WIRETAPPING AND SPOILATION
AUSTIN BAR ASSOCIATION BENCH BAR CONFERENCE
4 April 2014
Scott C. Smith - www.DefenseLawyer.net

I. KEYLOGGERS AND ELECTRONIC COMMUNICATION PRIVACY LAWS

As people tend to become increasingly dependent upon electronic communication, the acquisition and use of other persons emails is becoming much more frequent and significant. State legislatures and congress have moved to adapt old laws governing the "wiretaps" of phones to new technologies. Unfortunately, legislators often seem to not fully understand what they are attempting to regulate and use antiquated concepts as their starting points.

The basic structure of federal privacy laws, as with Texas privacy laws, is based in great part on the distinction between prospective surveillance and retrospective surveillance.

> "Prospective surveillance refers to obtaining communication still in the course of transmission, typically by installing a monitoring device at a particular point in the network and scanning the traffic as it passes by that point. The monitoring is prospective because of that the communication has not yet reached the place where the surveillance device is installed. For example, a traditional wiretapping device taps into the conversation while it is happening; any communications sent over the line will be tapped. Similarly, an Internet wiretapping program such as a "packet sniffer" scans packets of Internet traffic at a particular place in the network where the program is directed to function.
>
> In contrast, retrospective surveillance refers to access to storage communications that may be kept in the ordinary course of business by a third-party provider. For example if an FBI agent issues a subpoena ordering an ISP to disclose basic subscriber information about a particular Internet account, that excess is a type of retrospective surveillance. The ISP will have generated that record it sometime in the past in the ordinary course of its business; the subpoena seeks the disclosure of a stored record that already has been created."
> Orin S. Kerry, Computer Crime Law (Thomson - West 2006).

Sometimes if may be difficult to ascertain whether communications are obtained in violation 16.02 (unlawfully intercepted communications) or in violation of 16.04 (unlawfully accessed stored Communications). This distinction is significant because information obtained in violation of the former can be legally used or disseminated while there is no such prohibition on the use or dissemination of the latter.

Courts have wrestled with the "fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communication." *Obrien v. Obrien*, 899 So. 2d 1133 (5th Dist. Court of Appeals of FA - 2005). In *Obrien* a wife installed the Spector spyware program on her computer to access her husband's

emails. She argued that the spyware accessed emails that were in storage and, therefore, did not intercept them. However, the court found that the program copied them as they were transmitted and found that use of it did constitute "interception".

Generally speaking, covertly acquiring or guessing another person's password to log into their hotmail or G-mail accounts without their consent would be retrospective surveillance in violation of the statutes restricting access to stored communication. On the other hand, the use of spyware which intercept, copies and transmits e-mails as they are transmitted will violate statutes restricting unauthorized interception of electronic communications. Keylogger programs which record which keys are activated on a computer can fall in a gap between these two types of statutes.

Many cases hold that use of a keylogger is not a violation of the Federal Wiretap Act because did they not catch emails "in flight", i.e. the device does not access e-mail messages contemporaneously with their transmission and, therefore, do not "intercept" communications. However, there are no Texas cases on point and it is possible that a Texas court may decide differently in certain fact situations. Several decisions base their holding on the argument that the keylogger did not affect interstate or foreign commerce. This issue would be irrelevant to a state statute. Furthermore, one court noted, "Conceivably, the keylogger software at issue here could be used to contemporaneously capture information or signals being transmitted beyond the user's computer. If so, this would bring the keylogger software within the definition of a scanning receiver as "a device or apparatus that can be used to intercept a wire or electronic communication in violation of [the Wiretap Act]." 18 U.S.C. § 1029(e)(8) (emphasis added). However, the Government points to no evidence in the record showing that the keylogger at issue here had that capacity and we have found none." *United States v. Barrington*, 648 F.3d 1178, 1202-1203 (11th Cir. 2011)

Just how the keylogger functions is pertinent to the analysis of whether if violate 16.02. If the keylogger simply records and stores information on a stand alone computer for future viewing, it would likely not violate 16.02. However, if the keylogger automatically transmits this information to another computer, Texas courts could find that it does violate 16.02. In comparison, programs that automatically transmit outgoing or incoming emails to another address probably would violated 16.02.

