

**OP. NO. 04-021**

**CRIMINAL PROCEDURE: INTERCEPTION OF WIRE,  
ELECTRONIC OR ORAL COMMUNICATIONS.**

**CRIMES AND OFFENSES GENERALLY: CRIMES INVOLVING  
FRAUD – FALSE REPRESENTATIONS TO OBTAIN PROPERTY  
OR CREDIT.**

**Disclosure by telephone company employees of contents of  
intercepted telephone conversations to law-enforcement  
officers and in testimony at criminal trial for offense of  
fraudulently obtaining or using telephone service.**

The Honorable Harvey L. Bryant  
Commonwealth's Attorney for the City of Virginia Beach  
May 27, 2004

### **Issues Presented**

You ask whether, pursuant to § 19.2-62(B. 1), employees of a wire or electronic communications service who have intercepted telephone conversations in the course of investigating a complaint of fraudulent telephone service may disclose the contents of those intercepted conversations during testimony at a criminal trial for the offense of fraudulently obtaining or using telephone service. You also ask whether such employees may disclose to law-enforcement officers the contents of the intercepted telephone conversations.

### **Response**

It is my opinion that the subject telephone company employees may disclose the contents of the intercepted telephone conversations both to law-enforcement officers and in testimony at a criminal trial for the offense of fraudulently obtaining or using telephone service.

### **Background**

You state that a consumer received a bill from a telephone company for a telephone he did not own, order or use. The consumer complained to the telephone company, and the company began an investigation. During the investigation, telephone

company employees intercepted telephone calls from the subject telephone, in order to determine who was committing the fraud.

Telephone company employees recorded conversations that established crimes of fraudulently obtaining telephone service. They also recorded conversations that evidenced identity theft and credit card fraud. The employees disclosed the recorded conversations to the police. No party to the recorded conversations consented to the interception or recording of the conversations, nor were the conversations intercepted pursuant to court order.

For purposes of this opinion, you assume that the telephone company employees stopped intercepting telephone conversations once they determined who was fraudulently obtaining the telephone service. You also assume that the phone company intercepts telephone conversations as a normal investigative technique used in fraud investigations.

### **Applicable Law and Discussion**

Chapter 6 of Title 19.2, §§ 19.2-61 through 19.2-70.3, contains the provisions governing the interception of wire, electronic or oral communications. Section 19.2-62(A) provides that any person who intentionally intercepts wire, electronic or oral communications "shall be guilty of a Class 6 felony."<sup>1</sup> Section 19.2-62(B. 1), however, provides:

It shall not be unlawful under this chapter for ... an officer, employee or agent of a provider of wire or electronic communications service, whose facilities are used in the transmission of a wire communication,<sup>[2]</sup> to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.<sup>[3]</sup>

Federal law provides an exception to the general prohibition against interception in a manner similar to § 19.2-62(B. 1).<sup>4</sup>

While there are no Virginia case decisions on the subject, some federal courts have addressed the interception of telephone conversations by a telephone company.<sup>5</sup> In a federal district court case involving interception of telephone conversations by a telephone company, the court considered three issues in

determining whether the telephone company's actions violated federal wiretap law: (1) whether the provider of electronic communications service had reasonable cause to suspect that its property rights were being abused by a specific subscriber; (2) whether the interception activities were conducted upon a permissible telephone; and (3) whether the interception activities were reasonable.<sup>6</sup> The court noted that there must be some substantial nexus between the use of the telephone instrument to be monitored and the specific fraudulent activity being investigated.<sup>7</sup>

In the situation you describe, each of the questions posed in the federal district court case may be answered in the affirmative. Certainly, there was a substantial nexus between the suspected fraud and the subject telephone. Every use of the suspect telephone potentially was illegal since the billed customer had complained that he did not own or order the telephone. The interception of the telephone conversations, conducted in the ordinary course of the telephone company's investigation of a complaint of fraud, squarely falls within the exception to interception contemplated by § 19.2-62(B. 1).

Disclosure to law enforcement also falls within the permissible actions contemplated by the statute. Certainly, a report to the police of discovered criminal activity, ascertained in the ordinary course of investigating fraud and protecting the property of the telephone company, is proper under the statute.<sup>8</sup>

Testimony in court regarding the conversations intercepted by the telephone company employees also would be permissible under § 19.2-62. Under § 19.2-62(B. 1), the provider of wire or electronic communications service may "disclose or use" the intercepted wire communications "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." You conclude in your letter that, if it is the normal policy for the phone company to prosecute criminally those who commit telephone fraud, testimony at a criminal trial would be a necessary incident to the protection of the rights and property of the provider.<sup>9</sup> A criminal prosecution, indeed, may be a necessary incident to protect the rights and property of the telephone company. It may be the only way to stop fraud.

Section 19.2-65 provides that no part of an intercepted conversation or evidence derived therefrom may be received in any trial if the disclosure would violate Chapter 6. The disclosures

referenced in your request would not violate Chapter 6. Section 19.2-67(C) provides that testimony about communications or derivative evidence obtained from authorized interceptions is limited to criminal proceedings for the offenses listed in § 19.2-66, which is not applicable to the interceptions by employees of the phone company.<sup>10</sup>

### **Conclusion**

Accordingly, it is my opinion that the subject telephone company employees may disclose the contents of the intercepted telephone conversations both to law-enforcement officers and in testimony at a criminal trial for the offense of fraudulently obtaining or using telephone service.

<sup>1</sup>Va. Code Ann. § 19.2-62(A)(4) (Michie Repl. Vol. 2000).

<sup>2</sup>"*Wire communication*" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection, including the use of such connection in a switching station, furnished or operated by any person engaged in providing or operating such facilities for the transmission of communications." Section 19.2-61 (LexisNexis Supp. 2003). Thus, the term "wire communication" includes communication made over cellular telephones.

<sup>3</sup>Section 19.2-62(B. 1) prohibits random monitoring by a provider of wire communication service to the public "except for mechanical or service quality control checks."

<sup>4</sup>"It shall not be unlawful under this chapter for ... an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks." 18 U.S.C.A. § 2511(2)(a)(i) (West Supp. 2004).

<sup>5</sup>See *generally* 1 James G. Carr & Patricia L. Bellia, *The Law of Electronic Surveillance* §§ 3:32 to 3:43 (2004).

<sup>6</sup>*United States v. McLaren*, 957 F. Supp. 215, 217-18 (M.D. Fla. 1997).

<sup>7</sup>See *id.* at 219.

<sup>8</sup>See *generally* *United States v. Villanueva*, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998) (holding that defendant's argument that AT&T Wireless was not authorized to disclose tapes of intercepted telephone calls to law-enforcement officials ignores plain language of Common Carrier exception authorizing disclosure and disregards purpose of § 2511(a)(a)(i)).

<sup>9</sup>A request by a Commonwealth's attorney for an opinion from the Attorney General "shall itself be in the form of an opinion embodying a precise statement of all facts together with such attorney's legal conclusions." Va. Code Ann. § 2.2-505(B) (LexisNexis Repl. Vol. 2001).

<sup>10</sup>Section 19.2-67(C) applies to interceptions authorized under Chapter 6, pursuant to the requirements surrounding the request by the Attorney General, judicial approval, and other requirements.

[Back to May 2004 Opinion Index](#)