reasonable and in furtherance of the prison's duty to ensure security and protection of the public.

Privacy Expectation

According to the request letter, signs are placed around SCDC to alert visitors to the definition of contraband. Also, newly received inmates are informed of agency policies and procedures, specifically they are instructed of the prohibition against the possession and use of cell phones. Therefore, both inmates and visitors are made aware of relevant policies.

While "[p]rison walls do not form a barrier separating prison inmates from the protections of the Constitution," Turner v. Safley, 482 U.S. 78, 84, 107 S.Ct. 2254, 2259 (1987), it has been well recognized that these rights must be exercised with due regard for the "inordinately difficult undertaking" of administering and monitoring a secure correctional facility. Turner, 482 U.S. 78, 85. The rules and regulations set forth in SCDC's policy would undoubtedly be found legitimate as their purpose is expressly aimed at protecting and maintaining prison security and public safety. Pell v. Procunier, 417 U.S. 817, 823, 94 S.Ct. 2800, 2804 (1974).

In Hudson v. Palmer, 468 U.S. 517, 104 S.Ct. 3194 (1984), the U.S. Supreme Court held as follows:

> [S]ociety is not prepared to recognize as legitimate any subjective expectation of privacy that a prisoner might have in his prison cell and that, accordingly, the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell. The recognition of privacy rights for prisoners in their individual cells simply cannot

> be reconciled with the concept of incarceration and the needs and objectives of penal institutions.
>
> . . .
>
> We are satisfied that society would insist that the prisoner's expectation of privacy always yield to what must be considered the paramount interest in institutional security. We believe that it is accepted by our society that '[l]oss of freedom of choice and privacy are inherent incidents of confinement.' Bell v. Wolfish, 441 U.S. 520, 537, 99 S.Ct. 1861, 1873 (1979).

Hudson v. Palmer, 468 U.S. 517, 526 and 528.

SCDC has expressed the grave dangers that can come from inmates having access to cell phones, and making or attempting to make calls to those on the outside. In the interest of public safety, a certain level of monitoring inmate activity is necessary, including the interception of illegal phone calls made from within correctional facilities.[5]

In 1974, the U.S. Supreme Court specifically addressed the inspection of mail written by prisoners, but the concept can be extended to the idea of phone calls made by prisoners. Wolff v. McDonnell, 418 U.S. 539, 94 S.Ct. 2963 (1974). However, there is a logical added level of monitoring for cell phones because prisoners are not permitted to posses or use contraband, specifically cell phones, while letter writing is permissible. Also, under this managed access system the content of the phone conversation is not accessed, simply the fact that a call was made. In Wolff, the Supreme Court explained that "the prisoners' First Amendment rights are not violated by inspection of their mail for contraband, so long as the mail is not read and the inspection is done in the prisoner's presence so that he can be assured that the privacy of his communications is not breached. Such a procedure should adequately serve the prison administration's interest in ensuring that weapons, drugs, and other prohibited materials are not unlawfully introduced into the prison, while preserving the prisoner's First Amendment right to communicate with others through the mail." Wolff v. McDonnell, 418 U.S. 539, 601. In our view, the banning of cell phones to prisoners violates no provision of the Constitution.

Conclusion

It is the opinion of this Office that a court would likely find under S.C. Code § 17-29-20(B) that an electronic or wire communication service provider, in conjunction with SCDC, may install and use a pen register to identify calls made from the correctional facility and to identify the numbers being

---

[5] The data collected by the managed access equipment will include the electronic identifier of the cell phone, the network that provides service to that device and the telephone number that is being called by that device; the system will not capture the content of any intercepted calls.

called. While S.C. Code § 17-29-20(A) generally requires a court order to install or use a pen register, a court would likely find that the "consent of the user" exception applies, S.C. Code § 17-29-20(B)(3), as inmates consent to the monitoring when they chose to use cell phones after being informed of the prohibition against possessing or using cell phones. See, U.S. v. Rittweger, 258 F.Supp. 2d 345; U.S. v. Lindsey, 2010 WL 4822939. Such monitoring by the "managed access" system is necessary to further the correctional facilities' interest of preventing inmates from using contraband such as cell phones and promoting public safety. Regardless of the means of communication, there is no expectation of privacy when an inmate contacts or attempts to contact individuals outside the institution.[6] Wolff, 418 U.S. 539. Monitoring is necessary for public safety and for maintaining sound penological practices. Hudson v. Palmer, 468 U.S. 517. In our opinion, SCDC may ban and monitor cell phone calls in the manner indicated in your letter without violating the Constitution.

This Office does not generally address federal regulations; however, we caution SCDC that its activities should be in compliance with the FCC and any other relevant federal law.

Sincerely,

Henry McMaster
Attorney General

Leigha Blackwell

By: Leigha Blackwell
Assistant Attorney General

REVIEWED AND APPROVED BY:

Robert D. Cook

Robert D. Cook
Deputy Attorney General

---

[6] Some may raise concern that not only is the inmate's privacy at issue but the privacy of the receiver of the call. While this argument may be viewed as colorable, S.C. Code § 17-29-20(B) requires only the consent of the user, in this case the "user" is the inmate who initiates the call, not the receiver on the outside of the correctional institute.