Answering questions of whether particular means of surveillance will violate any currently existing privacy protection laws may often be difficult. The answer to each question will require a detailed knowledge of the facts of each situation, including what permissions were given, what type of consent can be implied and the particular technical details of how the communications were acquired. (As the *Barrington* case below shows, it may be important to look at not just what kind of device or program is used to access the communications, but also how it is configured.) This information will then need to be assessed in light of the following laws that may apply.

II. ELEMENTS (SIMPLIFIED) OF OFFENSES DESIGNED TO PROTECT ELECTRONIC COMMUNICATION PRIVACY

16.02 (b)(1) Tx Penal Code Unlawful Interception of Wire, Oral or Electronic Communications. [Also see 18 USC 2511 (1)(a)]
- Note: deals with communications that are "in flight" as distinguished from those that have already been transmitted and now are in storage.
- intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept. ("Intercept" means the aural or other acquisition of the contents of a wire, oral, or electronic communication through the use of an electronic, mechanical, or other device.18.20 (3) Texas Code of Criminal Procedure.)
- a wire, oral, or electronic communication
Penalties: Felony II
Defenses: the actor is the a party to the communication or has consent from a party to the communication and various other affirmative defenses where the actor has legal authority to intercept.

16.02 (b)(2) and (3) Tx Penal Code Disclosure or Use of Unlawfully Intercepted Wire, Oral or Electronic Communications.[Also see 18 USC 2511 (1)(b and c) which is slightly different.]
- Note: deals with communications that are "in flight" as distinguished from those that have already been transmitted and now are in storage.
- disclosure or endeavors to disclose communications one knows or has reason to know were intercepted
- uses or endeavors to use contents of a communication if the person knows or is reckless about it being intercepted.
Penalties: Felony II
Defenses: the actor is the a party to the communication or has consent from a party to the communication and various other affirmative defenses where the actor has legal authority to intercept.

16.04 Tx Penal Code Unlawful Access to Stored Communications [Also see 18 USC 2701 which is slightly different.]
- Note: deals with communications that have already been transmitted and now are in storage as distinguished from those that are "in flight".
- obtains, alters, or prevents authorized access to
- a wire or electronic communication
- while the communication is in " electronic storage" (see 18.21 CCP which refers to 18.20 which defines it as "any storage of electronic customer data in a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion, or transmission, and includes any storage of a wire or electronic communication by an electronic communications service or a remote computing service."“Electronic communications service" means a service that provides to users of the service the ability to send or receive wire

or electronic communications. Note: the definition of "electronic storage" was amended in the last legislative session to include data in individual computers whereas the federal statute only covers communications stored in a "facility" that provides "electronic communication service".)
- by obtaining access without authorization or exceeding authorization for access
- Note: This statute does not punish the use and disclosure of communication obtain in violation of it.
Penalty: Class A misd unless with intent to obtain a benefit or harm another in which case State Jail Felony
Defenses: conduct authorized by the service, the user of the service, the addressee or intended recipient, or 18.21 CCP.

33.02 (a) Tx Penal Code Breach of Computer Security
- access a computer, computer network or computer system
- without consent of owner
Penalty: Punishment ranges from class B Misd to State Jail Felony

33.02 (b) Tx Penal Code Breach of Computer Security
- same elements as (a)
- intent to defraud or harm another
- alters, damages or deletes property
Penalty: Punishment ranges from State Jail Felony - Felony I (depending on amount of loss and misc other factors).

