



Click below to link to our offices in:

Chattanooga

Nashville

Knoxville

Memphis

Dalton

The Perils of Electronic Surveillance in the Age of Spyware

Overview

There is an age-old and prominent legal principle between buyers and sellers that “the buyer beware.” The continuing advancement of technological devices and software has created a need for the new legal principle that “the ‘spyer’ beware.” Many individuals, employers, and spouses may not be aware that they are committing criminal violations and exposing themselves to non-dischargeable civil liability. Tenn. Code Ann. § 39-13-601 outlines prohibited activities related to wiretapping and electronic surveillance. The activities listed in this statute are considered an invasion of privacy and are classified as Class D felonies in Tenn. Code Ann. § 39-13-602. Although many electronic means used to eavesdrop on the conversations and communications of others have existed for decades, the abundance and availability of various types of invasive spyware create greater and easier opportunities for one person to virtually ‘spy’ on another and intercept private information. This can create potential criminal and civil liability not only for the person who implements the spyware and intercepts the electronic communications but also for one who unwittingly receives and utilizes the illegally-obtained private information.

§ 39-13-601(a)(1)

Tenn. Code Ann. § 39-13-601(a)(1)(A) explicitly states that a person commits a criminal offense who intentionally intercepts or attempts to intercept “any wire, oral, or electronic communication.” The statute also states that it is a criminal offense for one to intentionally disclose or attempt to disclose the contents of the intercepted information to a third party knowing or having reason to know the

If your server does not support graphics, [click here](#)

Leitner, Williams, Dooley and Napolitan, PLLC will be hosting many upcoming events! To see upcoming events: [click here](#)

information was obtained illegally. Finally, it is a criminal offense under the statute to intentionally use or attempt to use information knowing or having reason to know that this information was obtained illegally. This last offense makes it clear that, even if someone did not directly intercept the electronic communications of another, if he or she received wrongfully intercepted communication and had reason to know or suspect that it was obtained through suspicious means but used or attempted to use the information anyway, he or she will also face liability under this statute. This statute was created prior to the age of the Internet, but the development of the Internet, various advanced electronic tools, and certain software creates substantially more potential for liability under this statute.

Spyware

The rapidly increasing use of and reliance upon electronic devices for communication has created a significant market for spyware, or software that creates the ability for one person to 'spy' on and intercept the electronic communications of others. Anyone can purchase various brands of spyware over the Internet, and, after installing it on someone's computer, can immediately begin to intercept the other person's communications on that computer. Spyware has become so advanced that certain versions of this software can do any or all of the following: record sent and received emails, record instant messages received, record all keystrokes typed, record all downloads, and record all websites visited. Once the spyware is installed on a computer, the installer of the spyware can easily and effortlessly intercept all of this information. This enables the interceptor to obtain not only electronic communications but also passwords to private accounts and websites. Once this information is in the hands of the interceptor, he or she has the ability to freely utilize and disseminate this information.

It is the dissemination of this information that can create criminal and civil liability for third parties. If the interceptor provides the illegally-obtained information to someone else, that person's utilization of that information makes them equally liable. The statute states that a third person is liable for use of this information if that person knew or merely had reason to know of the illegal origins of the information. Granted, it is not always readily apparent that

information provided by someone else was obtained illegally. However, given the significant penalties associated with this statute, it is best to err on the side of caution. If information received from someone else seems ‘too good to be true’ or appears to be information not readily available through legitimate means, that information should not be utilized. There are countless personal- and business-related scenarios in which one person might illegally intercept the private information of another and provide it to another under the guise of legitimately-obtained information. Individuals and businesses must be aware of and consider Tenn. Code Ann. § 39-13-601(a)(1)(A) when they are given information that could be even remotely deemed to have doubtful origins.

Civil Liability

Tenn. Code Ann. § 39-13-601(a) provides for substantial civil damages for any person whose electronic information is intercepted in violation of Tenn. Code Ann. § 39-13-601. Damages awarded will include *the greater of*: 1) the sum of the actual personal or business reputation or relationship losses plus any profits may by the interceptor or 2) *the greater of* \$100.00 per day for each day of the violation or \$10,000.00. *Punitive damages and attorney’s fees will also be awarded to the wronged party.* Clearly, the legislature takes this issue seriously and has enabled the awarding of substantial penalties against anyone found in violation of the statute.

Conclusion

Increased electronic communications have created a market for software that can enable one person to intercept electronic communications made by another. This violation of privacy can create criminal and civil liability not only for the interceptor but also for anyone to whom the interceptor provides the wrongfully intercepted information. All persons should be aware of this statute and the ease with which spyware can allow the interception of personal electronic information. If someone is provided with information that seems likely to have been obtained by suspicious or illegal means, the information should not be used under any circumstances. No matter how useful the information may be, the

penalties are too high to risk potential violation of Tenn. Code Ann. § 39-13-601.

Submitted by:

David W. Noblit, Esq.

Mary C. DeCamp, Esq.

Leitner, Williams, Dooley, & Napolitan, PLLC

801 Broad Street, 3rd Floor

Chattanooga, TN 37402

Phone: 423.265.0214

Fax: 423.266.5490

mailto: david.noblit@leitnerfirm.com

mailto: mary.decamp@leitnerfirm.com

www.leitnerfirm.com

If you would like to unsubscribe to this newsletter, please reply to this email with "Unsubscribe" in the subject box. Thank you.

The LWDN Client Update Quick Flash is published for the benefit of our clients. While each article is written to be informative and helpful, we recognize that every situation is unique in its legal considerations. The firm encourages readers to consult an attorney regarding particular application and interpretation of the law. Permission is granted to make and distribute, without charge, copies of this entire document provided that such copies are complete and identify Leitner, Williams, Dooley & Napolitan, PLLC as the author. All other rights are reserved.