37.09 Tx Penal Code Tampering with Or Fabricating Physical Evidence
- knowing that an investigation or official proceeding is pending or in progress
- alters, destroys, or conceals
- any record, document, or thing
- with intent to impair its verity, legibility, or availability as evidence in the investigation or proceeding
Penalty: Felony III

7.01 Tx Penal Code Parties to Offenses
(a) A person is criminally responsible as a party to an offense if the offense is committed by his own conduct, by the conduct of another for which he is criminally responsible, or by both.
(b) Each party to an offense may be charged with commission of the offense.

III. CASE LAW

CONSENT

We do not necessarily limit the "under color of law" language in §2511 to law enforcement officers acting within the scope of their authority. Yet there must be some logical and reasonable connection between the government worker's job description and eavesdropping.
Thomas v. Pearl, 998 F.2d 447, 451 (C.A.7 (Ill.),1993)

Statute prohibiting unlawful interception of electronic communication applies to interspousal telephone wiretaps. V.T.C.A., Penal Code § 16.02(b)(1). *Duffy v. State*, 33 S.W.3d 17 (Tex.App. El Paso,2000)

Parent's surreptitious recording of child's conversation not a violation of wiretap statute because CCA recognizes parent-child vicarious exception to the Texas wiretap statute. "Appellant argues that the vicarious-consent exception does not apply to the wiretap laws. He bases this argument on Duffy v. State, 33 S.W.3d 17, 25 (Tex.App.-El Paso 2000, no pet.), and Kent v. State, 809 S.W.2d 664, 668 (Tex.App.-Amarillo 1991, pet. ref'd), in which both courts stated that section 16.02 must be applied in all circumstances that are not specifically excepted. However, as the court of appeals noted, Duffy and Kent are distinguishable from Appellant's case because those cases addressed whether one spouse can vicariously consent to the recording of the other spouse's conversation, rather than the issue of whether a parent can vicariously consent to the recording of her child's conversations. Alameda, 181 S.W.3d at 775 n. 1. The fact that there is no interspousal *222 consent exception to the wiretap statute does not preclude us from recognizing a parent-child vicarious-consent exception." *Alameda v. State*, 235 S.W.3d 218, 221-22 (Tex.Crim.App.,2007)

We are persuaded by the reasoning in Riley and the federal cases cited therein. It is undisputed that appellant's telephone conversations contained a prompt indicating that calls may be recorded or monitored. It is also undisputed that postings throughout the jail informed the inmates that their calls may be monitored or recorded. We therefore hold that, under the circumstances presented here, appellant impliedly consented to the recording of his telephone conversations. Consequently, the recording did not violate Texas Penal Code section 16.02. See Tex. Penal Code Ann. § 16.02(c)(3)(A). *Banargent v. State*, 228 S.W.3d 393, 404 (Tex.App. Houston [14 Dist.],2007)
We hold that words that are spoken into a telephone receiver and that can also be heard in the area surrounding the speaker without electronic assistance are not "wire communications" as defined in Article 18.20, § 1(1). Any recording of those words merely memorializes what could be seen and heard in the interview room. *Moseley v. State*, 252 S.W.3d 398, 403 (Tex.Crim.App.,2008)

INTERCEPTION VS. ACCESSING STORED COMMUNICATIONS

“The overwhelming body of case law, including from one district court in this circuit earlier this year, finds that, unless an e-mail is actually acquired in its split second transmission over a computer network, it cannot be "intercepted" as that term is reasonably understood. As discussed below, this court finds this interpretation persuasive, and, therefore, the defendants should prevail as a matter of law on Cardinal's wiretap act claims.

The Third, Fifth, Ninth, and Eleventh Circuits all agree that, for a communication to be "intercepted" under the FWA, that communication must be acquired during the "flight" of the communication. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3rd Cir.2003); U.S. v. Steiger, 318 F.3d 1039, 1047 (11th Cir.2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir.2002); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir.1994). In support of this view, there is, of course, the ordinary dictionary definition of "intercept," which is "to stop, seize, or interrupt in progress or course before arrival." Konop, 302 F.3d at 878 (citing Webster's Ninth New Collegiate Dictionary 630 (1985)). Also, there is the statutory history, which shows *980 that Congress created the SCA for the express purpose of addressing "access to stored ... electronic communications and transactional records." Id. at 879 (citing S. Rep. 99-541 at 3) (emphasis added). Also, until October 2001, the definition of "wire communication" in the FWA included information in electronic storage, such as a voicemail, but the definition of "electronic communication" in the FWA did not include information in electronic storage, indicating that something like an e-mail would not be covered by the FWA. Id.; Fraser, 352 F.3d at 114. Further, after 9/11, Congress amended the FWA to eliminate communications in electronic storage from the definition of "wire communication," further indicating a congressional intent that the FWA should be primarily concerned with information in active transport, not stored information. Id.” *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967.

"As an initial matter, the law in the Ninth Circuit is clear that gaining access to stored electronic information does not constitute a violation of § 2511. Konop, 302 F.3d at 878. That is, to "intercept" electronic communications means to acquire it during transmission, not while it is in electronic storage. *Id.* In *Konop*, the court concluded that the access to a protected section of a website does not constitute a violation of the Wiretap Act, reasoning that there is no interception of electronic communications, but only access to stored electronic information. Id. at 872-873, 879. Brahmana's claim that Lembo's access to his stored personal email by itself violates § 2511(1)(a) is precluded by *Konop*, and therefore does not constitute a violation of § 2511(1)(a)." *Brahmana v. Lembo*, 2009 WL 1424438 (N.D.Cal.), 2 (N.D.Cal.,2009) Communications are in electronic storage under the Stored Communications Act (SCA), and thus outside the scope of the Wiretap Act, even where the storage is transitory and lasts for only a few seconds. *Columbia Pictures, Inc. v. Bunnell*, C.D.Cal.2007, 245 F.R.D. 443.

KEYSTROKES GENERALLY NOT ELECTRONIC COMMUNICATIONS UNDER FEDERAL WIRETAP ACT

Transmission of keystrokes from keyboard to computer's processing unit was not "electronic communication," and thus defendant's interception of keystrokes did not violate Federal Wiretap Act, even though system was connected to network that affected interstate or foreign commerce,

where communication was intercepted before it was transmitted by network. *U.S. v. Ropp*, C.D.Cal.2004, 347 F.Supp.2d. 831.
"Informed by the decisions discussed in this memorandum, and the many cases cited in the papers submitted by the parties, the Court concludes that the communication in question is not an "electronic communication" within the meaning of the statute because it is not transmitted by a system that affects interstate or foreign commerce. The "system" involved consists *838 of the local computer's hardware-the Central Processing Unit, hard drive and peripherals (including the keyboard)-and one or more software programs including the computer's operating system (most likely some version of Microsoft Windows although other possibilities exist), and either an e-mail or other communications program being used to compose messages. Although this system is connected to a larger system-the network-which affects interstate or foreign commerce, the transmission in issue did not involve that system. The network connection is irrelevant to the transmissions, which could have been made on a stand-alone computer that had no link at all to the internet or any other external network. Thus, although defendant engaged in a gross invasion of privacy by his installation of the KeyKatcher on Ms. Beck's computer, his conduct did not violate the Wiretap Act. While this may be unfortunate, only Congress can cover bases untouched. *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 114 (3rd Cir.2003); see also *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir.), cert. denied, 538 U.S. 1051, 123 S.Ct. 2120, 155 L.Ed.2d 1095 (2003) (courts cannot create remedy where Congress had established none)." *U.S. v. Ropp*, 347 F.Supp.2d 831, 837-38 (C.D.Cal.,2004)

Co-workers' capture of employee's keystrokes using a keylogger program, such that co-workers obtained employee's passwords for various things, including her bank account, was not a system that affected interstate or foreign commerce, and therefore, keystrokes were not electronic communications under the Federal Wiretap Act (FWA). 18 U.S.C.A. § 2511(1)(c, d). *Rene v. G.F. Fishers, Inc.*, 817 F.Supp.2d 1090 (S.D.Ind.,2011).

We have held that, to violate the Wiretap Act, an interception of electronic communications must occur contemporaneously with their transmission. United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir.2003). Accordingly, use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce).[Footnote 25: Cf. United States v. Scarfo, 180 F.Supp.2d 572, 582 & n. 5 (D.N.J.2001) (keylogger configured to record a keystroke only if all the computer's communications ports were inactive did not entail interception of a communication); United States v. Ropp, 347 F.Supp.2d 831, 837-38 (C.D.Cal.2004) (Wiretap Act's definition of electronic communications applies only to data that is in fact being transmitted beyond a local computer by a system that affects interstate commerce).] ....**Conceivably, the keylogger software at issue here could be used to contemporaneously capture information or signals being transmitted beyond the user's computer. If so, this would bring the keylogger software within the definition of a scanning receiver as "a device or apparatus that can be used to intercept a wire or electronic communication in violation of [the Wiretap Act]." 18 U.S.C. § 1029(e)(8)** (emphasis added). However, the Government points to no evidence in the record showing that the keylogger at issue here had that capacity and we have found none. *United States v. Barrington*, 648 F.3d 1178, 1202-1203 (11th Cir. 2011)

In *Bailey v. Bailey*, 2008 WL 324156 (E.D. Mich., 2008), the husband installed key logger software on his home computers to obtain the password to his wife's new e-mail account. After he learned the password, he accessed the wife's e-mail account and read her messages. During the subsequent custody trial, the husband's lawyer impeached the wife's testimony with an e-mail obtained with the use of the password recorded by the key logger software (the wife testified that she had not been drinking while she had children under her care, as ordered by the court for both parties, but e-mails showed she attended a party where she drank alcohol and used illegal drugs). Wife lost the custody suit, and then sued the ex-husband and his attorney for violation of the FWA & SCA. The court entered summary judgment against the wife on her Federal Wiretap Act claim, concluding that the key logger software permitted the husband to learn his wife's password, which he then used to access the wife's e-mail messages. Since the e-mail messages were not obtained contemporaneously with their transmission, there was no violation of the Federal Wiretap Act.

INTERCEPTION HYPOTHETICAL

John and Sue have been married for 15 years. John thinks Sue is having an affair and is planning to leave the house and file for divorce. Before he leaves the house, he wants to get as much information about Sue's affair as he can. John and Sue and their kids all use a computer that is located in John's office at the house. John loads a keylogger program on the computer that sends to his e-mail account all of the keystrokes made on the computer. Sue checks her gmail account on that computer and keeps herself continuously logged in. John looks at Sue's Outlook folder and sees a few messages from to and from her lover and then logs on to her Google account and sees several other older messages which, due to their age, no longer reside on the computer. John sees Sue's e-mails with her boyfriend, which he then forwards to his own e-mail account.

John leaves the house two weeks after that. He decides not to take the office furniture or computer so that he can continue to monitor Sue's e-mails. He observes from the keylogger program that she changed her gmail password and uses the new password to log into gmail and read the e-mails she receives.

John hires Bob to represent him in the divorce and tells Bob that he has evidence of Sue's adultery that he wants to use in the trial. He gives Bob several e-mails, some of which he got before he left the house and some of which he got after he left the house. He tells Bob that he got them from the community computer with the gmail already logged in and does not tell him about the keylogger program or getting the new password. Bob does not notice the dates of the e-mails in relation to the date he left the house. In the temporary orders hearing, Bob questions Sue about the e-mails and admits them into evidence.

Sue gets suspicious of how Bob and John got the e-mails after he left the house. She takes her computer to a PI and he detects the keylogger program. Sue files a civil case against John and Bob for violations of the interception communication statute and the stored communication statute. She also calls the DA and requests that they press charges against Bob and John. Charges are brought against both Bob and John.

SPOLIATION HYPOTHETICAL

Sue had been worried that John would discover her affair. She had gotten in the habit of deleting all her text messages (not just those from her boyfriend) every night before bed. She continued to do so after John filed for divorce and after discovery was served. She had also established a secret e-mail address that she only used from her phone. She would communicate with her boyfriend on the e-mail account about how she felt bad about leaving her husband since he was such a good and involved dad. She would also communicate with him about how she was worried John would get custody of the kids because of her history with depression and medications. Once she realized (after the temporary orders hearing) that John had access to her e-mails, she deleted the secret account with all of its e-mails.

WIRETAPPING ISSUE ANALYSIS CHART

	16.02 (b)(1) Tx Penal Code Unlawful Interception of Wire, Oral or Electronic Communications. [Also see Federal Wiretap Act - 18 USC 2511 (1)(a)]	16.02 (b)(2) and (3) Tx Penal Code Disclosure or Use of Unlawfully Intercepted Wire, Oral or Electronic Communications.[Also see Federal Wiretap Act - 18 USC 2511 (1)(b and c) which is slightly different.]	16.04 Tx Penal Code Unlawful Access to Stored Communications [Also see 18 USC 2701 which is slightly different.]	33.02 Tx Penal Code Breach of Computer Security	37.09 Tx Penal Code Tampering with Or Fabricating Physical Evidence
John loads keylogger on the computer while living with Sue.	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	No violation because does not obtain communications while they are in storage.	No violation because he is "owner" of the computer.	No violation
John reads characters typed by Sue which are transmitted by keylogger while living with Sue.	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	No violation because does not obtain communications while they are in storage.	No. This is not accessing a computer, computer network or computer system.	No violation.

John goes into Outlook and reads Sues emails while living with Sue.	No violation b/c not in "flight."	No violation b/c not in "flight."	Yes, if he lacked or exceed authorization to look at her Outlook folder.	No violation because he is "owner" of the computer.	No violation.
John goes to Google website and logs on to Sue's email account and reads more emails while living with Sue.	No violation b/c not in "flight."	No violation b/c not in "flight."	Yes, assuming he lacked or exceed authorization to look at her Outlook folder.	No violation. This is not accessing a computer, computer network or computer system.	No violation.
John reads characters typed by Sue which are transmitted to him by key logger after moving out.	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	No violation because does not obtain communications while they are in storage.	No. This is not "accessing" a computer, computer network or computer system.	No violation.
John goes to Google website and logs on to Sue's email account with new password and reads Sue's email after moving out.	No violation b/c not in "flight."	No violation b/c not in "flight."	Yes, assuming he lacked or exceed authorization to look at her Outlook folder.	No. This is not accessing a computer, computer network or computer system.	No violation.

Bob uses Sue's emails obtained before John left home.	No. Bob did nothing to intercept, but would be guilty if he asked John to go get more emails ("procures another" and "party liability").	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	No violation to use or disclose information obtained in violation of this statute. No party liability since he did not encourage or assist John to violate the statute.	No violation.	No violation.
Bob uses Sue's emails obtained after John left home.	No. Bob did nothing to intercept, but would be guilty if he asked John to go get more emails ("procures another" and "party liability").	*Probably no violation, but depends on Texas court interpretation of statute and may be affected by how the keylogger is programmed.	No violation to use or disclose information obtained in violation of this statute.No party liability since he did not encourage or assist John to violate the statute.	No violation.	No violation.
Sue deletes text messages after divorce filed and discovery served.	No violation.	No violation.	No violation.	No violation.	Violation if intent to impair availability of emails as evidence.
Sue deleted her secret email account and emails to her boyfriend.	No violation.	No violation.	No violation.	No violation.	Violation if intent to impair availability of emails as evidence.